5

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES ARAGÓN

"AUDITORÍA DE DESARROLLO Y MANTENIMIENTO DE SISTEMAS A LA DIRECCIÓN GENERAL DEL DESTINO DE BIENES DE COMERCIO EXTERIOR PROPIEDAD DEL FISCO FEDERAL"

T E S I S

QUE PARA OBTENER EL TITÚLO DE

INGENIERÍA EN COMPUTACIÓN

P R E S E N T A:

SONIA O. CABALLERO AQUINO

ASESOR:
ING. JOSÉ MANUEL QUINTERO CERVANTES

MÉXICO

2002

Dedicatoria:

A mis Padres:

Por contar siempre con su apoyo incondicional en todos los aspectos, porque me enseñaron que no existe imposibles si se lucha para conseguirlo y porque me dejaron una gran herencia, la del conocimiento. Sin ellos no hubiera logrado lo que soy. Gracias por existir y haberme permitido ser parte de ellos.

A mis hermanos: Chelo y Gabriel porque siempre cuento con su apoyo incondicional y son mi mejor ejemplo a seguir.

Y gracias a todos ellos que creyeron en mi

Sonia Oliva Caballero Aquino

CONTENIDO

ÍNDICE

PÁGINA

CONTENIDO

ÍNDICE

PÁGINA

INTRODUCCIÓN

La auditoría en informática es la revisión y/o la evaluación de los controles, normas, políticas, sistemas referentes a la infraestructura informática, 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 eficaz y segura de la información que servirá para una adecuada toma de decisiones.

El presente trabajo de tesis, muestra la importancia de realizar auditoría en sistemas informáticos para el buen desempeño de los sistemas en desarrollo y mantenimiento, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un alto nivel de seguridad, además debe evaluar todo (informática, organización de centros de información, políticas, procedimientos, controles, hardware y software, etc.).

Se enfoca principalmente en la auditoría a sistemas en desarrollo y mantenimiento en función del llamado "Análisis y Programación de Sistemas y Aplicaciones", en donde se desarrollan puntos, de los cuales destacan:

- Metodología para auditar sistemas de información
- Metodología para auditar bases de datos
- Documentación de los sistemas
- Integridad, confiabilidad y seguridad de la base de datos y sistemas de información.

La auditoría en sistemas en el rubro de desarrollo y mantenimiento de sistemas habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.

El capítulo I hace referencia a las generalidades de auditoría, es decir, explica de manera general el concepto de auditoría, la evolución a través de los años, así como los tipos que existen.

El capítulo II se ocupa en el análisis de los elementos que conforman la auditoría a sistemas, así como los diferentes tipos de metodología que existen para auditar y la estrategia tomada para el desempeño de la auditoría de desarrollo y mantenimiento de sistemas. De igual manera se mencionan aspectos para la revisión de las bases de datos.

El capítulo III. Ejemplifica los métodos y procedimientos descritos en los dos capítulos anteriores aplicados en la auditoría de desarrollo y mantenimiento de sistemas a la Dirección General del Destino de los Bienes de Comercio Exterior Propiedad del Fisco Federal.

Capítulo I

Generalidades de Auditoría

I. GENERALIDADES DE AUDITORÍA

OBJETIVO

DAR A CONOCER EN FORMA GENERAL LOS CONCEPTOS PRINCIPALES DE LA AUDITORÍA.

I.1. ANTECEDENTES

La auditoría se define como la revisión del cumplimiento de lineamientos establecidos por la institución (Manual de Organización, Manual de Procedimientos y políticas de actuación) y/o empresa mediante el análisis de éstos, con el firme propósito de evitar errores, pérdidas económicas, fuga de información entre otras cosas.

La auditoría fue reconocida como profesión en Gran Bretaña por la Ley de Sociedades de 1862, en la que se establecía que las empresas llevarían un sistema normalizado de contabilidad y la necesidad de efectuar una revisión independiente a sus cuentas.

En ese entonces, la auditoría estaba enfocada principalmente en el sector financiero y administrativo ya que comúnmente era donde se detectaban fraudes que hacían que las empresas fueran a la quiebra. El propósito con el cual se realizaban estas auditorías, era analizar y evaluar los controles internos de la empresa, muchas de estas actividades como la revisión de balances, cuentas de pérdida, ganancia, etc., se hacían de manera manual.

Fue hasta 1950 que interviene la informática en las labores de la auditoría financiera, ya que permite que mediante la computadora se lleven a cabo procesos como operaciones, que realizadas manualmente consumirían muchos recursos, causando gastos extras en la empresa.

A raíz de que se vuelve necesaria la utilización de Sistemas de Información (SI) para la realización de auditorías financieras, surge la necesidad de verificar que dichos sistemas funcionen de manera adecuada y que los resultados que arrojen sean íntegros, ya que pudiera darse la manipulación de datos o hacer mal uso de la información.

Es por eso que surge la "auditoría informática" cuya finalidad es verificar el adecuado funcionamiento de la infraestructura informática.

En el campo de la auditoría se han dado cambios a través del tiempo, pero debido al avance tecnológico se adapta a la revisión de controles en los que interviene la tecnología.

Asimismo, para realizar una auditoría se debe contar con una metodología específica para que la auditoría pueda ser confiable, es decir, la planeación general y detallada, las técnicas a utilizar, la ejecución de los trabajos de auditoría, cronogramas de actividades entre otros aspectos con el propósito de llevar un control de actividades específicas a revisar y sustentar plenamente las inconsistencias detectadas a fin de lograr una mejora continua en el área.

Los Sistemas de Información (SI) se han constituido en las herramientas indispensables para automatizar uno de los conceptos más vitales y necesarios para cualquier organización empresarial "Sus procedimientos".

Actualmente la informática está implícita en la gestión integral de la empresa, y por eso las normas y estándares propiamente informáticos deben estar sometidos a una evaluación exhaustiva de manera que funcionen conforme a lo esperado.

En consecuencia, las organizaciones informáticas forman parte de lo que se ha denominado el "management" o gestión de la empresa. Cabe aclarar que la Informática no gestiona propiamente la empresa, ayuda a la toma de decisiones para el mejor desarrollo de la misma.

I.2. CONCEPTO DE AUDITORÍA

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

La función auditora debe ser absolutamente objetiva e independiente, ya que únicamente tiene la tarea de sugerir las acciones para el mejoramiento continuo de la institución y/o empresa. Queda a cargo de la institución o empresa tomar las decisiones pertinentes.

De acuerdo a lo anterior, destacan aspectos tales como:

- La objetividad de la auditoría.
- La independencia con el área auditada.
- La obtención de información.
- El uso de una metodología adecuada.
- El análisis de la información.
- Detección de las áreas de oportunidad.

En todo caso es una función que se acomete a *posteriori*, en relación con actividades ya realizadas, sobre las que hay que emitir una opinión.

La auditoría contiene elementos de análisis, de verificación y de exposición de debilidades y disfunciones. Aunque pueden aparecer sugerencias y planes de acción para eliminar las disfunciones y debilidades antedichas; estas sugerencias son plasmadas en un informe final, reciben el nombre de "Recomendaciones", este informe es realizado por el auditor, en él se plasman los antecedentes de la información (oficios de solicitud de información, oficios de entrega de documentación, atentas notas solicitud o entrega de información, etc.), el análisis de la información, las observaciones detectadas, las recomendaciones correctivas y/o preventivas y por último la firma de conformidad tanto del auditado como del auditor.

El auditor sólo puede emitir un criterio global o parcial basado en el análisis de la información y la observación, careciendo de facultades para modificar la situación en la institución o empresa analizada por él mismo.

Además del análisis de la documentación, otra herramienta aplicable al auditado son los cuestionarios, llamados Check List, ya que estos complementan la documentación entregada por el área auditada, en ellos se reflejan el grado de conocimientos que tiene el personal referente a políticas, lineamientos o procedimientos empleados en la misma.

I.3. AUDITORÍA INTERNA Y AUDITORÍA EXTERNA

La auditoría puede desarrollarse de dos formas:

- Auditoría interna.
- Auditoría externa.

La auditoría **interna** es la realizada con recursos materiales y personas que pertenecen a la empresa auditada. Este se realiza por expresa decisión de la empresa a fin de detectar debilidades y realizar las medidas correctivas y preventivas necesarias.

La auditoría informática interna cuenta con algunas ventajas adicionales respecto de la auditoría externa tales como:

- Son perceptibles al conocer mejor los procedimientos y políticas internas detectando las áreas de oportunidad.
- Conocen aquellos puntos vulnerables del área.
- Se realizan periódicamente revisiones globales como parte de su plan de trabajo.
- Se fomentan y se habitúan a las auditorías, especialmente cuando son sujetos a una auditoría externa.
- Se realizan propuestas de sugerencias a fin de ayudar a solventar las irregularidades detectadas.

Sin embargo existen ciertas desventajas de la realización de auditorías internas como:

- Pueden carecer de objetividad, ya que al estar involucrados o formar parte del área existe cierta tolerancia sobre algunos errores detectados.
- Esta propensa a no detectar áreas de oportunidad, ya que al estar inmerso en los procedimientos cotidianos no sé puede saber si estos están siendo aplicados de manera adecuada.
- Las recomendaciones no suelen ser tomadas y realizadas con seriedad y prontitud, ya que en la mayoría de las ocasiones no existe una autoridad que exija el cumplimientos de las mismas.

Por otro lado, la auditoría **externa** es realizada por personas ajenas a la empresa auditada. Se presupone una mayor objetividad que en la auditoría externa, debido al mayor distanciamiento entre auditores y auditados.

Las ventajas de la realización de una auditoría externa son:

- Mayor objetividad. Al no estar involucrados con las áreas auditadas existe una mayor imparcialidad.
- Se tiene el control de las actividades de investigación y desarrollo.
- Necesidad de auditar una materia de especialización, para la cual los servicios propios no están suficientemente capacitados.
- Confrontar algún Informe interno con el que resulte del externo, en donde se puede detectar si existen diferencias considerables de los resultados obtenidos.
- Obtener elementos de juicio fundamentados en la naturaleza de los hechos examinados.
- Aunque la auditoría interna sea independiente, sigue siendo la misma empresa, por lo tanto, es necesario que se le realicen auditorías externas para tener una visión desde afuera de la empresa.

En cuanto a empresas o instituciones se refiere, por lo general solamente las más grandes pueden poseer una auditoría propia y permanente, mientras que el resto acuden a las auditorías externas.

Finalmente, la propia auditoría requiere de su propio grupo de control interno, con implantación física en su estructura, puesto que si se ubicase dentro de la estructura Informática ya no sería independiente. Hoy en día, ya existen varias organizaciones Informáticas dentro de la misma empresa, y con diversos grados de autonomía, que son coordinadas por órganos corporativos de sistemas de información de las empresas.

La auditoría, tanto externa como interna, debe ser una actividad exenta de cualquier contenido o matiz "político" ajeno a la propia estrategia y política general de la empresa.

Asimismo, la función auditora puede actuar por iniciativa del propio órgano, o a instancias de parte, esto es, por encargo de la dirección o cliente.

I.4. CLASES DE AUDITORÍA

La auditoría es tan extensa por su concepto, que puede ser aplicable en muchas áreas, sin embargo, a continuación se detallan las más comunes.

Entre los principales enfoques de Auditoría tenemos los siguientes:

Administrativa:	Analiza: • Logros de los objetivos y metas cumplidas de la Administración de una empresa. • Desempeño de funciones administrativas.
Calidad:	• Analiza y evalúa métodos, mediciones y controles de los bienes y servicios.
Financiera:	• Autenticidad de los datos de estados financieros. • Integridad en los balances, cuenta de pérdida y ganancia. • Preparación de informes a principios contables.
Fiscal:	• Vigila el cumplimiento de las leyes fiscales.
Informática:	*Función informática:* • *Organización en el área informática, los sistemas de información, controles sobre el equipo informático e instalaciones físicas.* • *La seguridad, confidencialidad e integridad de la información y la optimización de recursos.* • *Cumplimento de lineamientos en materia informática.*
Operacional:	• Evalúa la eficiencia y eficacia de los procedimientos de la empresa. • Estrategia de los métodos que rigen un proceso de una empresa.

I.5. TÉCNICAS Y PROCEDIMIENTOS DE LA AUDITORÍA

El elemento básico de la auditoría, se fundamenta y se soporta por medio de procedimientos y/o técnicas específicos destinados a proporcionar una seguridad lógica de los resultados a los que se llega.

Cada una de las clases de auditoría cuenta con sus propios métodos para cumplir con objetivos que permitan alcanzar las metas propuestas. El alcance de la auditoría, se da por una buena planeación y la metodología que se aplique, esto dependerá de que tan detallada o específica sea.

Los puntos importantes con los que debe contar la realización de la auditoría son:

- Determinar si la auditoría será de forma integral o específica, determinando los alcances de la misma.
- Realizar cronogramas de actividades, que permitan evaluar el avance en tiempo y forma de la auditoría.
- Fijar objetivos y metas y por supuesto el cumplimiento de los mismos
- Contar con la evidencia documental debidamente integrada.

Sin embargo la planeación de actividades y la aplicación de metodologías, no solo compete a las auditorías, sino que es aplicable en cualquier ámbito laborar, ya que de ello dependerá en buena medida el éxito de la misma.

I.6. AUDITORÍA INFORMÁTICA

Como ya se mencionó existen muchos tipos de auditoría, pero sin duda la auditoría informática es una de las más importantes, ya que hoy en día el elemento informático está presente en cualquier ámbito de nuestra sociedad.

La auditoría informática realiza la revisión de controles y procedimientos de todo lo que se refiere a la tecnología de información, pasando por la organización, los sistemas de información, los controles sobre equipos de cómputo hasta las instalaciones físicas (la estructura del cableado de red, las condiciones del SITE[1], etc).

Los principales objetivos de la auditoría Informática son:

- Llevar el control de la función informática.
- Analizar la eficiencia de los Sistemas Informáticos utilizados en la institución y/o empresa.
- Verificar el cumplimiento de la Normativa general de la empresa en este ámbito (políticas internas).
- Revisar gestión adecuada de los recursos humanos, materiales y financieros.

El auditor informático vigila la adecuada aplicación de los recursos informáticos que la empresa posee de acuerdo a los lineamientos y políticas establecidas por la misma.

Claro está, que para la realización de una auditoría informática eficaz, se debe entender a la empresa en su más amplio sentido llámese hospitales, universidades, empresa privadas, el sector público; la gran mayoría utilizan la informática para gestionar sus "negocios" de

[1] Se denomina SITE al lugar donde se concentran los servidores, ruteadores, racks y todo el equipo de cómputo que suministra servicios informáticos a una institución o empresa.

forma rápida y eficiente con el fin de obtener beneficios económicos. Es por eso, que es sumamente importante conocer primero los procedimientos de la empresa auditada, saber cuales son sus objetivos y la función que realiza ya que eso dará la pauta para conocer si los lineamientos empleados por la empresa son los adecuados de acuerdo a la función gestionada.

Los sistemas de información son parte modular de una empresa, ya que ellos gestionan el empleo de recursos financieros, la actividad comercial y de ventas, el control de los recursos económicos, materiales y humanos, entre otras cosas.
Los sistemas de información están sometidos al control correspondiente. La necesidad de auditar a los Sistemas de Información (SI) se da por los siguientes aspectos:

- Establece y vigila que se lleven a cabo los controles de procesamiento de información, evitando así la pérdida o fuga de la misma.
- Vigila la integridad de la información. Si la información carece de este elemento los resultados que arrojen serán erróneos.
- Un SI mal diseñado puede convertirse en un dolor de cabeza de una empresa, ya que al no estar atendiendo a las necesidades puede causarle grandes pérdidas económicas.
- Lleva un control sobre las transacciones realizadas y detecta el inadecuado uso de la información.

Por otra parte, el alcance se define de acuerdo a los rubros en que se van a revisar durante la auditoría informática, se complementa con los objetivos de ésta, esto también depende de los recursos con los que cuente la empresa.

El alcance figura expresamente en el informe final, de modo que quede perfectamente determinado los puntos que han sido abarcados así como la justificación de los puntos que hayan sido omitidos.

I.6.1. CARACTERÍSTICAS DE LA AUDITORÍA INFORMÁTICA

La auditoría informática se divide principalmente en 5 rubros principales:

1. Planeación.
2. Organización.
3. Desarrollo y mantenimiento de sistemas.
4. Infraestructura del equipo de cómputo.
5. Esquema de seguridad (planes de contingencia y plan de respaldo de la información.)

1. Planeación. Se revisa que el área auditada cuente con un plan de trabajo detallado y que haya desarrollado su Programa Institucional de Desarrollo Informático (PIDI).

2. Organización. En ella se verifican los cambios estructurales del área de Informática, los manuales de organización y procedimientos, el grado de conocimiento de la estructura orgánica y los programas de capacitación efectuados por la empresa.

3. Desarrollo y mantenimiento de sistemas. Se verifica la documentación generada por los SI, el flujo de los datos, el inventario de los sistemas en desarrollo y producción, la metodología empleada para el desarrollo de los sistemas, las fases del ciclo de vida de los sistemas, el esquema de seguridad (claves de acceso).

4. Infraestructura del equipo de cómputo. Se verifica el control que permita identificar su asignación por área, salvaguarda y registro de acuerdo a las políticas y normas vigentes. Así mismo, se verifica la infraestructura de la red interna de trabajo (el cumplimiento del contrato de instalación de los nodos, el cableado, etc.), la fecha de inicio de operación y los términos con los que fueron entregados al área.

5. Esquema de seguridad. Se verifica que el "SITE" de servidores cuente con las medidas de seguridad físicas y lógicas que contribuyan a la integridad del personal y de los SI, de igual manera se evaluará el grado de conocimiento del personal referente a la normatividad implantada para tales efectos.

