Propuesta de implantación del área de auditoría en informática en un órgano legislativo

Seminario de auditoría en informática, informe de titulación

Yuritzin Aguirre Sánchez

Propuesta de implantación del área de auditoría en informática en un órgano legislativo: Seminario de auditoría en informática, informe de titulación

Yuritzin Aguirre Sánchez

Tabla de contenidos

Lista de figuras

Lista de tablas

Resumen

El vertiginoso avance tecnológico ha incrementado cada vez más la dependencia de las tecnologías de información en las instituciones mexicanas, el crecimiento de este fenómeno aumentan también los riesgos informáticos a los que se enfrentan; derivado de esta problemática se desarrolla el presente informe de seminario de titulación, en el cual se propone la implantación de del área de auditoría en informática dentro del Órgano Interno de Control de la Cámara de Diputados, siendo éste el encargado de la labor legislativa del país, en sus manos está en buena parte el futuro de la población, es por ello de singular importancia dotarla de las herramientas y mecanismos necesarios que la fortalezcan cada vez más.

No de forma idealista, sino más bien proactiva, se trata de comenzar a cambiar la situación de México desde su parte más fuerte, dentro del poder legislativo; introduciendo nuevas formas del quehacer gubernamental; para ello, se determina analizar la Cámara de Diputados del H. Congreso de la Unión, de esto se detecta que a pesar de que la Dirección General de Tecnologías de Información de la Cámara de Diputados crece y se moderniza constantemente atendiendo a los requerimientos propios de esta Institución, a la fecha su Órgano Interno de Control (Contraloría Interna) no cuenta con un área que realice las funciones de auditoría en informática, misma que se encargue de constatar que se sigan procedimientos que aseguren la confidencialidad, confiabilidad y disponibilidad de los datos, garanticen la seguridad de la información y prevean las posibles contingencias en cuanto a la seguridad de la información que se maneja en este órgano, misma que por definición es muy delicada, asimismo que regule la gestión de la infraestructura y que en general se dedique a guiar el desarrollo y correcto funcionamiento del área de sistemas de esta Institución mediante las auditorías correspondientes.

En este informe se realiza un análisis por medio de cuestionarios, entrevistas y visitas para conocer estas áreas y la investigación de las posibles herramientas que ayudarían en su desarrollo; asimismo un estudio de costo beneficio y de factibilidad, una estimación de los gastos que se llevarían a cabo en la realización de la propuesta de la implantación de un área de auditoría en informática en el Órgano Legislativo, así como la comparación de costos de las diferentes propuestas de software (CAAT por sus siglas en ingles) y mejores prácticas que pudieran ser adaptadas a las necesidades de la Contraloría Interna.

Se realiza un cuadro comparativo de las diferentes mejores prácticas y herramientas automatizadas con sus características respectivas, así como sus costos y cual es la que más se adapta a las necesidades específicas del área. En cuanto a la inversión a largo plazo se hace un análisis del costo de las existentes certificaciones de auditores en informática que cumplen con las características que se necesitan. Mientras que en el estudio de factibilidad se presentan todas las posibles ventajas para el órgano, sin descuidar ninguno de los elementos necesarios para que el proyecto funcione.

Este informe comprende también el análisis de estándares de la auditoría informática que puedan ser aplicados en el área, éstos son de suma importancia, ya que además de haber sido establecidos por organizaciones internacionales, son actualmente utilizados a nivel mundial y proporcionan a las organizaciones e instituciones que los aplican un mejoramiento en el aseguramiento de la información y de los activos informáticos, mediante la actualización de sus procesos.

En cuanto al estudio de los CAAT, se determina que aún sin la creación de un área de auditoría en informática, la implantación de una técnica de auditoría en informática en la Contraloría Interna sería de gran utilidad para el desempeño del trabajo actual, ya que el auditor se ve obligado, dependiendo del alcance de la auditoría, a recabar información de todos los recursos posibles, lo cual puede realizar con suma facilidad con los programas de auditora informática. En este informe de seminario se describen las técnicas para analizar programas, como se planifica la selección de una CAAT, cuales son los factores a tomar en cuenta al utilizar una de estas herramientas y los pasos para una adecuada selección de la misma. También se hace mención de como utilizar una CAAT una vez seleccionada, es decir la metodología en la realización de una auditoría (incluyendo papeles de trabajo e informes). Para complementar este estudio se realizaron diversas demostraciones al personal de la Contraloría Interna por parte de las empresas de las herramientas actualmente existen en el mercado y que mejor se adaptan a las necesidades específicas del área, de las cuales se realizaron cuestionarios a los auditores para

conocer su opinión en cuanto a cuáles son sus expectativas de cada producto y cuál les parece más conveniente adaptar al área.

De igual forma, se realiza un estudio de las diversas normas, técnicas y procedimientos de auditoría en informática, con el fin de poder seleccionar las más apropiadas. Es fundamental mencionar que para el auditor en informática, el conocer los productos de software que han sido creados para apoyar su función aparte de los componentes de la propia computadora resulta esencial para facilitar el manejo de la información.

También se mencionan los diversos procedimientos de auditoría en informática, los cuales permiten al auditor obtener información, analizar las características, verificar los resultados y fundamentar las conclusiones de la auditoría.

Para la propuesta de implantación del área de auditoría en informática, se presentan los pasos que se consideran necesarios para crearla, el primer paso se refiere a conocer los requisitos óptimos que el proyecto requiere en cuanto a estructura se refiere, como son el cambio en la estructura orgánica, objetivo, misión, visión y funciones ya que estos elementos son necesarios para que las actividades se realicen con eficiencia y las metas del área se cumplan. El segundo paso consiste en un estudio de requisitos mínimos del personal que son necesarios para que el proyecto logre obtener las metas y objetivos establecidos, y por último se propone la implantación concreta de una mejor practica para la gestión de tecnologías de información y de una CAAT que se adapte al 100% a las características de esta área, en este paso se trata de hacer uso de los recursos disponibles de la empresa para minimizar cualquier gasto o adquisición adicional mostrando así gráficamente los gastos y los beneficios que conlleva la puesta en marcha de el área.

Por lo cual se concluye que la implantación de un área de auditoría en informática dentro de la Contraloría Interna de la Cámara de Diputados, no sólo resulta benéfico sino indispensable, ya que aportará los elementos necesarios para que sea capaz de afrontar el reto de modernizar a este órgano, fundamentalmente con la participación de profesionales calificados, aplicación de los estándares mundiales, uso de herramientas de auditoría asistidas por computadora y la renovación de las funciones de la Contraloría Interna. Para lo cual adicionalmente a la formación en sí del área, se propone específicamente la metodología, técnicas de auditoría asistidas por computadora, mejores prácticas y demás herramientas en auditoría en informática de las que podrá hacer uso el área de auditoría en informática, con lo que en concreto se pretende que mejore considerablemente su rendimiento, eficacia, eficiencia y calidad en el trabajo que redunde por supuesto en lo que más quiere el pueblo mexicano, la utilización óptima de los recursos públicos que redunde en rendición de cuentas claras y transparentes.

Summary

Innovation and technological pace have caused that Mexican institutions are more dependant on information technology. This fact has incremented the related information technology risks that these institutions face; due to this situation, this paper has been prepared to show how an IT audit organization, might be implemented in the Control Intern Organism (CIO) of the Mexican Congress. This organism is responsible for all of the legislation work in the country. This is an important aspect, because part of the future of this country lies in their hands, that is why is very important to provide them with the tools and appropriate mechanisms to leverage their work.

Not in an ideal way, but using more proactive actions, it has to do with changing the status quo within its most important face, the legislative powefr; introducing new forms of government practices; To do that, it's determinant to analyze every aspect of the organization. Due to this analysis, it's important to notice that the Direction of Technology and Information of this organism leverages its potential constantly, attending the normal requirements. These days, the CIO (Contraloría Interna) doesn't have an organization that leads the audit practices in IT. The mission of this audit organization would be ensuring that all of the procedures related to information management, such as confidentiality and availability will be met. It's also important to manage the risks related to information security, manage the back out plans and disaster recovery plans to handle information. Due to the nature of the information that is being handled, it is necessary to control IT infrastructure. Another mission would be to guide the development and direction of the IT organization.

This analysis is based on checklists, interviews, on site visits, all of these activities lead to know the different areas and the research of tools that might help them; we built a business case, with a benefit-cost analysis attached, and the P&L analysis to know the aspects that the new IT audit organization requires. A comparative analysis about the software tools for audit processes has also been prepared, and a research about best practices that can be used and adapted.

A comparative matrix is being presented to show the different best practices and automated tools that are available, with their capabilities and costs. Covering the long term investments, the paper presents a cost analysis about the different commercial certifications in audit practices, outlining the benefits to the organism, without putting aside the practical elements to take this project to be up and running.