I.6.2. OBJETIVOS FUNDAMENTALES DE LA AUDITORÍA INFORMÁTICA

Dentro de los objetivos fundamentales de la informática destacan:

- Llevar un control referente al uso y manejo de software y hardware.
- Llevar un control del uso de licencias del software utilizado.
- Detectar errores o inconsistencias en los Sistemas de Información (SI).
- Llevar un control de calidad en los SI en los métodos de desarrollo.
- Documentar el ciclo de vida de un SI.
- Llevar una bitácora de cambios o versiones realizadas a los SI.
- Contar con políticas para la salvaguarda de los bienes informáticos

Uso y manejo de hardware y software. La revisión deberá verificar el uso adecuado de equipo de cómputo, así como del software que se encuentra instalado en él. Asimismo, se revisará que exista un inventario tanto de software como de hardware para llevar un control adecuado de recursos informáticos.

Control de licencias. Se verificará que exista un listado o control del uso de licencias de software y que estas coincidan con las instaladas en los equipos de cómputo. Esto se verifica realizado el levantamiento físico de programas que se encuentran instalados en los equipos, comúnmente la revisión de software se realiza cada 6 meses.

Inconsistencias en los Sistemas de Información. Se solicitará al área auditada el flujo de datos (DFD) y los diagrama de transición de estados (DTE) de los procesos que intervienen en los Sistemas de Información (SI), y se verificará mediante la observación que estos sean los descritos en la documentación técnica.

Control de calidad en los Sistemas de Información. Se verificará los procedimientos que hayan sido susceptibles de automatización, ya que estos deberán verse reflejados en los SI en producción (despliegue de pantallas, cuadros de ayuda, selección de catálogos, etc).

Documentación del ciclo de vida del Sistema de Información. Se verificará que se encuentre documentado el desarrollo de los SI, desde los requerimientos de los usuarios hasta las pruebas de los usuarios finales y su puesta en producción.

Bitácora de cambios de los Sistemas de Información. Se verificará que exista una bitácora de cambios realizados a los SI, así como las versiones realizadas, esto con el objetivo de llevar un antecedente de las modificaciones realizadas.

Políticas para la salvaguarda de los bienes informáticos. Se revisará que el área auditada cuente con políticas referentes a que hacer en caso de contingencia (comúnmente llamados "planes de contingencia") y que éstas sean conocidas y llevadas a cabo por la empresa.

I.6.3. PERFILES PROFESIONALES DE LOS AUDITORES DE SISTEMAS DE INFORMACIÓN

Dentro de los estándares profesionales para llevar a cabo una auditoría de sistemas, el perfil profesional con el que debe contar un auditor de sistemas de acuerdo a ISACF (*Information System Audit and Control Foundation: Fundación de Auditoria y Control de Sistemas de Información)*, es:

1. **ACTITUD Y APARIENCIA.** En todos los asuntos relacionados con auditoría, el auditor de sistemas de información debe ser independiente en actitud y apariencia al auditado.

2. **RELACIÓN ORGANIZACIONAL.** La función de auditoría de sistemas de información debe ser suficientemente independiente del área auditada para permitir un resultado objetivo de la auditoría.

3. **CÓDIGO DE ÉTICA PROFESIONAL.** El auditor de sistemas de información deberá adherirse al Código Profesional de Ética de la ISACF.

4. **HABILIDADES Y CONOCIMIENTOS.** El auditor de sistemas de información debe ser técnicamente competente y poseer las habilidades y el conocimiento necesario en el desempeño del trabajo de auditoría.

5. **PREPARACIÓN PROFESIONAL CONTÍNUA.** El auditor de sistemas de información para mantener competencia técnica deberá adquirir continuamente educación profesional apropiada.

6. **PLANEACIÓN Y SUPERVISIÓN.** Las auditorías de sistemas de información deben ser planeadas y supervisadas continuamente para proveer la seguridad de que los objetivos planteados se están logrando y cumpliendo de acuerdo a los estándares conocidos.

7. **EL REQUISITO DE EVIDENCIA.** Durante el curso de la auditoría, el auditor de sistemas de información deberá obtener evidencia suficiente y competente para soportar las observaciones y conclusiones reportadas en el informe.

8. **DEBIDO CUIDADO PROFESIONAL.** El debido cuidado profesional, deberá ser ejercido en todos los aspectos del trabajo del auditor de Sistemas de Información, incluyendo las observaciones aplicables a los estándares de auditoría.

9. **INFORMAR EL ALCANCE DE LA AUDITORÍA.** En informes preparados, el auditor de sistemas de información deberá plantear los objetivos de la auditoría, el período de cobertura, la naturaleza y extensión del trabajo de auditoría desempeñado.

10. **INFORMAR OBSERVACIONES Y CONCLUSIONES.** En informes preparados, el auditor de sistemas de información deberá plantear observaciones y conclusiones concernientes al trabajo de auditoría desempeñado y cualquier salvedad o calificación que tenga respecto a la auditoría.

I.6.4. NECESIDAD DE UNA AUDITORÍA INFORMÁTICA

Las empresas acuden a las auditorías externas cuando existen síntomas perceptibles de debilidad o simplemente para conocer el grado de mejoramiento de la empresa. Estos síntomas pueden agruparse en clases:

- Falta de coordinación y organización en la empresa:
  - Los estándares de productividad difieren sensiblemente de los promedios conseguidos habitualmente.
  - Reestructuración fallida de alguna área o en la modificación de alguna política importante.
  - Duplicidad de funciones.

- Mala imagen e insatisfacción de los usuarios:
  - No se atienden las peticiones de cambios de los usuarios. Ejemplos: cambios de software en las terminales de usuario, refrescamiento de paneles, variación de los archivos que deben ponerse diariamente a su disposición, etc.

- No se atienden las solicitudes de los usuarios en materia de Hardware (falla en los equipos-CPU, monitores, impresoras, etc.,-) ni se resuelven incidencias en plazos razonables. El usuario percibe que está abandonado y desatendido permanentemente.
- No se cumplen en todos los casos los plazos de entrega de resultados periódicos. Pequeñas desviaciones pueden causar importantes desajustes en la actividad del usuario, en especial en los resultados de aplicaciones críticas y sensibles.

➢ Debilidades económico-financiero:
- Incremento desmesurado de costos.
- Justificación de inversiones informáticas (la empresa no está absolutamente convencida de tal necesidad y decide contrastar opiniones).
- Desviaciones presupuestarias significativas.
- Costos y plazos de nuevos proyectos (deben auditarse simultáneamente a desarrollo de proyectos y al órgano que realizó la petición).

➢ Evaluación de nivel de riesgos
- Seguridad Lógica.
- Seguridad Física.
- Confidencialidad.

1.7. CONCLUSIONES

La auditoría es la revisión del cumplimiento de controles o políticas que ayudan a detectar errores en la empresa que en la mayoría de las ocasiones representan pérdidas de recursos humanos, económicos, y materiales.

La importancia de la Auditoría en todos los ámbitos es establecer y vigilar que se cumplan los controles que coadyuvan al procesamiento completo de la información. Es por eso que la auditoría no es limitante de una área, sino por el contrario, es aplicable a toda aquella área que desee medir el rendimiento de sus procedimientos y si estos han sido los adecuados de acuerdo a las funciones específicas de la empresa.

La función auditora es absolutamente objetiva; observa, analiza y emite un diagnóstico en donde expone las debilidades, disfunciones y áreas de oportunidad con el firme propósito de sugerir planes de acción para eliminar debilidades y disfunciones antes dichas.

Es por eso, que actualmente la Auditoría es una necesidad que debe aplicarse en cualquier empresa si se desea un mejoramiento continuo.

Es importante conocer los orígenes de la auditoría en general, ya que como hemos visto, no sólo compete al área financiera, ya que ésta puede ser empleada en cualquier ámbito de nuestra vida diaria. La auditoría como tal es una medición que se emplea para conocer que tan adecuados son los procedimientos que empleamos en nuestra empresa y detectar aquellas inconsistencias que están ahí, pero que muchas veces no logramos ver o no

queremos ver y que al paso del tiempo se convierten en errores graves que afectan de manera significativa el crecimiento de la empresa.

En el siguiente capítulo, nos enfocaremos a la "auditoría de sistemas", en donde se detallará los elementos que deben ser considerados para evaluar la vida en desarrollo y producción de un sistema de información.

Capítulo II

Auditoría de Sistemas

II. AUDITORÍA DE SISTEMAS

OBJETIVOS

- CONOCER LAS METODOLOGÍAS EXISTENTES PARA AUDITAR LOS SISTEMAS DE INFORMACIÓN.
- CONOCER LA METODOLOGÍA EMPLEADA EN LA CONTRALORÍA INTERNA EN LA SHCP.
- CONOCER LOS PUNTOS AUDITABLES EN UN SISTEMA DE INFORMACIÓN.

El avance de la tecnología lleva a una serie de cuestiones que involucran la planificación del resguardo y cuidado de la información, ya que es considerada uno de los activos más importantes de cualquier organización.

La auditoría de sistemas implica emitir una opinión profesional sobre el correcto funcionamiento de la infraestructura informática (hardware, software e instalaciones), misma que implica analizar aspectos, cuya revisión requiere profesionales con formación en sistemas

La Auditoría de Sistemas de Información está definida como cualquier auditoría que abarca la revisión y evaluación de todos los aspectos (ó la mayoría de ellos) de los sistemas automatizados de procesamiento de información, incluyendo procedimientos relacionados no automáticos, y las interfaces entre ellos.

La Auditoría de Sistema analiza y verifica que los Sistemas de Información (SI) tanto en desarrollo y producción cumplan con los aspectos mínimos del ciclo de vida de un sistema, que además cuenten con una metodología conocida y plenamente sustentada y que cumpla por supuesto con las necesidades del usuario, ya que esta es una de las principales razones por la que fueron creados.

II.1 DEFINICIÓN DE AUDITORÍA DE SISTEMAS

La Auditoría de Sistemas es:

- La verificación de controles en el procesamiento de la información, desarrollo de sistemas e instalación con el objetivo de evaluar su efectividad y presentar recomendaciones a la empresa.
- La actividad dirigida a verificar y juzgar información.
- 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.

II.2 METODOLOGÍAS DE AUDITORÍA DE SISTEMAS

El uso de metodologías es necesario para conseguir resultados homogéneos en equipos de trabajo, asimismo es útil para desarrollar cualquier proyecto que se plantee de manera ordenada y eficaz.

Existen dos familias en las que se agrupan las metodologías desarrolladas y utilizadas en la auditoría y el control informático, estas son:

- **Cuantitativas**. Basadas en un modelo matemático numérico como por ejemplo los datos de probabilidad de ocurrencia de un evento que se debe extraer de un registro de incidencias.
- **Cualitativas**. Basadas en el criterio y experiencia acumulada del auditor. Éstas dependen de la habilidad y calidad del profesional involucrado.

Dentro de las metodologías más comunes de auditoría de sistemas están las de Análisis de riesgos, las de Plan de Contingencias y la Metodología de COBIT

II.2.1 METODOLOGÍA DE ANÁLISIS DE RIESGO

Esta metodología se ocupa de identificar la ausencia de controles internos, políticas de actuación y contramedidas en caso que se suscite alguna contingencia. Las etapas que la conforman se presentan a continuación:

Etapa 1. Cuestionario

Etapa 2. Identificar los riesgos

Etapa 3. Calcular el impacto

Etapa 4. Identificar las contramedidas y costo

Etapa 5. Pruebas y simulaciones

Etapa 6. Elaboración de los informes

Durante la **etapa 1**, se identifican las vulnerabilidades y riesgos. Los cuestionarios deben ser objetivos en cuanto a establecer criterios medibles de respuesta y deben ser enfocados de acuerdo al área auditada (desarrollo, soporte técnico, etc.).

Durante la **etapa 2**, basándose en los resultados obtenidos de los cuestionarios, se identifican los riesgos o puntos vulnerables de la organización.

Durante la **etapa 3**, se analiza el impacto que propician éstos riesgos y en que medida a corto o largo plazo afectan a la organización.

Durante la **etapa 4**, se identifican las contramedidas y el costo que propiciará llevarlas a cabo.

Durante la **etapa 5**, se realiza las simulaciones o pruebas piloto con el objeto de observar si han disminuido los riesgos dentro de la organización.

Durante la **etapa 6**, se plasman los resultados de estas pruebas eligiendo así un plan de seguridad.

II.2.2. METODOLOGÍA DE PLAN DE CONTINGENCIA

Esta metodología se enfoca principalmente a verificar los recursos y procedimientos de actuación con que cuenta la institución en caso de presentarse caídas de sistemas, pérdida de información, etc.; es decir eventos que suceden dentro del centro de procesamientos de datos. Su objetivo es conseguir una pronta restauración de servicios afectados por una paralización total o parcial en la institución.

Cabe señalar que el concepto fundamental es "la continuidad en el servicio"; estudiar todo lo que puede paralizar la actividad operativa y producir pérdidas. Las fases de este plan se mencionan a continuación:

Fase I. Análisis y diseño

Fase II. Desarrollo del plan

Fase III. Pruebas y mantenimiento
- Herramientas

Fase I. Análisis y Diseño

Se estudia la problemática, las necesidades de recursos, las alternativas de respaldo y se analiza el costo/beneficio de las mismas.

Existe un factor a determinar en esta fase "Time Frame" o el tiempo que la empresa puede asumir con la paralización de la actividad operativa antes de incurrir en pérdidas significativas.

Fase II. Desarrollo del Plan

En esta fase se desarrolla la estrategia seleccionada implantándose todas las acciones previstas. Se desarrollan las acciones de emergencia y los procedimientos de actuación generando así el plan de contingencia ("que hacer en caso de").

Fase III. Pruebas y Mantenimiento

Se definen las pruebas, las características, ciclos y la puesta en marcha de todo el trabajo realizado, así como la capacitación del personal involucrado.

De igual manera, se define la estrategia de mantenimiento, el personal encargado, la normativa y los procedimientos necesarios para llevarlo a cabo.

- **Herramientas**

Dentro de la fase de pruebas y mantenimiento, las herramientas son el valor agregado. En la mayoría de las metodologías, lo más importante es contar con una metodología apropiada para desarrollar más adelante la herramienta que se necesite. El esquema de una herramienta, debe contener al menos:

- Base de datos relacional
- Módulo de entrada de datos
- Módulo de consultas
- Proceso de textos
- Generador de informes
- Ayuda en línea
- Hoja de cálculo
- Gestor de Proyectos
- Generador de gráficos.

II.2.3. METODOLOGÍA DE COBIT

COBIT significa: Objetivos de Control para la Información y Tecnologías Relacionadas (Control Objetives for Information and Related Technology). Esta estructura ha sido desarrollada como un estándar generalmente aplicable y aceptado para la práctica del control de la tecnología informática.

II.2.3.1. EL MODELO DE CONTROL

El concepto que sostiene la estructura COBIT es el control en Tecnología Informática enfocado hacia la información que se necesita en los procesos del negocio y hacia la información resultante de la aplicación combinada de recursos relacionados con Tecnología Informática, que requieren ser administrados mediante procesos de Tecnología Informática.

II.2.3.2. ESTRUCTURA

La estructura del modelo COBIT esta formada por:

- RECURSOS DE TECNOLOGÍA INFORMÁTICA
- DOMINIOS
- CRITERIOS DE INFORMACIÓN

RECURSOS DE TECNOLOGÍA INFORMÁTICA

Los recursos de Tecnología Informática son:

Datos: Objetos en su más amplio sentido, (externos e internos), estructurados y no estructurados, gráficos, sonido, etc.

Sistemas de Aplicación: Se entiende como sistemas de aplicación la suma de procedimientos programados y manuales.

Tecnología: La tecnología cubre el hardware, los sistemas operativos, los sistemas de administración de bases de datos, las redes, etc.

Instalaciones: Recursos para albergar y soportar los sistemas de información.

Recursos humanos: Habilidades del personal, concientización y productividad para planear, organizar, adquirir, entregar, soportar y monitorear sistemas de información y servicios.

DOMINIOS

Son procesos los que a su vez se componen de actividades. Los Dominios se clasifican de la siguiente forma:

Planeación y Organización: Este Dominio cubre la estrategia y las tácticas y le concierne la identificación de la forma en que la tecnología informática puede contribuir mejor al logro de los objetivos del negocio. Más aún, la realización de la visión estratégica necesita planearse, comunicarse y administrarse desde diferentes perspectivas. Finalmente, debe instalarse una organización apropiada así como una infraestructura tecnológica.

Adquisición e Implementación: Para comprender la estrategia de Tecnología Informática, las soluciones de Tecnología Informática necesitan ser identificadas, desarrolladas o adquiridas así como implementadas e integradas en el proceso del negocio. Además, se cubren en este Dominio los cambios y el mantenimiento de los sistemas existentes.

Entrega y Soporte: A este Dominio le concierne la entrega real de los servicios requeridos, que cubre desde las operaciones tradicionales sobre aspectos de seguridad y continuidad hasta el entrenamiento. Para brindar servicios deben instalarse los procesos de soporte necesarios. Este Dominio incluye el procesamiento real de los datos por los sistemas de aplicación, a menudo clasificados como controles de las aplicaciones.

Monitoreo: Todos los procesos de Tecnología Informática necesitan ser evaluados regularmente en el tiempo en su calidad y cumplimiento con los requerimientos de control.

CRITERIOS DE INFORMACIÓN

Comenzando el análisis desde los requerimientos amplios de Calidad, Financieros y Seguridad, se extrajeron siete categorías distintas:

1. **Efectividad**: trata con información relevante y pertinente al proceso de negocios, así como entregada de una manera oportuna, correcta, consistente y útil.
2. **Eficiencia**: concierne a la provisión de información mediante el uso óptimo (más productivo y económico) de los recursos.
3. **Confidencialidad**: concierne a la protección de la información sensible respecto de la disposición no autorizada.
4. **Integridad**: se relaciona con la precisión de la información así como con su validez de acuerdo con los valores y expectativas del negocio.
5. **Disponibilidad**: se refiere a que la información esté disponible cuando sea requerida por el proceso del negocio, ahora y en el futuro. También concierne a la salvaguarda de los recursos necesarios y las capacidades asociadas.
6. **Cumplimiento**: trata con el cumplimiento de aquellas leyes, regulaciones y arreglos contractuales a los cuales está sujeto el proceso del negocio, ej: criterios del negocio impuestos desde el exterior.
7. **Confiabilidad de la Información**: se relaciona con la provisión de información apropiada a la gerencia para operar la entidad y también para ejercer sus responsabilidades de elaboración de informes financieros y de cumplimiento.

II.3. METODOLOGÍA EMPLEADA EN LA CONTRALORÍA INTERNA EN LA SHCP PARA AUDITAR SISTEMAS DE INFORMACIÓN

La metodología utilizada en la Contraloría Interna tiene como objetivo verificar que la organización del área informática, los sistemas de información y los controles sobre equipo informático e instalaciones físicas, atiendan las necesidades de las Unidades Administrativas de la SHCP (Secretaría de Hacienda y Crédito Público), conforme a lo estipulado en el Programa de Modernización de la Administración Pública (PROMAP) y en

el Programa Institucional de Desarrollo Informático (PIDI), así como a las disposiciones de racionalidad, austeridad y disciplina presupuestal[2].

II.3.1. DESARROLLO Y MANTENIMIENTO DE SISTEMAS

El auditor deberá conocer los sistemas informáticos con los que cuenta, en este caso, la Unidad Administrativa, por que deberá solicitar al área auditada aspectos como:

- Nombre del sistema o aplicación
- Plataforma de operación
- Base de Datos
- Lenguaje de desarrollo
- Objetivo

El auditor deberá solicitar al área auditada la metodología de desarrollo de nuevos sistemas y para el mantenimiento de los existentes que permita una administración adecuada de los mismos.

Se verificará que previamente al inicio de un sistema se lleve a cabo un estudio de requerimientos del mismo.

Se verificará la existencia de la documentación de todos los sistemas en producción, donde compruebe y detallen las fases, de acuerdo a lo estipulado en la metodología utilizada para el desarrollo de sistemas. Se verificaran aspectos como:

- Requerimientos por parte del usuario al área encargada del desarrollo del sistema.
- Deberá existir entrevistas y/o cuestionarios (documentación) que avale la realización de la etapa de análisis.
- Diagramas de entidad-relación, diagramas de flujo de datos, diccionario de datos, así como los programas fuentes.
- Documento formal que determine la liberación del sistema y la aceptación final por parte del usuario.
- Documentación que avale la capacitación de usuarios por parte del área de desarrollo del sistema.
- Control de versiones.
- Bitácora de control de cambios que haya sufrido el sistema.

Además el auditor deberá verificar la integración de manuales de usuario y técnico de los sistemas en producción.

Cabe mencionar que el auditor deberá verificar que cuando se utilicen sistemas desarrollados por proveedores, existan controles que eviten que el usuario pueda modificar el código fuente.

[2] Programa específico de revisión de sistemas de la Subdirección de Auditoría de Sistemas, enero 1999.

II.4. NORMATIVIDAD APLICABLE EN LA REALIZACIÓN DE AUDITORÍAS DE SISTEMAS EN LA SECRETARIA DE HACIENDA Y CRÉDITO PÚBLICO

Como resultado de las Auditorías de sistemas que practica la Contraloría Interna en la Secretaría de Hacienda y Crédito Público a las diversas Unidades Administrativas que la conforman, es factible que se identifiquen irregularidades que se encuentran establecidas en marcos jurídicos, por lo a continuación se señalan aquellos reglamentos y artículos normativos que se aplican en la auditoría de sistemas.

- **Manual de Organización de la Contraloría Interna en la Secretaría de hacienda y Crédito Público.**
  - Dirección de Auditoría a Sistemas y Servicios Informáticos
- **Reglamento Interior de la Secretaría de Contraloría y Desarrollo Administrativo.**
  - Capítulo VI de la Contraloría Interna
    - Artículo 27, Fracción IX. Comprobar y evaluar en forma selectiva que los sistemas de información.
- **Ley Federal de Derechos de Autor**
  - Capítulo I Reglas Generales Fracción XI, Programas de Cómputo.
  - Capítulo IV de los Programas de Computación y las Bases de Datos.
    - Artículo 101 al artículo 114.

II.5. ELEMENTOS AUDITABLES EN UN SISTEMA DE INFORMACIÓN

Los aspectos que deberán ser considerados por el auditor para evaluar si un Sistema de Información (SI) es confiable son:

Salvaguarda de bienes informáticos	Daños Destrucción Uso no autorizado Robo
Mantiene Integridad de los datos	Información Precisa Completa Oportuna Confiable

Alcanza metas de la Organización	Cumplimiento de requerimientos por parte de los usuarios. Logro de objetivos y metas cumplidas
Consume recursos eficientemente	Utiliza los recursos adecuadamente en el procesamiento de la información

Por otra parte, la auditoría de cada proyecto de desarrollo tendrá un plan distinto dependiendo del riesgo, la complejidad del mismo y los recursos disponibles para realizar la auditoría.

La aprobación del proyecto es un hecho previo al comienzo del mismo, mientras que la gestión se aplica a lo largo de su desarrollo. La planificación se realiza antes de iniciarse, pero sufrirá cambios a medida que el proyecto avanza en el tiempo.

Las técnicas a utilizar y los elementos a inspeccionar, normalmente los productos y los documentos generados en cada fase de desarrollo, serán los mismos en ambos casos. La única diferencia es que en el primer caso las conclusiones que vaya aportando el auditor pueden afectar al desarrollo del proyecto, aunque nunca participará en la toma de decisiones del mismo.

II.5.1. APROBACIÓN DEL PROYECTO

En esta fase, el auditor deberá revisar y evaluar la documentación referente al desarrollo de proyecto, ya que éste debe estar definido y justificado plenamente, de manera que pueda ser aprobado formalmente. Debe contar con aspectos como:

- Realizar y documentar el estudio de viabilidad tomando en cuenta los recursos humanos, económicos y materiales.
- Documentar y hacer formal la aprobación del desarrollo del proyecto, defiendo objetivos, metas y tiempos de avances.
- Identificar a las áreas participantes y realizar un compromiso de trabajo conjunto con el área de desarrollo, es decir, el área involucrada debe dar las facilidades necesarias a fin de exponer las tareas susceptibles de automatización, explicar de manera clara y precisa el flujo de la información.

Asimismo, se deberá contar con un líder de proyecto, el cual es el responsable de verificar que se cumplan en tiempo y forma con las metas propuestas.

Basándose en las características del proyecto, el auditor deberá revisar y analizar la metodología aplicada al mismo tomando aspectos como:

- Verificar que existan requerimientos de los usuarios por escrito (minutas).
- Verificar los alcances del proyecto y el grado de cumplimiento.
- Verificar si existe un plan de trabajo, el cual deberá contar con las metas y el personal asignado en cada actividad.
- Evaluar los riesgos asociados al proyecto, particularmente si se van emplear nuevas tecnologías.
- Verificar los recursos con los que se cuenta.
- Verificar el tiempo de desarrollo, el compromiso de entrega del proyecto, y los resultados .
- Verificar (si que existe) información histórica con la que se cuente.
- Verificar la existencia del prototipo del proyecto.

El auditor deberá verificar que el área auditada cuente con el equipo técnico que realizará el proyecto tomando en cuenta lo siguiente:

- Los perfiles profesionales adecuados para el desarrollo del proyecto.
- Personal de otras áreas que han solicitado el desarrollo del proyecto que conozcan plenamente el flujo de información que deberá llevar éste.
- Integrar grupos de trabajo para el análisis y elaboración del modelo del proyecto.

El auditor deberá solicitar documentación y/o información comprobatoria referente a los responsables de las áreas involucradas en el proyecto que deben participar en la gestión del mismo, considerando lo siguiente:

- Integración formal de un grupo de trabajo o comité en el que están incluidos los responsables de todas las unidades afectadas.
- Se deberá llevar a cabo reuniones periódicas entre el comité y el área de desarrollo a fin de conocer los avances del proyecto y su caso modificar el plan de trabajo de proyecto con base a los resultados de las revisiones.
- Establecer el día de las reuniones (pueden ser semanales) y realizar minutas de las reuniones, a manera de que se encuentren documentados los acuerdos a los que se llegaron.
- Realizar pruebas parciales de los avances del proyecto.

Una vez que se haya completado la etapa de *Aprobación del Proyecto*, el auditor deberá solicitar y evaluar la *Metodología Aplicada para el Desarrollo de Sistema* y verificar que el área auditada haya cumplido con cada una de sus etapas.

Se debe comprobar que:

- Cada etapa debe estar plenamente documentada antes de comenzar una nueva. Esta deberá ser revisada y aceptada, especialmente en las fases de análisis y diseño.
- La documentación deberá seguir un estándar establecido en el área (formato).
- Ejecución de pruebas con los responsables de las áreas afectadas.

Una vez concluido el proyecto se debe concentrar toda la documentación del mismo y liberar los recursos empleados. Se debe verificar que:

- La documentación del proyecto este completa.
- Se de por concluido formalmente la liberación del proyecto.
- Se realice la entrega formal del manual de usuario y la memoria técnica del proyecto.
- Se incorporé al inventario de aplicaciones existentes del nuevo proyecto.

II.6. AUDITORÍA A BASES DE DATOS

La importancia de la auditoría del entorno de bases de datos (BD) radica en que es el punto de partida para poder realizar la auditoría de las aplicaciones que utilizan esta tecnología.

Para poder realizar una auditoría a las BD de los SI se deberá conocer los elementos que conforman una BD.

Definición de una Base de datos

Una base de datos es un conjunto o depósito de datos almacenados que se encuentran lógicamente relacionados entre sí, para ser manipulados simultaneamente por varios usuarios de forma selectiva y en tiempo oportuno.

II.6.1. SISTEMA DE GESTIÓN DE BASES DE DATOS (SGBD)

Se define al Sistema de Gestión de Base de Datos[3] "como un conjunto coordinado de programas, procedimientos, lenguajes, etc., que suministra a los distintos tipos de usuarios los medios necesarios para describir y manipular los datos almacenados en la base, garantizando su seguridad".

Durante la auditoría se deberán revisar el manejador de base de datos que utiliza la organización, las utilerias, funciones y/o precedimientos con los que cuenta dicho manejador. Así como cuales son las más utilizadas en la organización.

[3] Definición de acuerdo al libro "Auditoría Informática" de Mario Piattini

Se debe verificar la estructura de la base de datos, si se cuenta con procedimientos o políticas de operación y acceso al manejados de base de datos, para valorar si son suficientes o si deben ser mejorados.

Moeller (1989) establece cinco objetivos de control a la hora de revisar la distribución de datos:

1. El sistema de proceso distribuido debe tener una función de administración de datos centralizada que establezca estándares generales para la distribución de datos a través de las aplicaciones.
2. Deben establecerse unas funciones de administración de datos y de base de datos fuertes, para que puedan controlar la distribución de los datos.
3. Deben existir pistas de auditoría para todas las actividades realizadas por las aplicaciones contra sus propias bases de datos y otras compartidas.
4. Deben existir controles software para prevenir interferencias de actualización sobre las bases de datos en sistemas distribuidos.

Deben realizarse las consideraciones adecuadas de costos y beneficios en el diseño de entornos distribuidos.

II.6.2. METODOLOGÍAS PARA LA AUDITORÍA DE BASES DE DATOS

Existen diversas metodologías para la realización de auditorías a las bases de datos, ya que por la importancia de la información es conveniente verificar la integridad, confidencialidad, confiabilidad y seguridad de la misma. Estas pueden ser divididas en :

- Metodología tradicional
- Metodología de evaluación de riesgos

II.6.2.1. METODOLOGÍA TRADICIONAL

En este tipo de metodología se revisa la situación con la ayuda de una lista de control (Checklist), que consta de una serie de cuestiones a verificar.

Las preguntas formuladas deberán ser especificas a fin de obtener respuestas coherentes que permitan detectar los puntos débiles de la empresa.
Los checklist se clasifican en:

1. Checklist de rango : Contiene preguntas que el auditor debe puntuar dentro de un rango preestablecido (por ejemplo, de 1 a 5, siendo 1 la respuesta con el valor más bajo y el 5 el valor más alto).
2. Checklist Binaria: Es la constituida por preguntas con respuesta única y excluyente: Si o No.

Los Checklists de rango son adecuados si el equipo auditor no es muy grande y mantiene criterios uniformes y equivalentes en las valoraciones. Permiten una mayor precisión en la

evaluación que en los checklist binarios. En base a los resultados se pueden establecer puntos de medición que servirán de gran ayuda para el diagnóstico final.

Los Checklists Binarios deben estar contenidos en preguntas de gran precisión por ser respuestas cuyos valores se encuentran en intervalos tan específicos.
Este tipo de técnica suele ser aplicada a la auditoría de productos de bases de datos, especificándose en la lista de control todos los aspectos que deben ser considerados. Así, por ejemplo, si el auditor se enfrenta a un entorno Oracle 8, en la lista de control se recogerán los parámetros de instalación que más riesgos presentan, señalando cuál es su rango adecuado. De esta manera, si no cuenta con la asistencia de un experto en el producto, puede comporbar por lo menos los aspectos más importantes de su instalación.

II.6.2.2. METODOLOGÍA DE EVALUACIÓN DE RIESGOS

Conocida también por *risk oriented approach* , es la que propone la ISACA (Information Systems Audit and Control Association/Foundation), y determina los objetivos de control que minimizan los riesgos a los que está sometido el entorno. En Touriño y Fernández (1991) se señalan los riesgos más importantes que lleva consigo la utilización de una base de datos, la cual se muestra a continuación[4]:

- Incremento de la dependencia del servicio informático debido a la concentración de datos.

- Mayores posibilidades de acceso en la figura del administrador de la base de datos.

- Incompatibilidades entre sistemas de seguridad de acceso propios del SGBD(Sistema de Gestión de Base de Datos) y en general de la instalación.

- Mayor impacto de los errores en datos o programas que en los sistemas tradicionales.
- Ruptura de enlaces o cadenas por fallos del sofware o de los programas de aplicación.

- Mayor impacto de accesos no autirizados al diccionario de la base de datos que a un archivo tradicional.

Mayor dependencia del nivel de conocimientos técnicos del personal que realice tareas relacionadas con el software de base de datos (administrador, programadores, etc.)

Asimismo, dentro de la metodología de evaluación de riesgo se encuentran:

- **Objetivo de control.** El Sistema de Gestión de Bases de Datos (SGBD) deberá salvaguardar la confidencialidad de la información contenida en la base de datos.

- **Técnica de control.** Se deberán definir los perfiles y privilegios del usuario necesarios para controlar el acceso a la base de datos. Con el propósito de evitar que la información sea corrompida o se hago un mal uso de ella.

[4] Aspectos tomados en base al libro "Auditoría Informática, un enfoque práctico" de Mario G. Piattini y Emilio del Peso.

Una vez valorados los resultados de las pruebas se elaborará un diagnóstico en donde se describa la situación, el riesgo existente y la deficiencia a solucionar, y, en su caso, sugerirá la posible solución.

Como resultado de la auditoría, se presentará un informe final en el que se expongan las conclusiones más importantes a las que se ha llegado, así como el alcance que ha tenido la auditoría.

Para la realización de la auditoría de base de datos a la Dirección General del Destino de Bienes de Comercio Exterior Propiedad del Fisco Federal se utilizarón aspectos de ambas metologías. Los aspectos se listan a continuación:

- Aplicación de cuestionarios que incluyen checklist de rango y binarios, así como preguntas de respuestas abiertas.
- Documentación de su estructura lógica que especifiquen las restricciones de uso tales como insertar, modificar o borra un registro.
- Relación de las claves de usuarios en donde se encuentren plenamente establecidos los perfiles y privilegios de cada usuario.
- Documetación de su estructura global, es decir la descripción de todos los datos y relaciones entre éstos.

- Documentación referente a su estructura física, que establece la asignación de espacios de almacenamiento, la inclusión de índices o punteros, optimización de recursos, técnicas de encriptamiento y compresión de datos.

II.6.2.3. TÉCNICA DE CONTROL EN EL CICLO DE VIDA DE UNA BASE DE DATOS

Los objetivos y técnicas de control a tener en cuenta a lo largo del ciclo de vida de una base de datos (Ver figura II.a.) que abarca desde su estudio previo hasta su explotación, los tomaremos, basándonos en los propuestos por la ISACA, MENKUS (1990) y en los recientemente publicados COBIT, ISACF (1996).

Estudio Previo

En esta fase es importante elaborar un estudio de viabilidad en el cual se incluyan alternativas para lograr objetivo del proyecto.

Son pocas las organizaciones que desarrollan un estudio de viabildad, ya que no toman en cuenta riesgo que puede implicar no saber si el proyecto es rentable.

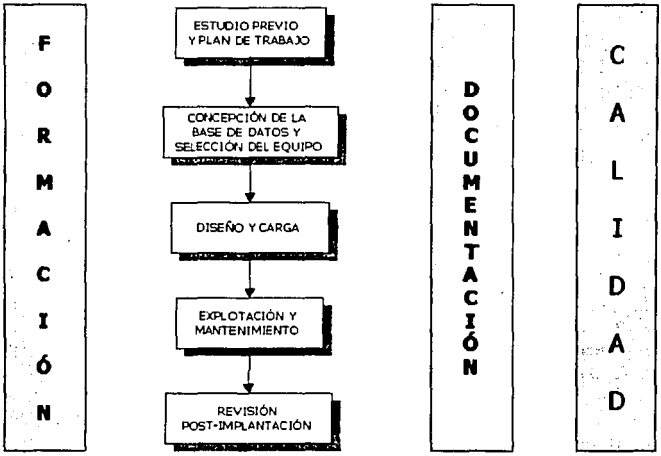


Fig. II.a. *Ciclo de vida de una base de datos*

Otro aspecto importante es definir el papel que desempeñará los responsables de la gestión y control de la base de datos. Se recomienda definir aspectos tales:

- El personal de desarrollo de sistemas y el de explotación.
- Explotación y control de datos.
- Administración de bases de datos y desarrollo.

Cuando se realiza una auditoría es común encontrar que las funciones de la organización no se encuentran definidas, ocasionando que haya tiempos muertos y duplicidad de funciones.

Concepción de la base de datos y selección del equipo

En esta fase se empieza a diseñar la estructura de la base de datos, por lo que deben tomarse en cuenta modelos y la técnicas previamente definidas, esto de acuerdo a la metodología de desarrollo de sistemas de la organización.

El auditor debe analizar, en primer lugar, la metodología de diseño propuesta por la organización y si esta cuenta con aspectos tales como:

- **Diseño conceptual**. Representación de los recursos de información de la organización.

- **Diseño lógico**. Realizar el esquema conceptual adoptandolo a el modelo de datos en el que se apoya el Sistema de Gestión de Bases de Datos (SGBD).

- **Diseño físico**. Desarrollar la instrumentación, lo más eficientemente posible del esquema lógico.

Diseño y Carga

En esta fase se llevarán a cabo los diseños lógicos y físicos de la base de datos, por lo que se verificará si la definición de los datos contempla además de su estructura, las relaciones y las restricciones oportunas, las especificaciones de almacenamiento de datos y las cuestiones relativas a la seguridad.

Se tomará en cuenta elementos como tablas, vistas, índices y se comprobará que su definición sea completa, que satisfaga las necesidades demandadas por los usuarios.

Una vez diseñada la BD, se procederá a su carga, ya sea migrando datos de un soporte magnético o introduciéndolos manualmente. Cabe señalar que la migración de datos así como el paso de un sistema de archivos a uno de bases de datos, o de un tipo de SGBD (de jerárquico a relacional), significa un riesgo muy importante, por lo que deberán estar claramente planificadas para evitar pérdida de información y la transmisión al nuevo sistema de datos erróneos.

Explotación y mantenimiento

Una vez realizadas las pruebas de aceptación, con la participación de los usuarios, el sistema se pondrá en explotación.

En esta fase, se debe comprobar que se establecen los procedimientos de explotación y mantenimiento que aseguren que los datos sean integros y que el contenido de los sistemas sólo se modifique mediante la autorización respectiva.

Revisión post-implantación

En esta etapa se deberá verificar si:

- Se han conseguido los resultados esperados
- Se satisfacen las necesidades de los usuarios
- Los costos y beneficios coinciden con los previstos.

Además, el se que revisará la documentación que se produzca a lo largo de todo el proceso, para verificar si son congruentes a los establecidos por la metodología adoptada en la organización.

II.7. SEGURIDAD EN DATOS

Hoy en día la seguridad de la información es primordial para cualquier organización y es importante verificar que no puededan tener acceso a ella personas no autorizadas.
La protección de los datos debe llevarse a cabo contra fallos físicos (servidores), fallos lógicos (de programación, queries) y fallos humanos.

Los aspectos a considerarse para la seguridad de los datos son:

1. **Confidencialidad.** Privacidad en los datos, la información no debe ser divulgada a usuarios no autorizados.
2. **Accesibildad.** La información debe estar disponible cuando se requiera de ella.
3. **Integridad.** Los datos no deben ser erroneos, deben ser confiables.

1. Confidencialidad.

El auditor deberá verificar que existan mecanismos de acceso controlado a los datos, es decir, autentificación de usuarios mediante claves y passwods. Por lo que el administrador de la BD deberá especificar los privilegios de los usuarios como:

1. La utilización de la BD.
2. Consulta de datos.
3. Modificación de los datos.
4. ejecución de procesos.

El mecanismo de control de acceso se encarga de administrar el acceso de los usuarios, con el propósito de mantener la integridad de los datos en caso de realizar operaciones de actualización.

Por otro lado es conveniente contar en todo sistema con la utlizacióin de pistas de auditoría, ya que nos ayudan a detectar accesos no permitidos o transaccciones realizadas por los usuarios.

2. Accesibilidad.

Consiste en dotar a los sistemas de bases de datos con los mecanismos necesarios para asegurar la disponibilidad de la información en caso de sucitarse fallos lógicos o físicos.

El auditor deberá verificar que el manejador de bases de datos cuente con mecanimos que ayudan a la recuperación de los datos, entre los cuales el más conocido es el archivo denominado LOG , en el cual se va guardando toda la información necesaria para *desahacer* en caso de fracasar o *rehacer* en caso de recuperar las transacciones.

3. Integridad

Consiste en salvaguardar la información de la base de datos contra sintanxis inadecuada, o inconsistencias en la captura. Por lo que el sistema deberá contener reglas de validación de datos a fin de evitar falta de integridad de la información.

Cuando hablamos de la función informática generalmente nos referimos a tecnología nueva, de nuevas aplicaciones, nuevos dispositivos hardware, nuevas formas de elaborar información más consistente, etc.

Para tener un sistema integral de seguridad el audior deberá verificar que el área auditada cuente con aspectos como:

- Políticas de seguridad
- Seguridad física contra catástrofes (incendios, terremotos, inundaciones, etc.)
- Prácticas de seguridad para el personal:
- Plan de emergencia (plan de evacuación, uso de recursos de emergencia como extinguidores.
- Elementos técnicos de procedimientos de seguridad para:
- Hardware y software
- Aplicación de los sistemas de seguridad incluyendo datos y archivos
- Planificación de programas de desastre y sus pruebas (simulación)
- Planificación de equipos de contingencia con carácter periódico
- Control de desechos de los nodos importantes del sistema:
- Política de destrucción de basura copias, fotocopias, etc.
- Consideración de las normas ISO 14000

Cabe señalar que a fin de elaborar un sistema de seguridad, se debe considerar:

- Sensibilizar a los mandos superiores de la organización en torno al tema de seguridad.
- Realizar un diagnóstico de la situación de riesgo y seguridad de la información en la organización a nivel software, hardware, recursos humanos, y ambientales.
- Elaborar un plan para un programa de seguridad.
- Elaborar un plan de contingencia.

II.8. PAPELES DE TRABAJO

En el argot de auditoría se conoce como papeles de trabajo la "Totalidad de los documentos preparados o recibidos por el auditor", de manera que, en conjunto, constituyen un compendio de la información utilizada y de las pruebas efectuadas en la ejecución de su trabajo, junto con las decisiones que ha debido tomar para llegar a formarse su opinión.

Durante toda la realización de la auditoría deberá mantener una buena organización de la documentación que se obtiene, asimismo deberá asegurarse de que esté debidamente certificada. En conformidad con los estándares emitidos por la ISACF (Information System Audit and Control Foundation: Fundación de Auditoría y Control de Sistemas de Información), particularmente el VII "El requisito de evidencia", IX "Informar el alcance de la auditoría", X "Informar observaciones y conclusiones", el Código de ética profesional y el apartado 420 "Examinar y evaluar información" de la IIA.

Deberá tener el área alguna normatividad que especifique de forma clara y sin ambigüedades la manera de integrar el legajo correspondiente, especificando de que forma serán las referencias a la documentación soporte de las observaciones. En la documentación, deberán ser observables las marcas de supervisión.

Consolidación del legajo de "Papeles de Trabajo", el cual deberá contener como mínima información lo siguiente:

1. **Antecedentes**
2. **Carta de Presentación**
3. **Cronograma**
4. **Actividades a desarrollar (Procedimientos de forma genérica)**
5. **Informe Final**
6. **Notas de Solicitud de información**
7. **Información proporcionada por el área (documental o en medio magnético)**
8. **Cédula de Observaciones**
9. **Evidencia documental**

ANTECEDENTES. Se refieren a la información de la empresa desde su formación física hasta su formación organica o funcional. Se mencionan únicamente los aspectos sobresalientes de la misma.

CARTA DE PRESENTACIÓN. Lo constituye un documento en donde se le informa al área a revisar la orden de auditoría, los auditores encargados y la fecha de realización de la misma.

CRONOGRAMA. En el se describren las actividades a realizar durante la auditoría, así como el personal participante para cada una de ellas. Se mencionan tiempos estimados y reales para cada actividad a realizar.

ACTIVIDADES A DESARROLLAR. En este espacio se mencionan la técnicas específicas a desarrollar y los procedimientos que llevará a cabo el auditor para cumplir con su objetivo. El desglose de los procedimientos debe tener un orden cronológico y ser congruente con las operaciones a revisar.

INFORME FINAL. Consiste en la realización tanto del alcance de la auditoría como los resultados u conclusiones.

Los puntos esenciales, genéricos y mínimos del informe de auditoría son los siguientes:

- Identificación del informe: El título del informe deberá identificarse con objeto de distinguirlo de otros informes.
- Identificación del cliente: debe identificarse a los destinatarios y a las personas que efectúen el encargo.
- Identificación a la entidad auditada: Identificación de la entidad objeto de la auditoría.
- Objetivos de la auditoría: Declaración de los objetivos de la auditoría para identificar su propósito, señalando los objetivos incumplidos.
- Normativa aplicada y excepciones: Identificación de las normas legales y profesionales utilizadas, así como las excepciones significativas de uso y el posible impacto en los resultados de la auditoría.
- Informe corto: en el se establecen las observaciones generadas de la revisión.

En el Informe debe contener uno de los siguientes tipos de opinión: **Favorable sin observaciones, con salvedades, desfavorable** o **adversa**, y **denegada.**

- Favorable sin observaciones: La opinión calificada como favorable, sin salvedades o limpia, deberá manifestarse de forma clara y precisa, y es el resultado de un trabajo realizado sin limitaciones de alcance y sin incertidumbre, de acuerdo a la normatividad legal y profesional.

- Opinión con salvedades: Se reitera lo dicho en la opinión favorable al respecto de las salvedades cuando sean significativas en relación con los objetivos de auditoría, describiéndose con precisión la naturaleza y razones.

- Opinión desfavorable: la opinión desfavorable o adversa es aplicable en el caso de:

    - Identificación de irregularidades.
    - Incumplimiento de la norma legal y profesional, que afecten significativamente a los objetivos de auditoría informática estipulados, incluso con incertidumbres: todo ello en la evaluación de conjunto y reseñando detalladamente las razones correspondientes.

- Opinión denegada: La denegación de opinión puede tener su origen en:

    - Las limitaciones al alcance de la auditoría.
    - Incertidumbres significativas de un modo tal que impidan al auditor formarse una opinión.
    - Irregularidades.
    - El incumplimiento de normativa legal y profesional.

NOTAS DE SOLICITUD DE INFORMACIÓN. Son documentos generados en los que se detallan la información que solicita el grupo de auditores al área auditada.

INFORMACIÓN PROPORCIONADA EN MEDIO MAGNÉTICO. Es la información o datos proporcionados por el área auditada a través de éste medio.

CÉDULA DE OBSERVACIONES. Es el formato utilizado para plasmar de manera específica la observación a la cual es sujeta el área auditada.

EVIDENCIA DOCUMENTAL. Es toda la evidencia documental generada durante la auditoría. Es la información proporcionada por el área auditada como documentación soporte de las observaciones encontradas en la revisión (manuales de usuario y técnicos, metodología empleada para el desarrollo de los sistemas, reportes del sistema, etc.).

II.9. CONCLUSIONES

Uno de los aspecto substanciales de la Auditoría de Sistemas es tener claro el objetivo por el cual de realiza la revisión y lo más importante, llevar una planeación de tiempo y forma como se llevará a cabo la auditoría.

Es por eso que es necesario contar con una metodología bien diseñada que nos lleve de la mano para realizar un trabajo de trascendencia en la toma de decisiones de la empresa o institución.

De acuerdo a lo anterior la metodología para la realización de la auditoría informática deberá contar con aspectos mínimos tales como:

- Alcance y Objetivos de la Auditoría Informática.
- Estudio inicial del entorno auditable.
- Determinación de los recursos necesarios para realizar la auditoría.
- Elaboración del plan y de los Programas de Trabajo.
- Actividades propiamente dichas de la auditoría.
- Confección y redacción del Informe Final.
- Redacción de la Carta de Introducción o Carta de Presentación del Informe final.

La Auditoría de Sistemas es una vertebra de la Auditoría Informática, ya que dependiendo de los resultados que arrojen la revisión a los sistemas de información se medirá que tan eficiente, eficaz y vulnerable es la información.

Una vez detallados los elementos que el auditor deberá considerar en la auditoría de sistemas, empleando la metodología que mejor se aplique a sus necesidades y conociendo los puntos susceptibles a revisar, en el siguiente capítulo se aplica lo visto en los capítuos I y II, realizando en un caso práctico la auditoría de sistemas a la Dirección General del Destinos de los Bienes de Comercio Exterior Propiedad del Fisco Federal.

Capítulo III

Auditoría de Sistemas a la Dirección General del Destino de Bienes de Comercio Exterior Propiedad del Fisco Federal

III. AUDITORÍA DE SISTEMAS A LA DIRECCIÓN GENERAL DEL DESTINO DE BIENES DE COMERCIO EXTERIOR PROPIEDAD DEL FISCO FEDERAL.

OBJETIVO

REALIZAR UNA AUDITORÍA DE SISTEMAS A LA DIRECCIÓN GENERAL DEL DESTINO DE BIENES DE COMERCIO EXTERIOR PROPIEDAD DEL FISCO FEDERAL (D.G.D.B.C.E.P.F.F.) EN EL RUBRO DE DESARROLLO Y MANTENIMIENTO DE SISTEMAS.

OBJETIVOS ESPECÍFICOS

INVENTARIO DE SISTEMAS EN DESARROLLO Y EN PRODUCCIÓN

- Verificar que la Dirección de Informática de la D.G.D.B.C.E.P.F.F. cuente con el inventario actualizado de los sistemas en desarrollo y producción.

METODOLOGÍA DE DESARROLLO DE SISTEMAS

- Revisar la metodología aplicada por la Dirección de Informática de la D.G.D.B.C.E.P.F.F. en el desarrollo de sistemas, para poder determinar su funcionalidad e identificar que fueron cubiertas las etapas del ciclo de vida de desarrollo de los sistemas. Asimismo verificar que cumplan con el fin para el cual se desarrollaron.

FASE DEL CICLO DE VIDA DE DESARROLLO DE SISTEMAS

Verificar que la Dirección de Informática de la D.G.D.B.C.E.P.F.F. considere en su ciclo de vida de desarrollo de sistemas los siguientes rubros:

- *Estudio de factibilidad*
- *Análisis*
- *Diseño*
- *Desarrollo*
- *Pruebas e implementación*
- *Mantenimiento*

DOCUMENTACIÓN DE LOS SISTEMAS CRÍTICOS

- Verificar que exista la documentación que permita llevar una narrativa de los sistemas, así como su estatus actual, objetivos, alcances, diseño y operación de los mismos.

INTEGRIDAD, CONFIABILIDAD Y SEGURIDAD DE LA BASE DE DATOS Y SISTEMAS DE INFORMACIÓN

- Verificar que en la base de datos, la entrada de la información sea validada y, que los errores que se presenten sean detectados y controlados de manera que la alimentación de datos sea auténtica, exacta, completa, oportuna y que durante el proceso que se lleva a cabo entre la entrada y salida, que ningún dato sea

agregado, removido o alterado. Asimismo, determinar si la información necesaria está disponible en los dispositivos que trabajan en línea y si ésta información es exacta, confiable y útil.

En este capítulo se aplican los los conceptos antes detallados y se pone en practica la auditoría de sistemas a la Dirección General del Destino de los Bienes de Comercio Exterior Propiedad del Fisco Federal, en donde se verifiará los controles internos de los procesos que intervienen en los sistemas en producción y los sistemas en desarrollo.

De igual forma se verificará la integridad, confiabilidad y seguridad de la información contenida en la BD.

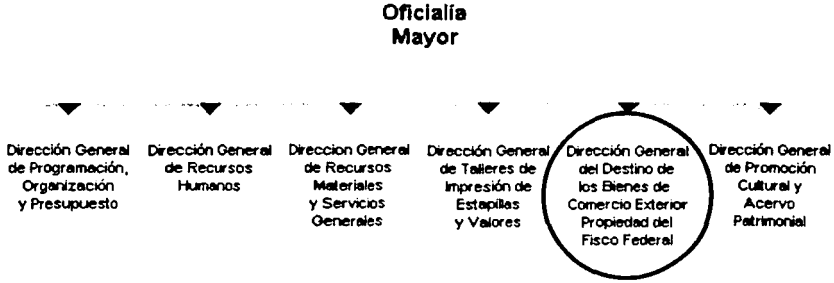
Es importante mencionar que los datos referidos a continuación son de carácter confidencial, por lo anterior, y para salvaguarda de la información en este documento no seran citados datos verdaderos. Los datos reales existen y son propiedad de la Contraloría Interna en la Secretaría de Hacienda y Crédito Público.

III.1. ANTECEDENTES

La Secretaría de Hacienda y Crédito Público está conformada de la siguiente manera:

El 30 de junio de 1997 se publicaron en el Diario Oficial de la Federación, reformas al Reglamento Interior de la Secretaría de Hacienda y Crédito Público, mediante las cuales se transformó el Consejo Asesor adscribiéndose orgánicamente como unidad administrativa bajo la denominación de Dirección General del Destino de los Bienes de Comercio Exterior Propiedad del Fisco Federal (D.G.D.B.C.E.P.F.F.), dependiente de la Oficialía Mayor.

La estructura es la siguiente:



Las actividades de la Dirección General del Destino de los Bienes de Comercio Exterior Propiedad del Fisco Federal abarcan la dirección, planeación y organización de las actividades necesarias para el control, administración y destino final de los bienes de comercio exterior que prevé la legislación aduanera, puestos a disposición de esta Dirección General, mediante la instrumentación de los acuerdos adoptados por los plenos del Consejo Asesor para la Determinación del Destino de las Mercancías que pasen a propiedad del Fisco Federal y del Comité de Asignación de Bienes al Sector Público, relativos a las operaciones de donación y venta de bienes; así como, de asignación, enajenación de excedentes detectados a maquiladoras o empresas con programas de exportación autorizados, destrucción, devolución, resarcimiento y pago de incentivos a entidades federativas adheridas en materia de Coordinación Fiscal, con sujeción al marco jurídico vigente.

Entre las funciones realizadas por la Dirección General del Destino de los Bienes de Comercio Exterior Propiedad del Fisco Federal de acuerdo al artículo 69-A del Reglamento Interior están:

- Determinar las políticas, procedimientos y criterios para el control, administración y destino de las mercancías de comercio exterior que han pasado a propiedad del Fisco Federal o se encuentren en los casos previstos en el artículo 157 de la Ley Aduanera;
- Informar a las personas que presten los servicios señalados en el artículo 14 de la Ley Aduanera, de las mercancías en abandono que no será objeto de destino por parte de esta Dirección General.
- Resarcir o indemnizar por mercancías dispuestas por esta Dirección General, en cumplimiento de resolución o sentencia que cause ejecutoria emitida por autoridad administrativa o judicial, mediante la devolución de la mercancía, y ante la imposibilidad práctica de esto, a través de mercancía de valor similar, o en su caso, mediante el pago pecuniario, que determine la autoridad competente.

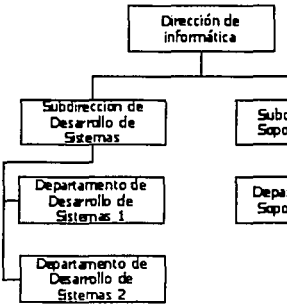
- Instruir que los ingresos obtenidos por la comercialización de las mercancías de comercio exterior se depositen en la Tesorería de la Federación de conformidad con la legislación aduanera y aplicar contra el fondo que se constituya, los pagos por resarcimiento o indemnización.
- Instruir a la unidad administrativa que corresponda, de los hechos de que tenga conocimiento con motivo de sus actividades, que puedan constituir delitos fiscales o delitos de servidores públicos de la Secretaría en el desempeño de sus funciones; así como coadyuvar en la esfera de su competencia, con la unidad administrativa que corresponda, en la investigación de hechos presumiblemente delictivos.
- Informar periódicamente y en forma anual al Oficial Mayor del resultado de las operaciones de destino de bienes; Así como, de los inventarios pendientes a disponerse.

La Dirección de Informática es medular para el buen funcionamiento de la D.G.D.B.C.E.P.F.F., ya que lleva a cargo el mantenimiento del Sistema Integral de Control Administrativo del Destino de Bienes (SICADEB) el cual tiene como propósito llevar el control, administración y destino de los bienes puestos a disposición del Fisco Federal, siendo éste el sistema sustantivo de la Dirección General.

Estructura Orgánica autorizada.

Con fecha 9 de noviembre de 2000, la Dirección General de Programación, Organización y Presupuesto de la Oficialía Mayor de la SHCP, notificó al Director General del Destino de los Bienes de Comercio Exterior Propiedad del Fisco Federal, del dictamen que contiene los cambios organizacionales, así como la Estructura Orgánica y Ocupacional conformada con 105 plazas de mando, autorizadas presupuestalmente por la Dirección General de Recursos Humanos, misma que quedó registrada en la DGPOP, con vigencia al mes de noviembre de 2000.

A continuación se describe la estructura registrada en la DGPOP, de la Dirección Informática, autorizada en el oficio mencionado en el párrafo anterior:



El manual proporcionado por la Dirección de Informática para su análisis fue autorizado con fecha 16 de diciembre de 1998, donde la Dirección General de Programación, Organización y Presupuesto de la Oficialía Mayor de la SHCP, notificó al Director General del Destino de los Bienes de Comercio Exterior Propiedad del Fisco Federal, el registro del Manual de Organización Específico de la DGDBCEPFF.

En el Manual de Organización Específico de la DGDBCEPFF se encuentran descritas las funciones y objetivo de la Dirección de Informática, de sus dos Subdirecciones y sus dos departamentos, a continuación se muestran los objetivos y principales funciones de cada Departamento, Subdirección y de la Dirección:

Dirección de Informática.

- ❖ Dirigir, coordinar, organizar, programar y evaluar el desarrollo de los programas en materia de sistematización y procesamiento de datos que contribuyan a eficientar la administración y control de las operaciones que realizan las áreas sustantivas de la Dirección General; así como, el óptimo aprovechamiento de los recursos y la eficiencia de su manejo, salvaguarda y registro, a fin de proporcionar a las áreas usuarias los apoyos necesarios de soporte técnico, capacitación, diseño y desarrollo de sistemas que faciliten el procesamiento de información.

Subdirección de Desarrollo de Sistemas.

- ⇒ Coordinar, programar y evaluar el desarrollo de programas en materia de sistematización y procesamientos de datos que contribuyan a eficientar la administración y control de las operaciones que realizan las áreas sustantivas de la Dirección General; así como, el óptimo aprovechamiento de los recursos y la eficiencia de su manejo, salvaguarda y registro.

Departamento de Desarrollo de Sistemas.

- ⇒ Instrumentar a través del procesamiento electrónico de datos, los requerimientos de las áreas usuarias para un mejor manejo de la información, proporcionado con oportunidad la información derivada de los procesos de cómputo electrónico de acuerdo a las normas y procedimientos establecidos.

Subdirección de Soporte Técnico.

- ⇒ Coordinar, programar, aplicar y mantener en forma permanente la disponibilidad del hardware y software en condiciones óptimas de operatividad por parte de las áreas usuarias que reciben el servicio; administrar de manera racional los equipos de cómputo y suministros necesarios, el programa de mantenimiento y soporte técnico de equipos, redes, instalaciones y paquetes informáticos; Así como la capacitación necesaria para la optimización y aprovechamiento de los equipos y sistemas.

Departamento de Soporte Técnico.

⇒ Llevar a cabo las actividades encaminadas a proporcionar asesoría en paquetes informáticos; así como, vigilar y auxiliar a las áreas usuarias en el uso apropiado de las herramientas informáticas para contribuir al óptimo desempeño de sus labores, supervisando que los equipos de cómputo asignados a cada área operen eficientemente para proporcionar la continuidad de operación.

III.2. ANÁLISIS DE LA INFORMACIÓN

De acuerdo a la información proporcionada por la Dirección General del Destino de los Bienes de Comercio Exterior Propiedad del Fisco Federal se tiene lo siguiente:

III.2.1. INVENTARIO DE SISTEMAS DE LA DGDBCEPFF

a) Sistemas en Operación

A continuación se señalan aquellos sistemas que actualmente se encuentran en producción en la DGDBCEPFF.

Sistema Integral de Control Administrativo del Destino de Bienes (SICADEB)

Este sistema tiene como propósito llevar el control, administración y destino de los bienes puestos a disposición del Fisco Federal. Conforme a la documentación proporcionada, lo integran 12 módulos que son:

ID	Nombre del Sistema y/o Módulo	Plataforma de operación	Bases de datos	Lenguaje de operación	Objetivo
1	Apartado y destino	Windows NT 4.0 (BD) Windows 95-98 (Cliente)	SQL Server 6.0	MS Visual Basic 5.0	Contar con una herramienta que agilice y facilite los procesos de destino de bienes.
2	Apartado y destino con seguimiento	Windows NT 4.0 (BD) Windows 95-98 (Cliente)	SQL Server 6.0	MS Visual Basic 5.0	Contar con una herramienta que agilice y facilite los procesos de destino de bienes.
3	Consultas a inventario	Windows NT 4.0 (BD) Windows 95-98 (Cliente)	SQL Server 6.0	MS Visual Basic 5.0	Contar con una herramienta que permita conocer las condiciones en que se encuentran los bienes que conforman el inventario temporal y definitivo de la Dirección General.
4	Ctrl. y Seguimiento de asignaciones y donaciones	Windows NT 4.0 (BD) Windows 95-98 (Cliente)	SQL Server 6.0	MS Visual Basic 5.0	Llevar el control automatizado y a detalle de las solicitudes que se presenten a esta Dirección General, asegurando en todo momento la obtención de información del estado que guarde cada una de ellas hasta llegar a solventarlas.
5	Correo	Windows NT 4.0 (BD) Windows 95-98 (Cliente)	SQL Server 6.0	MS Visual Basic 5.0	Controlar la documentación y por ende los asuntos que ésta trate, asegurando el registro, control y atención oportuna, así como, la facilidad de poder consultar información de carácter histórico.
6	Inventario definitivo	Windows NT 4.0 (BD) Windows 95-98	SQL Server 6.0	MS Visual Basic 5.0	Integrar los inventarios reales de la mercancía y vehículos que han sido

ID	Nombre del Sistema y/o Módulo	Plataforma de operación	Bases de datos	Lenguaje de operación	Objetivo
		(Cliente)			puesto a disposición en los almacenes fiscales a efecto de estar en posibilidad de atender las solicitudes del Comité y Consejo así como para destinar la destrucción los bienes no aprovechables para de esta manera desalojar los almacenes fiscales.
7	Inventario Temporal	Windows NT 4.0 (BD) Windows 95-98 (Cliente)	SQL Server 6.0	MS Visual Basic 5.0	Llevar el registro y control en inventario de los bienes que se encuentren puestos a disposición y que no han sido validados.
8	Libros blancos	Windows NT 4.0 (BD) Windows 95-98 (Cliente)	SQL Server 6.0	MS Visual Basic 5.0	Contar con una herramienta que apoye en el cierre de operaciones y en la emisión de cuadros con cifras finales para los Libros Blancos de la Dirección General.
9	No destine	Windows NT 4.0 (BD) Windows 95-98 (Cliente)	SQL Server 6.0	MS Visual Basic 5.0	Es una herramienta definida para apoyar las tareas relacionadas con los bienes, que por sus características no son considerados por esta Dirección General como susceptibles de ser asignados, donados o vendidos.
10	Transmisión Talisman	Windows NT 4.0 (BD) Windows 95-98 (Cliente)	SQL Server 6.0	MS Visual Basic 5.0	Mantener actualizado y sincronizado el inventario entre la Dirección General del Destino de Bienes de Comercio Exterior Propiedad del Fisco Federal y el almacén de Talismán.
11	Vales	Windows NT 4.0 (BD) Windows 95-98 (Cliente)	SQL Server 6.0	MS Visual Basic 5.0	Controlar la salida provisional de mercancías del almacén Talismán a través de vales de salida
12	Envíos SNSP	Windows NT 4.0 (BD) Windows 95-98 (Cliente)	SQL Server 6.0	MS Visual Basic 5.0	Informar al Sistema Nacional de Seguridad Pública (SNSP) de los movimientos de vehículos puestos a disposición de la Dirección General

De igual manera existen tres sistemas que trabajan a la par del SICADEB, son:

- Subsistema talismán.
- Oficios de salida.
- Sistema de información estratégica (S.I.E.).

Los cuales se detallan a continuación:

Subsistema Talismán

Este sistema tiene como propósito conocer el estado que guardan los bienes en el almacén de Talismán, así como, controlar administrativamente las entregas programadas. Consta de 3 módulos, que son:

ID	Nombre del Sistema y/o Módulo	Plataforma de operación	Bases de datos	Lenguaje de operación	Objetivo
1	Consultas a inventario Talismán	Windows NT 4.0 (BD) Windows 95-98 (Cliente)	SQL Server 6.0	MS Visual Basic 5.0	Contar con una herramienta que permita conocer las condiciones en que se encuentran los bienes en el almacén de manera rápida y confiable.

ID	Nombre del Sistema y/o Módulo	Plataforma de operación	Bases de datos	Lenguaje de operación	Objetivo
2	Correo Talismán	Windows NT 4.0 (BD) Windows 95-98 (Cliente)	SQL Server 6.0	MS Visual Basic 5.0	Contar con una herramienta adecuada para controlar la documentación y los asuntos que ésta trate, asegurando la atención oportuna así como la facilidad de poder consultar información de carácter histórico.
3	Salidas Talismán	Windows NT 4.0 (BD) Windows 95-98 (Cliente)	SQL Server 6.0	MS Visual Basic 5.0	Controlar administrativamente las entregas programadas en el almacén Talismán

Oficios de Salida

Este sistema tiene como propósito apoyar el registro y control de documentos de información de salida emitidos por la Dirección General del Destino de Bienes.

ID	Nombre del Sistema y/o Módulo	Plataforma de operación	Bases de datos	Lenguaje de operación	Objetivo
1	Oficios de Salida	Windows NT 4.0 (BD) Windows 95-98 (Cliente)	SQL Server 6.0	MS Visual Basic 5.0	Apoyar en el registro y control de los documentos emitidos por la Dirección General del Destino de Bienes.

S.I.E.

El sistema de Sistema de Información Estratégica (SIE), tiene como función principal mantener un registro actualizado de la trayectoria de personajes políticos de México.

ID	Nombre del Sistema y/o Módulo	Plataforma de operación	Bases de datos	Lenguaje de operación	Objetivo
1	SIE	Windows NT 4.0 (BD) Windows 95-98 (Cliente)	SQL Server 6.0	MS Visual Basic 5.0	Mantener un registro actualizado de la trayectoria de personajes políticos de México.

b) Inventario de Sistemas en Desarrollo

Actualmente la Dirección de Informática desarrolla un Módulo llamado "Traslados", que formará parte del SICADEB.

ID	Nombre del Sistema y/o Módulo	Plataforma de operación	Bases de datos	Lenguaje de operación	Objetivo
1	Traslados	Windows NT 4.0 (BD) Windows 95-98 (Cliente)	SQL Server 6.0	MS Visual Basic 5.0	Automatizar los traslados de mercancías.

III.3. METODOLOGÍA DE DESARROLLO DE SISTEMAS

La Dirección de Informática utiliza como metodología de desarrollo de sistemas un documento llamado "Proyecto de Análisis y Diseño de Sistemas" que contiene aspectos tales como:

- Nombre del proyecto
- Logotipo.
- Objetivo General
- Metodología de Desarrollo
- Entrevistas
- Cuestionarios
- Observación
- Fuentes de Datos Internas y Externas
- El sistema actual
- Análisis y Diseño Estructurado Moderno
- Lista de Eventos
- Diagramas Entidad-Relación
- Diagramas Causa-Efecto
- Diagrama de Contexto
- Diagramas de Flujo de Datos
- Diagramas de Transición de Estados (DTE)
- Construcción de Prototipos
- Diccionario de Datos
- Pseudo-código
- Mini especificaciones

Sin embargo, de la verificación de la documentación técnica del SICADEB, contra las especificaciones de la Metodología de desarrollo de sistemas de la DGDBCEPFF se tiene que no se entregó evidencia documental de los siguientes puntos:

- Lista de eventos
- Diagramas Causa-Efecto
- Diagrama de Contexto
- Diagrama de Flujo de Datos (DFD)
- Diagramas de Transición de Estados (DTE)

III.4. ANÁLISIS DE CUESTIONARIOS REFERENTES A LA METODOLOGÍA DE SISTEMAS UTILIZADA POR LA D.G.D.B.C.E.P.F.F.

Se aplicaron 6 cuestionarios (Ver anexo: "Formato de cuestionarios") a la Dirección de Informática, referentes a las fases que constituyen la metodología para el desarrollo de sistemas, de los cuales se desprenden los siguientes resultados:

a) Estudio de Factibilidad:

La Dirección de Informática realiza estudios de factibilidad técnica en los sistemas que desarrolla, en los cuales se incluyen aspectos tales como:

- Necesidades de equipo y su disponibilidad
- Necesidades de software de sistema y su disponibilidad
- Equipo de comunicaciones y su disponibilidad

b) Evaluación de la Metodología:

De acuerdo a lo contestado en el cuestionario "Evaluación de la Metodología" se tiene lo siguiente.

Puntos que se cubren de metodología de desarrollo de sistemas:

- Determinar requerimientos
- Objetivo
- Diagramas de flujo de datos (DFD)
- Diagramas de entidad-relación
- Diccionario de datos

El porcentaje que se considera que es conocida la metodología de desarrollo de sistemas varía entre 75% y 100%, esto de acuerdo a lo descrito en el cuestionario.

Cabe señalar, que de acuerdo a lo contestado, la Metodología no es llevada a cabo en su totalidad debido a la carga de trabajo que presenta el Área y a la falta de recursos humanos.

III.5. FASES DEL CICLO DE VIDA DE DESARROLLO DE SISTEMAS

En esta parte se muestra la evaluación de las Etapas de Análisis, Desarrollo, Implementación y Mantenimiento de Sistemas

III.5.1. ANÁLISIS

Durante la etapa de análisis, las actividades previas al inicio de un sistemas son:

- Reunión con usuarios
- Especificación de requerimientos
- Determinación de los requisitos de la información

Los grupos de trabajo para el análisis y elaboración del modelo del sistema los integran personal de la Subdirección de Desarrollo de Sistemas y personal involucrado por parte del área solicitante.

Los pasos que se siguen para la aprobación formal del sistema son:

- Reunión de mandos superiores
- Formulación de minutas de acuerdo

Una vez que el modelo es aprobado, los pasos que se siguen para la planeación del proyecto son:

- Se define el tiempo requerido y magnitud del proyecto.
- Se definen especificaciones técnicas.
- Se asignan actividades al personal seleccionado.

El Subdirector de Desarrollo indicó que en el "Programa de trabajo" se incluyen las actividades relacionadas con el desarrollo de sistemas, además señaló que él es el encargado de asignar personal para el desarrollo del mismo.

Por otro lado, señaló que, las reuniones para dar continuidad al proyecto las conforman personal de desarrollo asignado y la periodicidad de las mismas, depende en gran medida a la magnitud del proyecto.

De lo anterior, el Área proporcionó como ejemplo los siguientes documentos generados en esta fase:

- Minutas de acuerdo:
  - Sesión de trabajo "Presentación del sistema de control y seguimiento de destinos" 27 de marzo de 1999.
  - Sesión de trabajo 14 de septiembre de 1999.
  - Sesión de trabajo "Presentación del sistema Talismán" 29 de septiembre de1999

- Minuta junta 001/Informática "Actualización y puesta en operación del Sistema de Información y Estrategia Política (SIEP) y el Sistema de Identificación de Municipios (SIM)"

III.5.2. DESARROLLO

En esta etapa se elaboran aspectos como:

- Diagramas de flujo de datos (DFD).
- Diagramas de entidad-relación.
- Diccionario de datos

El Subdirector de Desarrollo indicó que dichos puntos son documentados por la Subdirección a su cargo y aprobados por el Director de Informática.

Cabe señalar que de la documentación proporcionada por el Área, con relación al SICADEB, únicamente fue proporcionado el diagrama Entidad-Relación y el diccionario de datos.

III.5.3. IMPLANTACIÓN

Las pruebas para conocer el grado de avance del sistema constan de un prototipo presentado por la Subdirección de desarrollo del Área usuaria (mandos superiores), con el propósito de conocer sus impresiones y considerarlas para la conclusión del mismo.

El procedimiento que se realiza una vez que los sistemas son aprobados por el usuario es:

1. Se libera el sistema con una atenta nota dirigida por el Director de Informática al Área usuaria.
2. Se instala el módulo en el área usuaria

3. Se programan los cursos de capacitación
4. Se entregan los manuales de usuario

De lo anterior, el Área proporcionó como ejemplo los siguientes documentos generados en esta fase:

- Atenta Nota No. 126/99 de fecha 23 de mayo de 2000, asunto: liberación del módulo de No Destino v100.
- Atenta Nota No. 234/2000 de fecha 10 de noviembre de 2000, asunto: Liberación del sistema de información estratégica.

Cabe señalar que los manuales de usuario se entregan en los cursos de capacitación a los usuarios, esto indicó el Director de informática, sin embargo, esta entrega se hace de manera económica, es decir no se tiene la evidencia documental de que el usuario recibe dichos manuales.

Asimismo, el Director de Informática entregó una Atenta Nota a los Directores Generales Adjuntos, Secretario Particular y Directores de Área de fecha 22 de febrero de 2001, en donde informa la ruta en el servidor donde podrán obtener y consultar en línea los Manuales de Usuario de los sistemas en operación y le solicita hacerlo del conocimiento de su personal en las Áreas a su cargo.

Referente a los cursos de capacitación de acuerdo con el Director de Informática, una vez liberado el sistema, los mandos superiores de las Áreas usuarias hacen llegar a la Dirección de Informática una relación de usuarios para impartirles cursos de capacitación del nuevo sistema.

De lo anterior, el Área proporcionó como ejemplo los siguientes documentos generados en esta fase:

- Atenta Nota No. DDA/084.2000 y No. DDA/084A.2000 de fecha 8 de mayo de 2000, asunto: calendario para el curso de capacitación del Sistema de Control y Seguimiento.
- Atenta Nota No. DDA/100.2000 de fecha 17 de mayo de mayo de 2000, asunto: Cursos de capacitación para la liberación del Sistema de Control y Seguimiento.
- Atenta Nota No. DDA/108.2000 de fecha 24 de mayo de 2000, asunto: Reprogramación de cursos de capacitación.
- Atenta Nota No. DDA/17.2000 de fecha 30 de mayo de 2000, asunto: Reprogramación de cursos de capacitación.
- Atenta Nota No. DDA/138.2000 de fecha 14 de junio de 2000, asunto: Cursos de capacitación.

De manera general el contenido de los manuales de usuario es el siguiente:

- Objetivo
- Políticas
- Descripción de las opciones

El contenido de la documentación técnica está constituido por:

- Objetivo
- Lenguaje de programación
- Plataforma de operación
- Código fuente (impresión).
- Referencias cruzadas
- Estadísticas
- Árbol de llamadas

III.5.4. MANTENIMIENTO

La Dirección de Informática no cuenta con un procedimiento por escrito para solicitar cambios o modificaciones al sistema, ya que estas se solicitan mediante Atenta Nota dirigida por el Área usuaria a la Dirección de Informática. Las personas encargadas de solicitar estas modificaciones generalmente son mandos superiores.

Asimismo, se menciona en los cuestionarios que la Dirección de Informática lleva un registro de los cambios realizados a los sistemas (control de versiones) en el cuál se indica las modificaciones, problemática detectada y la fecha en que se atendió, cuyo control es llevado directamente por la misma Dirección.

La bitácora de actualizaciones o modificaciones al SICADEB cuenta con los siguientes aspectos:

- Fecha
- Número de modificación
- Persona quién realizó la modificación
- Módulo del SICADEB afectado
- Nombre de los archivos fuentes originales
- Localización de los archivos fuentes modificados (nombre de equipo y directorio)
- Nombres de los archivos fuentes modificados
- Localización de archivos fuentes modificados (nombre de equipo y directorio)
- Tipo de modificación
- Descripción de la modificación
- Objetos modificados
- Evento modificado
- Observaciones
- Objetivo de la modificación
- Fecha de implementación de modificaciones
- Anexos
- Firma de quién llevó a cabo la modificación

III.6. DOCUMENTACIÓN TÉCNICA Y DE USUARIO DEL SICADEB

De acuerdo a la información proporcionada por la Dirección de Informática de la DGDBCEPFF referente a los manuales técnicos, de usuario y diccionario de datos se tiene que:

a) Manuales de Usuario

El SICADEB está integrado por 12 módulos y cada uno de ellos cuenta con manual de usuario y técnico. El Manual de Usuario contempla los siguientes aspectos:

- **Presentación:** Este apartado menciona de manera general el propósito por el cual fue creado el módulo, así como, él porque de su inclusión al SICADEB.
- **Objetivo:** Describe la finalidad por el cuál fue creado el sistema.
- **Políticas:**
  - *Operación*: el manejo que deberá tener el usuario para poder trabajar dentro del módulo.
  - *Seguridad*: el manejo que deberá tener el usuario a cerca del uso de la información.
- **Operación del Sistema:** Indica de manera detallada los pasos a seguir para uso y manejo del módulo.

Cabe señalar que dentro de la operación del sistema se incluyen los posibles mensajes de error y qué hacer en caso que se presenten.

b) Manual Técnico

El manual técnico del SICADEB contempla aspectos tales como:

- **Objetivo:** Describe la finalidad por el cuál fue creado el módulo.
- **Lenguaje de Programación:** Visual Basic 5.0
- **Plataforma**
  - *Red*: Windows NT 4.0
  - *Base de datos*: SQL Server 6.0
- **Localización de programas fuentes:** Indica la ruta en la que se localiza el código fuente en el servidor.
- **Código fuente:** especifica las instrucciones utilizadas para la automatización de procesos del sistema.

Cabe señalar que aspectos como: diagramas de Entidad-Relación, descripción de módulos, diccionario de datos, bitácora de actualización y/o mantenimiento y acta de liberación o de actualización son controles que llevan por separado.

c) Diccionario de Datos

De acuerdo a la documentación proporcionada por la Dirección de Informática, el diccionario de datos del SICADEB contempla los siguientes puntos:

- Nombre del campo
- Tipo
- Longitud
- Precisión
- Escala
- Nulos
- Descripción del campo

Asimismo, el SICADEB está constituido por 88 tablas las cuales se mencionan a continuación:

Id	Nombre de la tabla	Id	Nombre de la tabla	Id	Nombre de la tabla	Id	Nombre de la tabla
1	Aclaraciones	26	Copias_NoDestino	51	Negativas	76	Status
2	Aduanas	27	Copias_oficio	52	Nivel_gobierno	77	Status_oficios
3	Aduanas_E_Fed	28	Correo	53	Nivel_secretaria	78	Subclasificaciones
4	Almacenes fiscalizados	29	Destino	54	No_destino	79	Textos_oficios
5	Area_designa	30	Entidades_federales	55	Oficios_98	80	Tipo_filantrópicas
6	Articulos	31	Estado_general	56	Oficios_NoDestino	81	Tipos_cancelación
7	Articulos_faltantes	32	Expedientes	57	Permisos	82	Tipos_negociacion
8	Articulos_Temp.	33	Folio_env_SNSP	58	Personal	83	Tipos_permisos
9	Articulos_valid	34	Folios	59	Precarpetas	84	Turnados
10	Asuntos	35	Folios_transmisión	60	prioridades	85	Ubicación_expediente
11	Automoviles	36	Funcionarios	61	Rdes_tot_m	86	Usuarios
12	Automoviles_faltantes	37	Gestor_solicitud	62	Rdes_tot_v	87	Vales
13	Automoviles_Temp.	38	Gestores	63	Referencias	88	Zona_inv
14	Automóviles_valid	39	Historico	64	Region_Inv		
15	Autoridad	40	Horarios	65	Reporte_global		
16	Autorizaciones	41	Indicadores	66	Resoluciones		
17	Bajas	41	Inst_filantrópicas	67	Rj_ad_alaf_clas_UM		
18	Bajas_matching	43	Inst_publicas	68	Rj_e_fed_clas_UM		
19	Bajas_NoDestino	44	Instrucciones	69	Rj_tot_clas_UM		
20	Bajas vales	45	Mapeo_asunto_oficio	70	Rj_tot_veh_scl		
21	Bene_X_A	46	Matching	71	Rj_tot_veh_scl_E_fed		
22	Cancelaciones	47	Mercancía_solicitada	72	Rj_tot_veh_scl_rec		
23	Categorías	48	Mercancías	73	Secretarias_de_estado		
24	Clasif96	49	Modalidad_documento	74	Secretarias_rep_G		
25	Clasificaciones	50	Municipios	75	Solicitud		

III.7. INTEGRIDAD, CONFIABILIDAD Y SEGURIDAD DE LA BASE DE DATOS DEL SICADEB

La estructura de la base de datos es de tipo relacional, ya que permite expresar de forma gráfica las relaciones entres las tablas entrando en el diseño detallado campo a campo, esto de acuerdo al esquema de entidad-relación del SICADEB.

III.8. ANÁLISIS DE LA INFORMACIÓN PROPORCIONADA EN MEDIO ÓPTICO (CD-ROM)

De acuerdo a la información solicitada a la Dirección General Adjunto Operativo de la DGDBCEPFF y el apoyo técnico de la Dirección de Informática con relación a los módulos de Correo, Inventario Definitivo e Inventario Temporal, las tablas principales que fueron entregadas en CD-ROM (4 archivos) y que están involucradas en dichos módulos son:

Nombre del archivo	No. de columnas	No. de registros	Suma del campo de cantidad	Tamaño del archivo
Articulos.rpt	40	226,019	12,262,657.52	101,119 kb
Articulos_Temp.rpt	38	14,174	21,810,399.4	5,653 kb
Automóviles.rpt	42	39,451	10,153	18,261 kb
Automoviles_Temp.rpt	40	4,927	4,930	2,051 kb

Al momento de la verificación de los archivos, fueron identificados registros vacíos asimismo la cantidad de registros no coincidió con las cifras de control de la DGDBCEPFF, por lo cual se llevó a cabo una verificación a las tablas de la base de datos del SICADEB en línea el día 15 de marzo de 2000 en presencia del Subdirector de Desarrollo, para verificar la existencia de registros vacíos relacionados con los inventarios temporal y definitivo de artículos y automóviles.

Se verificó físicamente que existiera un identificador (primary key) para los objetos diversos de la base de datos, esto de acuerdo a lo establecido en el diccionario de datos del SICADEB.

Por lo que se identificaron en el diccionario de datos de las tablas antes mencionadas, los campos que se establecieron como únicos o llave y se realizó la verificación física de los mismos, validando que dichos campos por ser llave no se encontraran vacíos o presentaran registros duplicados.

La validación física se realizó en la herramienta incorporada en SQL Server (El manejador de la base de datos que utiliza la Dirección de Informática) llamada ISQL/w.

En este entorno se realizaron los queries necesarios a fin de comprobar la integridad de los campos llave, la sintaxis del query fue el siguiente:

Select registros=count(*) from articulos where no_articulo =null
Select registros=count(*) from articulos where no_aduana =null
Select registros=count(*) from articulos where no_clasificacion =null
Select registros=count(*) from articulos where no_subclasificacion =null

Lo que indica el query selecciona todos los campos de la tabla articulos mientras el campo no_articulo se encuentre vacío.

La misma sintaxis del query fue aplicada para las tablas restantes (articulos_Temp., automoviles y automoviles_Temp.) en donde no se encontraron registros vacíos y/o duplicados.

III.9. ANÁLISIS A LOS CUESTIONARIOS

Se aplicó al Subdirector de Desarrollo, quien es el administrador de la Base de Datos, el cuestionario "Integridad, confiabilidad y seguridad de la base de datos y sistemas de información" obteniendo de acuerdo a lo descrito los siguientes resultados:

a) Especificaciones del Sistema Manejador de Base de Datos (SMBD)

El manejador de la base de datos que utiliza la Dirección de Informática es Microsoft SQL Server 6.0. las utilerías con las que cuenta el manejador para mantener la integridad de la información son: Enterprice manager, transact SQL , entre otras.
Las utilerías más utilizadas por la subdirección de desarrollo son: enterprice manager, ISQL/w, backup, restore y DBCC CheckDB.

La estructura de la base de datos es centralizada y relacional, y los procedimientos o políticas para la operación y acceso al manejador de la Base de Datos son: Procedimiento de respaldo y recuperación de la Base de datos, procedimiento de alta de usuarios y baja de usuarios.

b) Integridad de la Información de la Base de Datos

Dentro de los procedimientos para el desarrollo de sistemas se contempla aspectos como:

- Pruebas formales con usuarios (consiste en reuniones con los altos mandos que se registran en las minutas de acuerdos).
- Integridad del código fuente y ejecutable(Manuales técnicos).
- Área reservada para pruebas (el servidor de desarrollo para pruebas).
- Pistas de auditorías.
- Control de versiones (bitácora de actualizaciones o modificaciones al SICADEB).

Las áreas usuarias (operativas) son las encargadas y responsables del control de los datos que son introducidos en las pantallas de los sistemas en producción y los controles para la validación de la entrada de datos en los módulos están contenidos en el manual de captura del SICADEB.

Asimismo, los procedimiento que se contempla para la validación de los datos son las transacciones en las aplicaciones de desarrollo.

c) Confidencialidad de la información en la base de datos

Los principales procesos que atiende el administrador con relación a la Base de Datos son: Respaldo de la base de datos, generación de queries, administración de la base de datos (desbloqueos y transacciones).

El equipo para desarrollo de sistemas esta protegido contra:

- Robo
- Acceso no autorizado (Letreros)
- Contingencias (plan de contingencia de la Dirección de Informática)
- Perdida de información (respaldos diarios)
- Modificación de información (Personalización de claves de acceso)
- Daños físicos (Contrato de mantenimiento preventivo y/o correctivo)

Los documentos que soportan estos controles de seguridad son: las políticas de acceso y el manual de contingencia.

Por otra parte, el lugar donde se realiza el desarrollo de sistemas es un área aislada de resto de las áreas y solo el personal de informática tiene llave.

Dentro del análisis de los sistemas, los procedimientos de autorización que se encuentran establecidos son:

- Equipo restringido (se utiliza un servidor de desarrollo)
- Niveles de seguridad preasignados
- Autentificación de usuarios
- Verificación de permisos
- Niveles de autorización en el manejo de sistemas como lectura, adiciones y modificaciones.

d) Confiabilidad de la información de la base de datos

Los procedimientos y/o políticas para la administración de las claves de acceso a los sistemas para el usuario final se encuentran descritas en un documento llamado "Manual de procedimiento de alta de usuarios".

Los procedimientos de captura y verificación de la información que se ingresa al SICADEB se encuentran descritos en el manual de captura y manual de usuarios de la aplicación a la que se tenga acceso.

e) Controles de la base de datos

La forma de prevenir que la información capturada en el SICADEB no se duplique es que en el inventario de vehículos se verifica el número de serie en el sistema y en el inventario de mercancías el área operativa tiene un procedimiento de validación.

Asimismo, la base de datos del SICADEB cuenta con transacciones y triggers (procedimientos almacenados) a fin de asegurar que la información se íntegra y confiable.

f) Desarrollo y mantenimiento de sistemas

El usuario para tener acceso a los sistemas requiere estar dado de alta en la red, estar dado de alta en la base de datos (si tienen acceso a los sistemas internos) y contar con un perfil en la tabla de usuarios.

La forma de cómo el administrador identifica a un usuario en la red es mediante su RFC y los privilegios otorgados de acuerdo al área que la solicita y a las aplicaciones a las que el usuario tenga acceso.

g) Control de acceso a los sistemas

Las claves de acceso a los sistemas se otorgan de manera personalizada y se encuentran descritos en un documento llamado "Relación de claves de usuarios activos".

h) ...guridad lógica de los sistemas

Los procedimientos establecidos para el control del mantenimiento (modificación de tablas, programas, menús) del SICADEB son:

- Para la modificación de información contenida en el sistema, existe una bitácora de acceso en donde se registran aquellos usuarios que realizan principalmente alta, baja o modificaciones.
- Para modificaciones (mantenimiento) de la estructura de la base de datos del SICADEB se cuenta con una bitácora de modificaciones realizadas al SICADEB.

III.10. CONCLUSIONES, OBSERVACIONES Y RECOMENDACIONES

Una vez analizado la información proporcionada por la Dirección de Informática, dio como resultado lo siguiente:

III.10.1. *METODOLOGÍA DE DESARROLLO*

Del análisis a la información referente a la Metodología de desarrollo de sistemas se tiene que:

- De la documentación de los 12 módulos en operación que integran el SICADEB, así como de los tres sistemas independientes (Subsistema de Talismán, Oficios de Salidas y el Sistemas de Información Estratégica), proporcionados por la Dirección de Informática, no se documenta la totalidad de los puntos descritos en la Metodología de Desarrollo de Sistemas establecida por el Área (Proyecto de Análisis y Diseño de Sistemas), ya que no se encontraron los siguientes aspectos:
  - Lista de eventos
  - Diagramas Causa-Efecto
  - Diagrama de Contexto
  - Diagrama de Flujo de Datos (DFD)
  - Diagramas de Transición de Estados (DTE)

CAUSA:

El Director de informática indicó que no se han documentado todos los puntos contenidos en la metodología de desarrollo de sistemas llamado "Proyecto de análisis y diseño de sistemas" debido a la carga de trabajo que actualmente tiene la Dirección.

Asimismo, el Subdirector de Desarrollo indicó que están analizando la posibilidad de cambiar la metodología de desarrollo de sistemas que actualmente se utiliza en el Área.

EFECTO:

Retrasa el mantenimiento técnico de los sistemas en producción a personal de nuevo ingreso, lo que repercute en el tiempo de respuesta al usuario y dificulta la administración de los sistemas en producción al no contar con la totalidad de documentación técnica.

RECOMENDACIONES

CORRECTIVA:

La Dirección de Informática deberá complementar la documentación técnica de los sistemas en producción, a fin de contar con toda la información para su mantenimiento y cumplir con todos los aspectos que contempla su metodología de desarrollo de sistemas.

PREVENTIVA:

La Dirección de Informática deberá mantener actualizada la documentación técnica y los manuales de usuario de sus sistemas en caso de que estos sufran algún cambio o se generen versiones nuevas.

III.10.2. *INTEGRIDAD, CONFIABILIDAD Y SEGURIDAD DE LA BASE DE DATOS*

Referente al análisis de la integridad, confiabilidad y seguridad de la base de datos del SICEDEB se tiene que:

El SICADEB es una Base de Datos de modelo relacional, que basándose en el análisis realizado a la documentación proporcionada por la Dirección de Informática cumple con lo siguiente:

- En la base de datos se define una llave primaria (primary key) que es única para cada objeto; es decir, no hay dos identificadores iguales para objetos (instancias) del mismo tipo.

- La primary key no contiene registros nulos, es decir, es de tipo NOT NULL

La base de datos del SICADEB está compuesta por 88 tablas de las cuales se analizaron las siguientes:

- Articulos.rpt
- Articulos_Temp.rpt

- Automoviles.rpt
- Automóviles_Temp.rpt

Y de acuerdo al diccionario de datos, los campos no_articulo, no_aduanas, no_clasificacion y no_subclasificacion de cada una de las tablas antes mencionadas, son descritos como requeridos o NOT NULL y de la verificación a la base de datos en línea del SICADEB no fueron encontrados registros vacíos y/o duplicados.

Por lo anterior se concluye:

La estructura de la base de datos corresponde con lo establecido en el diccionario de datos proporcionado por la Dirección de Informática como parte de la documentación técnica del sistema.

III.11. INTEGRACIÓN DE PAPELES DE TRABAJO

La integración de papeles de trabajo lo conforman toda la evidencia documental proporcionada por el área auditada a fin de realizar el análisis de la información y con base a los resultados emitir un diagnóstico.

CARÁTULA: en ella se pone los datos generales de la revisión.

OFICIO DE COMISIÓN: Es un oficio en el cual se le comunica al Área la práctica de auditoría

INFORME DE AUDITORÍA: En el se comunica al responsable del área auditada los resultados de la revisión, para su conocimiento.

CÉDULA ÚNICA DE AUDITORÍA: Es un formato en donde se lleva un control de la cantidad total de observaciones hechas al área.

ACTA DE INICIO DE AUDITORÍA: Es el documento legal que compromete al área auditada en proporcionar a los auditores encargados la información que éstos soliciten.

CARTA PLANEACIÓN: Es un documento en donde se especifica de manera detallada el objetivo de la auditoría, el alcance y los rubros que se revisarán.

CRONOGRAMA DE ACTIVIDADES: Es un programa que determina las actividades y el tiempo empleado en la revisión de cada uno de los puntos a auditar.

OFICIOS DE SOLICITUD DE INFORMACIÓN AL ÁREA: Son los oficios y/o notas que se remiten al área auditada a fin de proporcionar documentación para fines de la auditoría.

PAPELES DE TRABAJO: Es toda la evidencia documental que soporta los resultados obtenidos en la auditoría.

INFORMACIÓN EN MEDIO MAGNÉTICO: Es la información que proporciona el área auditada en medio magnético.

De los papeles de trabajo obtenidos en esta revisión, únicamente se muestra el informe largo de las observaciones arrojadas de la auditoría realizada al Área. *Ya que por tratarse de una auditoría, la información es estrictamente confidencial para prevenir el mal uso de la misma.* (Ver anexo"Papeles de trabajo")

Conclusiones Finales

CONCLUSIONES FINALES

La misión primordial de la auditoría es proporcionar información a los niveles directivos de las áreas de cualquier entidad tanto pública como privada, y de cualquier sector, como herramienta para la toma de decisiones. Es por ello que a esta función se le debe dar un lugar dentro de cualquier estructura orgánica.

El auditor no es más que un aliado para el logro de los objetivos en una organización, encargado de encontrar áreas de oportunidad y/o debilidades en los controles para su posterior canalización a instancias reguladoras y normativas para su sanción. Para esto, el auditor debe tener una capacidad de análisis y objetividad, a fin de que la relación entre la debilidad detectada, por pequeña que pudiera parecer y las actividades y procedimientos vitales o críticos sea tal que de no resolverse pueda implicar un uso inadecuado de recursos (humanos, materiales, financieros y tiempo), reflejándose en pérdidas monetarias para la organización.

Al realizar el presente trabajo se investigó acerca de elementos tales como:

- Antecedentes de auditoría.
- Metodologías utilizadas para auditar sistemas de información.
- Metodolc · ías utilizadas para auditar bases de datos
- Seguridad, integridad y confidencialidad en datos.
- Normatividad aplicable en la realización de auditorías de sistemas.

Que pudieran servir para emitir una correcta evaluación, así como darse cuenta que dentro del ambiente laboral es de vital importancia contar con información en tiempo y forma, clara y precisa para que se constituya en una herramienta poderosa para la toma de decisiones.

La Auditoría de Sistemas es una parte mínima de lo que abarca la Auditoría Informática, sin embargo esto no quiere decir que no sea importante, por el contrario, es una parte sustantiva en el logro de los objetivos, que sin duda es salvaguardar la información, ya que el uso de la información debe ser adecuada y sobre todo explotado de tal forma que

reditúe lo que en ésta se invierte, cualquier abuso mal encaminado se reflejará en los resultados generados en cada una de las áreas usuarias.

La conclusión principal, es que toda empresa, pública o privada, que posean Sistemas de Información deben de someterse a un control estricto de evaluación de eficacia y eficiencia. Aproximadamente hoy en día, el 90 por ciento de las empresas tienen toda su información estructurada en Sistemas Informáticos, de aquí, la vital importancia que los sistemas de información funcionen correctamente. Una empresa puede tener un staff de gente de primera, pero si tiene un sistema informático propenso a errores, lento, vulnerable e inestable; si no hay un balance entre estas dos cosas, la empresa nunca saldrá a adelante. En cuanto al trabajo de la auditoría en sí, podemos remarcar que se precisa de gran conocimiento de Informática, seriedad, capacidad, minuciosidad y responsabilidad; la auditoría de Sistemas debe hacerse por gente altamente capacitada, una auditoría mal hecha puede acarrear consecuencias drásticas para la empresa auditada, principalmente económicas.

El presente trabajo de tesis, mostró un panorama general de lo que actualmente es la Auditoría a Sistemas. Confiando en que el presente trabajo tenga una aportación útil para aquellos que tienen como tarea principal la salvaguarda de la información de todos los recursos en las organizaciones, espero les sirva como referencia en auditorías de sistemas de información.

Anexo

Papeles de trabajo

INFORME DE AUDITORÍA

No. DE REVISIÓN:	S-01/2001
SECTOR:	HACIENDA Y CRÉDITO PÚBLICO
DEPENDENCIA O ENTIDAD:	SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO
ÁREA AUDITADA:	DIRECCIÓN GENERAL DEL DESTINO DE LOS BIENES DE COMERCIO EXTERIOR PROPIEDAD DEL FISCO FEDERAL
TIPO DE AUDITORÍA:	ESPECÍFICA
PERIODO REVISADO:	ENERO DE 1997 A MARZO DE 2001 DE LAS TABLAS ARTÍCULOS, ARTÍCULOS_TEMP, AUTOMÓVILES Y AUTOMÓVILES_TEMP DE LA BASE DE DATOS DEL SISTEMA INTEGRAL DE CONTROL ADMINISTRATIVO DEL DESTINO DE BIENES (SICADEB)
FECHA DE INICIO:	22 DE ENERO DE 2001
FECHA DE CONCLUSIÓN:	30 DE MARZO DE 2001
FECHA DE DISCUSIÓN:	DURANTE LA AUDITORÍA
SUPERVISOR ENCARGADO:	
AUDITOR ENCARGADO:	

ÍNDICE

PÁGINA

I. ANTECEDENTES.

El 30 de junio de 1997 se publicaron en el Diario Oficial de la Federación, reformas al Reglamento Interior de la Secretaría de Hacienda y Crédito Público, mediante las cuales se transformó el Consejo Asesor adscribiéndose orgánicamente como unidad administrativa bajo la denominación de Dirección General del Destino de los Bienes de Comercio Exterior Propiedad del Fisco Federal (DGDBCEPFF), dependiente de la Oficialía Mayor.

Las actividades de la Dirección General del Destino de los Bienes de Comercio Exterior Propiedad del Fisco Federal abarcan la dirección, planeación y organización de las actividades necesarias para el control, administración y destino final de los bienes de comercio exterior que prevé la legislación aduanera, puestos a disposición de esta Dirección General, mediante la instrumentación de los acuerdos adoptados por los plenos del Consejo Asesor para la Determinación del Destino de las Mercancías que pasen a propiedad del Fisco Federal y del Comité de Asignación de Bienes al Sector Público, relativos a las operaciones de donación y venta de bienes; así como, de asignación, enajenación de excedentes detectados a maquiladoras o empresas con programas de exportación autorizados, destrucción, devolución, resarcimiento y pago de incentivos a entidades federativas adheridas en materia de Coordinación Fiscal, con sujeción al marco jurídico vigente.

Con base al Programa Anual de Control y Auditoría (PACA) 2001, se programó una revisión a la Dirección General del Destino de los Bienes de Comercio Exterior Propiedad del Fisco Federal (DGDBCEPFF) con el objetivo de evaluar la administración de la Tecnología de Información utilizada en esa área.

II. PERIODO, OBJETIVO Y ALCANCE DE LA REVISIÓN.

2.1. PERIODO.

La revisión se llevó a cabo del 26 de enero al 22 de marzo de 2001, en las instalaciones de la Dirección General del Destino de los Bienes de Comercio Exterior Propiedad del Fisco Federal, ubicadas en Av. División del Norte No. 2786, Col. Parque San Andrés, Delegación Coyoacán, C.P. 04040, México, D. F.

2.2. OBJETIVO

Comprobar que los procedimientos, registros y controles establecidos sobre la Tecnología de Información por la Dirección General del Destino de los Bienes de Comercio Exterior Propiedad del Fisco Federal, permitan efectuar la correcta administración de los sistemas de cómputo, para que la información producida por estos sea confiable y oportuna.

2.3. ALCANCE.

Mediante pruebas selectivas que se aplicaron de conformidad con las Normas Generales de Auditoría Pública y con los procedimientos de Auditoría de Sistemas que se consideraron necesarios para cada concepto revisado, se evaluaron las tablas Artículos, Artículos_Temp, Automóviles, Automóviles_Temp de la Base de Datos del Sistema Integral de Control Administrativo del Destino de Bienes (SICADEB) del mes de enero de 1997 a marzo de 2001 y las operaciones realizadas por la Dirección de Informática en los rubros de:

1.- PLANEACIÓN.

- Plan de Trabajo del área informática de la DGDBCEPFF para 2000 y resultados obtenidos hasta el 31 de diciembre de 2000; así como el Plan de Trabajo 2001 con avances a la fecha de revisión.

2. - ORGANIZACIÓN.

- Estructura Orgánica del área informática y grado de conocimiento de la misma.
- Manuales de Organización y Procedimientos.
- Programa de Capacitación.
- Programas y procedimientos de seguridad y protección que consideren:
  - Acceso restringido a personas no autorizadas a recursos informáticos.
  - Plan de Contingencias Informático y Plan de Respaldos de Información.

3. - DESARROLLO Y MANTENIMIENTO DE SISTEMAS.

- Metodología de desarrollo de sistemas.
- Inventario de sistemas en operación y en desarrollo.
- Documentación de los sistemas en operación:

  - Manuales de usuario.
  - Manuales técnicos.

- INTEGRIDAD DE LAS TABLAS ARTÍCULOS, ARTÍCULOS_TEMP., AUTOMÓVILES Y AUTOMÓVILES_TEMP DE LA BASE DE DATOS DEL SISTEMA INTEGRAL DE CONTROL ADMINISTRATIVO DEL DESTINO DE BIENES (SICADEB).

4.- INFRAESTRUCTURA DE EQUIPO DE CÓMPUTO.

- Inventario de Bienes Informáticos.
- Ubicación del Centro de Cómputo (Site de Servidores)
- Red de Datos y su Administración..

5.- ESQUEMA DE SEGURIDAD.

- Esquema de Seguridad informático, incluyendo centro de cómputo (Site de Servidores) y Red de Datos.

III. RESULTADO DEL TRABAJO DESARROLLADO.

Derivado del trabajo de revisión se determinó 1 observación relevante que a continuación se describe:

METODOLOGÍA DE DESARROLLO DE SISTEMAS

De la documentación de los 12 módulos en operación que integran el SICADEB, así como de los tres sistemas independientes (Subsistema de Talismán, Oficios de Salidas y el Sistemas de Información Estratégica), proporcionados por la Dirección de Informática, no se localizo la Lista de eventos, los Diagramas de Causa-Efecto, el Diagrama de Contexto, el Diagrama de Flujo de Datos (DFD) y los Diagramas de Transición de Estados (DTE), mismos que deberían existir en la documentación técnica, de acuerdo a la Metodología de Desarrollo de Sistemas establecida por el Área de Informática.

IV. CONCLUSIÓN Y RECOMENDACIÓN GENERAL.

De la revisión practicada a la Dirección de Informática de la Dirección General del Destino de los Bienes de Comercio Exterior Propiedad del Fisco Federal, se desprende que los registros y controles establecidos sobre la Tecnología de Información son adecuados; sin embargo, se detectaron inconsistencias en la Metodología de Desarrollo de Sistemas, por lo que es importante que el área informática realice de inmediato las siguiente recomendaciones:

La Dirección de Informática deberá complementar la documentación técnica de los sistemas en producción, a fin de contar con toda la información para su mantenimiento y cumplir con todos los aspectos que contempla en su metodología de desarrollo de sistemas; así como, mantener actualizada la documentación técnica y los manuales de usuario de sus sistemas.

Es importante que la Dirección de Informática lleve a cabo la instrumentación de las medidas correctivas y preventivas plasmadas en el informe de referencia, a fin de promover la eficiencia y eficacia en el uso y administración de la Tecnología de Información utilizada en la Dirección General del Destino de los Bienes de Comercio Exterior Propiedad del Fisco Federal; al mismo tiempo, deberá de reforzar los controles internos establecidos para evitar la recurrencia de las observaciones detectadas.

V. OBSERVACIONES.

OBSERVACIÓN

La Dirección de Informática no documenta en su totalidad los puntos descritos en su metodología para el desarrollo de sistemas.

De la documentación de los 12 módulos en operación que integran el SICADEB, así como de los tres sistemas independientes (Subsistema de Talismán, Oficios de Salidas y el Sistemas de Información Estratégica), proporcionados por la Dirección de Informática, no se documenta la totalidad de los puntos descritos en la Metodología de Desarrollo de Sistemas establecida por el Área (Proyecto de Análisis y Diseño de Sistemas), ya que no se encontraron los siguientes aspectos:

- ⇨ Lista de eventos
- ⇨ Diagramas Causa-Efecto
- ⇨ Diagrama de Contexto
- ⇨ Diagrama de Flujo de Datos (DFD)
- ⇨ Diagramas de Transición de Estados (DTE)

FUNDAMENTO LEGAL: Manual de Políticas y Lineamientos para el Aprovechamiento y Cuidado de los Elementos de Tecnologías de la Información de la SHCP

RECOMENDACIONES

La Dirección de Informática deberá complementar la documentación técnica de los sistemas en producción, a fin de contar con toda la información para su mantenimiento y cumplir con todos los aspectos que contempla su metodología de desarrollo de sistemas.

Asimismo, la Dirección de Informática deberá mantener actualizada la documentación técnica y los manuales de usuario de sus sistemas en caso de que estos sufran algún cambio o se generen versiones nuevas.

FECHA COMPROMISO

Se acepta la observación y recomendaciones de la Contraloría Interna (Fecha y firma por el responsable del Área de Informática)

_____

Nombre y puesto

Anexo

Formato de Cuestionarios

La elaboración de los formatos del cuestionario "Evaluación de la metodología" que a continuación se presentan se realizaron basándose en los aspectos mínimos con los que debe contar una metodología de desarrollo de sistemas[5]

La elaboración de los formatos del cuestionario "Integridad, confiabilidad y seguridad de la base de datos y sistemas de información" se desarrollaron basándose en fundamentos y modelos de bases de datos.

[5] Metodología basada en Structured Systems Análisis and Design Meted (SSADM)

FORMATO DE CUESTIONARIOS

CUESTIONARIO PARA LA EVALUACIÓN DE LA METODOLOGÍA.

NOMBRE:_____ PUESTO:_____

ÁREA:_____ FECHA: ____/____/____

Instrucciones: **Conteste con veracidad y tan ampliamente como lo considere necesario, cancelando los espacios que no utilice. Use tinta azul o negra, además** deberá rubricar cada una de las páginas y firmar en la última.

1. ¿ Existe una metodología para el desarrollo de los sistemas?

SÍ ( ) NO( ) ¿Por qué?

2. Liste los puntos que cubre la metodología.

3. ¿Con base a qué criterios fue desarrollada la metodología?

4. ¿En que porcentaje considera que es conocida en el área de sistemas?

5. ¿ La metodología establecida es realizada en un 100%?

SÍ( ) NO( ) ¿Por qué?

6. ¿ Es flexible en algunos puntos?

SÍ( ) ¿Cuáles? NO( ) ¿Por qué?

CUESTIONARIO PARA LA EVALUACIÓN DE LA METODOLOGÍA.

7. ¿ La metodología incluye consideraciones para controlar los cambios que podrían ocurrir durante el ciclo de vida del sistema?

SÍ( ) ¿Cuáles? NO( ) ¿Por qué?

8. ¿ La metodología ha tenido modificaciones?

SÍ ( ) ¿Cuáles? NO( ) ¿Por qué?

9. ¿ La metodología incluye el reconocimiento formal de grupos de trabajo, por ejemplo usuarios, sistemas, seguridad, control, etc., y sus respectivas responsabilidades?

SÍ( ) ¿Cuáles? NO( ) ¿Por qué?

10. ¿Qué adecuaciones realizaría en la metodología vigente?

FIRMA DE CONFORMIDAD

CUESTIONARIO PARA LA EVALUACIÓN DE LA ETAPA DE ANÁLISIS, DESARROLLO, IMPLANTACIÓN Y MANTENIMIENTO DE SISTEMAS

NOMBRE:_____ PUESTO: _____

ÁREA:_____ FECHA: _____/_____/_____

Instrucciones: **Conteste con veracidad y tan ampliamente como lo considere necesario, cancelando los espacios que no utilice. Use tinta azul o negra, además** deberá rubricar cada una de las páginas y firmar en la última.

ETAPA DE ANÁLISIS

1.- ¿Se realizan las siguientes actividades de análisis, previas al inicio de un Sistema?: (Escriba SÍ o NO).

- ¿Reunión con usuarios?..... ( )
- ¿Especificación de requerimientos?..... ( )
- ¿Se determinan los requisitos de la información?..... ( )

2.- ¿ Cómo considera la participación del usuario durante el desarrollo del proyecto ?

( ) Poca 10% - 30%
( ) Considerable 70%
( ) Otra. Especifique:
( ) media 40% - 50%
( ) activa 100%

3.- ¿ Se integran grupos de trabajo para el análisis y elaboración del modelo del sistema?

SÍ( )¿Quiénes integran estos grupos? NO( ) ¿Por qué?

4.- Enumere los pasos que siguen para la aprobación formal del proyecto.

5.- ¿Cuándo el modelo del sistema es aprobado, que pasos se siguen para la planeación del mismo?

CUESTIONARIO PARA LA EVALUACIÓN DE LA ETAPA DE ANÁLISIS, DESARROLLO, IMPLANTACIÓN Y MANTENIMIENTO DE SISTEMAS

6.- ¿Se llevan a cabo reuniones para dar seguimiento a los avances del proyecto?

Si ( )
- ¿Quiénes participan y con que periodicidad se realizan?

No ( )
- ¿Cómo se realiza el seguimiento?

ETAPA DE DESARROLLO

7.- Durante la etapa de desarrollo se elaboran aspectos tales como:

• Diagramas Causa-Efecto	SI( )	NO( )
• Diagramas de flujo de datos (DFD).	SI( )	NO( )
• Diagramas de transición de estados(DTE).	SI( )	NO( )
• Diagrama de Entidad-Relación	SI( )	NO( )
• Diccionario de Datos	SI( )	NO( )
• Otros		

IMPLANTACIÓN

8.- Se realizan pruebas periódicas con él (los) usuario (s) para conocer el grado de avance del sistema?

SÍ( ) ¿De que tipo? NO( ) ¿Por qué ?

9.- Mencione el procedimiento que realizan una vez que el sistema es aprobado por él (os) usuario (s)?

10.- Realiza cursos de capacitación referentes al nuevo sistema?

SÍ( ) NO( ) ¿Por qué ?

CUESTIONARIO PARA LA EVALUACIÓN DE LA ETAPA DE ANÁLISIS, DESARROLLO, IMPLANTACIÓN Y MANTENIMIENTO DE SISTEMAS

11.- Realiza el manual de usuario del(os) Sistema(s)?

SÍ( ) NO( )¿Por qué?

12.- Existe una entrega formal de manuales de usuario?

SÍ( ) ¿De que tipo? NO( )¿Por qué?

13.- Liste de manera general el contenido de los manuales de usuario que ha elaborado:

14.- ¿ Se realizan pruebas de control de calidad al(os) Sistema(s) que garanticen el funcionamiento correcto del (los) Sistema(s), antes de su liberación?

SÍ( ) Especifique el área encargada de llevarlas a cabo NO( ) ¿Por qué ?

15.- ¿Están definidas las pruebas de control de calidad?

SÍ( ) ¿Cuáles son? NO( )¿Por qué?

16.- ¿Son revisadas las pruebas y existe documentación de estas revisiones?

SÍ( ) NO( )

CUESTIONARIO PARA LA EVALUACIÓN DE LA ETAPA DE ANÁLISIS, DESARROLLO, IMPLANTACIÓN Y MANTENIMIENTO DE SISTEMAS

17.- Existe documentación técnicas de los sistemas en producción?

SI ( ) NO ( ) ¿Por qué?

18.- Liste de manera general en que consiste la documentación técnica:

ETAPA DE MANTENIMIENTO

19.- ¿ Existe un procedimiento por escrito para solicitar cambios o modificaciones al sistema?

SÍ( ) NO( ) ¿Por qué?

20.- ¿ Existe una relación autorizada de personas facultadas para solicitar cambios?

Si ( ) ¿Qué datos contiene ésta relación? No ( )¿ Por qué ?

21.- ¿ Se lleva un registro por escrito de los cambios realizados a los sistemas?

SÍ( ) NO( ) ¿Por qué?

CUESTIONARIO PARA LA EVALUACIÓN DE LA ETAPA DE ANÁLISIS, DESARROLLO, IMPLANTACIÓN Y MANTENIMIENTO DE SISTEMAS

22.- La documentación de mantenimiento del sistema incluye:

Requisitos del cambio	SÍ( )	NO( ) ¿Por qué?_____
Aprobación de la modificación.	SÍ( )	NO( ) ¿Por qué?_____
Descripción de la modificación	SÍ( )	NO( ) ¿Por qué?_____
Actualización a los diagramas de flujo	SÍ( )	NO( ) ¿Por qué?_____
Documentación de los resultados de prueba.	SÍ( )	NO( ) ¿Por qué?_____
Aceptación del usuario.	SÍ( )	NO( ) ¿Por qué?_____

_____

FIRMA DE CONFORMIDAD

INTEGRIDAD, CONFIABILIDAD Y SEGURIDAD DE LA BASE DE DATOS Y SISTEMAS DE INFORMACIÓN

NOMBRE:_____ PUESTO:_____

ÁREA:_____ FECHA: ____/_____/_____

Instrucciones: **Conteste con veracidad y tan ampliamente como lo considere necesario, cancelando los espacios que no utilice. Use tinta azul o negra, además** deberá rubricar cada una de las páginas y firmar en la última.

ESPECIFICACIÓN DEL SISTEMA MANEJADOR DE BASE DE DATOS (SMBD)

1.- ¿Cuál es el manejador de bases de datos que utiliza?

_____

_____

2.- ¿Conoce las utilerías, funciones, procedimientos, etc. con que cuenta dicho manejador para mantener la integridad de la información?

SÍ ( ) ¿Cuáles son? No ( ) ¿Por qué?

_____

_____

_____

3.- ¿Cuáles son las utilerías y/o funciones más utilizadas en el área?

_____

_____

_____

_____

_____

4.- ¿Cuál es la estructura de la Base de Datos?

Centralizada ☐

Relacional ☐

Otra ☐ Especifique_____

_____

5.- ¿Se cuenta con procedimientos o políticas para la operación y acceso al manejador de la Base de Datos?

Sí ____ ¿Cuáles son? No ____ ¿Por qué?

_____

_____

_____

_____

INTEGRIDAD, CONFIABILIDAD Y SEGURIDAD DE LA BASE DE DATOS Y SISTEMAS DE INFORMACIÓN

6.- ¿Cuáles herramientas o utilerías tiene el Manejador de la Base de Datos que utiliza?

_____
_____
_____
_____

Integridad en la información de la base de datos

7.- Dentro de los procedimientos para el desarrollo de sistemas se contempla:

	SÍ	NO
Procedimientos de Prueba formales	☐	☐
Integridad del Código fuente y ejecutable	☐	☐
Área reservada para pruebas	☐	☐
Pistas de auditoría	☐	☐
Control de versiones	☐	☐

8.- ¿Existe algún grupo (área usuaria o informática) que controle los datos que serán introducidos en las pantallas de los sistemas en desarrollo y/o mantenimiento?

Sí ____ ¿Cuál y de que forma? No ____ ¿Por qué?

_____
_____
_____

9.- ¿Qué tipos de controles están establecidos para la validación de la entrada de datos en los módulos del SICADEB?

_____
_____
_____
_____
_____

10.- ¿Qué procedimientos contempla para validación de datos, y en que etapa del proyecto son considerados?

_____
_____
_____
_____

CONFIDENCIALIDAD DE LA INFORMACIÓN EN LA BASE DE DATOS

Protección de datos

11.- ¿Cómo administrador cuáles son los principales procesos que atiende en relación a las Base de Datos (desbloqueo de registros, generación de queries, etc)?

INTEGRIDAD, CONFIABILIDAD Y SEGURIDAD DE LA BASE DE DATOS Y SISTEMAS DE INFORMACIÓN

Proceso	Area solicitante	Frecuencia

Esquema de seguridad

12.- El equipo para el desarrollo de sistemas está protegido contra:

	SÍ	NO
Robo	☐	☐
Acceso no autorizado	☐	☐
Contingencias	☐	☐
Perdida de información	☐	☐
Modificación de información	☐	☐
Daños físicos	☐	☐

13.- ¿En que documentos se soportan estos controles de seguridad?

14.- El lugar donde se realiza el desarrollo de sistemas está restringido o controlado en sus accesos?

SÍ ____ ¿De que forma? No ____ ¿Por qué?

15.- Dentro el análisis de los sistemas, ¿qué procedimientos de autorización se tienen establecidos?

	SÍ	NO
Equipo restringido	☐	☐
Niveles de seguridad preasignados	☐	☐
Autenticación de usuarios	☐	☐
Verificación de permisos	☐	☐
Niveles de autorización en el manejo de sistemas como sólo lectura, adiciones, y Modificaciones.	☐	☐

Otros _____

INTEGRIDAD, CONFIABILIDAD Y SEGURIDAD DE LA BASE DE DATOS Y SISTEMAS DE INFORMACIÓN

16.- Se han considerado algunos mecanismos de protección contra la intersección o la penetración en la transmisión o intercambio de los datos que existen entre el sistema de Talismán y el SITE de servidores ubicado división del norte?

SÍ ____ ¿De que forma? No ____ ¿Por qué?

17.- ¿Qué componentes de auditabilidad (pistas de auditoría) se contemplan en el SICADEB?

CONFIABILIDAD DE LA INFORMACIÓN DE LA BASE DE DATOS

Procedimientos de entrada de datos

18.- ¿Existen procedimientos y políticas para la administración de las claves de acceso a los sistemas para el usuario final?

SÍ ____ ¿Cuáles son? NO ____ ¿Por qué?

19.- ¿Existen procedimientos escritos donde se explique al usuario los procedimientos de captura y verificación de la información que se ingresa al SICADEB?

SÍ ____ ¿Cuáles son? NO ____ ¿Por qué?

Controles de la base de datos

20.- Mencione ¿De qué forma se previene que la información capturada en el SICADEB no se duplique?

INTEGRIDAD, CONFIABILIDAD Y SEGURIDAD DE LA BASE DE DATOS Y SISTEMAS DE INFORMACIÓN

21.- ¿Cuenta la Base de Datos del SICADEB con las validaciones necesarias que aseguren que la información sea íntegra y confiable?

SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN

Desarrollo y mantenimiento de sistemas

22.- ¿Qué requiere un usuario para accesar al sistema?

23.- ¿Cómo se identifica un usuario?

24.- ¿ Qué privilegios tienen los usuarios y como los determinan?

25.- ¿Se registra en un archivo o campo los siguientes datos de acceso a los Sistemas?

Datos del registro accesado	( )
Clave personal del usuario que accesa el registro	( )
Hora y fecha en que se acceso el registro	( )
Datos de modificación del registro en caso de existir	( )
Hora de inicio y finalización de una sesión de trabajo	( )

CONTROL DE ACCESO A LOS SISTEMAS

26.- ¿Los sistemas cuentan con una facilidad que permita el registro de los usuarios que los accesan?

SÍ ( ) No ( )

INTEGRIDAD, CONFIABILIDAD Y SEGURIDAD DE LA BASE DE DATOS Y SISTEMAS DE INFORMACIÓN

27.- ¿Existen claves personalizadas por cada uno de los usuarios de los sistemas?

Sí ( ) No ( )
¿Por qué?

28.- ¿De qué tipo es el control de acceso?

Clave de acceso a la aplicación (Password) ( )
Archivo histórico de acceso a la aplicación ( )
Archivo histórico de acceso a registros ( )

29.- ¿Existe una relación de usuarios autorizados para accesar a los sistemas?

Sí ( ) No ( )
¿Por qué?

SEGURIDAD LOGICA DE LOS SISTEMAS.

30.- ¿ Existen procedimientos establecidos para el control del mantenimiento (modificación de tablas, programas, menús, etc.) del SICADEB ?

SI ( ) NO ( )
¿Por qué?

FIRMA DE CONFORMIDAD

Bibliografía

BIBLIOGRAFÍA

PÁGINA WEB DEL SERVICIO DE ADMINISTRACIÓN TRIBUTARIA (SAT)
http:\www.sat.gob.mx

PÁGINA WEB DE LA CONTRALORÍA INTERNA EN LA SHCP
http:\www.ci.shcp.gob.mx

PÁGINA WEB DE LA SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO (SHCP)
http:\www.shcp.gob.mx

PROGRAMA ESPECÍFICO DE LA REVISIÓN DE SISTEMA
CONTRALORÍA INTERNA EN LA S.H.C.P.
"AUDITORÍA DE SISTEMAS"

PROGRAMA DE MODERNIZACIÓN DE LA ADMINISTRACIÓN PÚBLICA.

MANUAL DE ORGANIZACIÓN DE LA DIRECCIÓN DE AUDITORÍA DE SISTEMAS Y SERVICIOS INFORMÁTICOS. PUBLICADO POR LA CONTRALORÍA INTERNA EN LA SHCP.

MARIO G. PIATTINI
EMILIO DEL PESO
AUDITORÍA INFORMÁTICA UN ENFOQUE PRÁCTICO
ALFAOMEGA, 1998

ADORACIÓN DE MIGUEL
MARIO PIATTINI
FUNDAMENTOS Y MODELOS DE BASES DE DATOS
ALFAOMEGA 2DA. EDICIÓN, 1999.

MARIO G. PIATTINI, JOSÉ A. CALVO MANZANO, JOAQUÍN CERVERA Y LUIS FERNÁNDEZ
ANÁLISIS Y DISEÑO DETALLADO DE APLICACIONES INFORMÁTICAS DE GESTIÓN
ALFAOMEGA, 2000

A., SENN, JAMES
ANÁLISIS Y DISEÑO DE SISTEMAS DE INFORMACIÓN
MC GRAW-HILL, SEGUNDA EDICIÓN, 1992.

KENDALL, E., KENNETH
KENDALL, E., JULIE
ANÁLISIS Y DISEÑO DE SISTEMAS
PRENTICE-HALL, HISPANOAMERICANA, S.A. 1991

YANN DERRIEN
TÉCNICAS DE LA AUDITORÍA INFORMÁTICA
MARCOMBO, 1994

PILAR GÓMEZ MIRANDA
FERNANDO VÁZQUEZ TORRES
FRANCISCO JAVIER ALVAREZ SOLÍS
AUDITORÍA Y SEGURIDAD INFORMÁTICA
SPANTA, 1998

FAIRLEY, RICHARD,
INGENIERÍA DE SOFTWARE
MC GRAW HILL, INC., U.S.A. , 1985