This paper also covers the analysis of IT audit standards. These standards are very important, because they have been created by international organisms, and they are used broadly, and provide benefits that can be measured with process improvement methods and information and asset management practices.

About CAAT's, it's determined that even without creating an IT audit organization, the use of an audit technique would be very useful to improve actual work, because a former audit person needs to retrieve information using all of the resources available, but using a software tool it is easier. In this paper, we present some techniques that can be used to analyze the tools, how to select a CAAT, how to use it once it is chosen. We also present how to use a methodology with a tool, including all of the paperwork and reports. As a complementary report, we show different demonstrations to the personnel of internal auditing, guided by the actual companies that distribute the tools in the market. As an extra activity we applied questionnaires to audit personnel to know their opinions and recommendations about each tool and to know what they state as the most convenient feature for each area.

A study about different techniques and procedures to conduct an IT audit is also presented, in order to select the most appropriate to the organism. It's important to mention that the IT audit people should know the software tools that have been developed and have a clear understanding of IT concepts.

It's also mentioned that there are different procedures in IT audit, in order to provide information, gather characteristics, show the results and leverage the conclusions.

In this paper we present the necessary steps to build an IT audit area from scratch. The first step is related to the necessary structure and requirements, strategic planning, mission, objectives, vision, functional charts, etc. The second step is related to gather the correct people skills and human resources to score

the desired results. As a third step, we recommend to define an IT management strategy and a tool that meets the requirements at a 100%.

As a conclusion we state that the implementation of an IT audit area within the internal auditing area of the Mexican's Congress is not only suggested but it is necessary, because it will provide the appropiate elements so the organism is capable of facing the challenge to bring the organism to new and modern status quo, including qualified professionals, international standards, automated audit tools, best practices. These set of elements must enhance the overall performance of the organism, with key indicators such as efficiency, quality, service level, etc. The use of these key performance indicators will contribute to a transparent and optimal use of public resources, because that is what all of Mexican people ask for.

Introducción

A lo largo de este informe de seminario de titulación, se propone la implantación del área de auditoría informática dentro de la Contraloría Interna de la H. Cámara de Diputados, ya que no obstante de que este Órgano tiene 10 años de creación, a la fecha no se cuenta con ésta ni con las funciones dedicadas específicamente a las IT; este es el motivo que motivó la realización de este informe.

Para ello, se comienza por dar una semblanza de los antecedentes, conformación y legislación de la Cámara de Diputados; a fin de que se comprenda cuál es la ubicación del Órgano Interno de Control (Contraloría Interna) dentro de esta institución, dentro de su estructura se encuentra a la Subcontraloría de Auditoría, ésta última objeto de este estudio.

De ésta última se realiza un análisis y se comienza por sus aspectos generales para terminar con el estudio de sus particularidades a fin de fundamentar esta investigación.

En seguida se analiza el área de sistemas del Órgano, en este caso la Dirección General de Tecnologías de Información, de la misma forma que con el Órgano Interno de Control se analiza de lo general a lo particular.

En seguida, se proporciona toda la investigación y análisis correspondiente de las actuales herramientas informáticas y manuales que pueden ser usadas por los auditores, las mejores prácticas y demás estrategias que puedan auxiliar a los empleados de la Contraloría Interna y así contribuir con la mejor rendición de cuentas y cumplimiento a las actuales leyes de transparencia y acceso a la información pública gubernamental.

Para concluir, se proporcionan las recomendaciones de cómo deberá estar conformada el área de auditoría en informática de acuerdo a la magnitud del área de sistemas; los pasos que se consideran necesarios seguir para su implantación y por último de todas las herramientas estudiadas, se hace una propuesta de aquella que esté más acorde a las funciones y características tanto de la Subcontraloría de Auditoría como del área de sistemas del Órgano.

Es importante mencionar que el presente informe de seminario de titulación tiene un sentido preventivo por muchas razones, entre ellas: la creciente importancia de mantener seguros los activos informáticos y en particular los datos (tanto del área de la Contraloría Interna como del área de Sistemas); ya que si bien la información es intangible, ésta representa el elemento fundamental que sirve de base para el correcto desarrollo de todas las funciones dentro de la H. Cámara de Diputados.

Por otro lado, la reciente creación e implantación de la Ley Federal de Acceso a la Información Pública Gubernamental obliga en el mediano plazo a todos los órganos de control de gobierno a mejorar, actualizar y modernizar sus mecanismos de revisión y control.

Así, en este informe se plantea la problemática a la que hoy día se enfrenta la Subcontraloría de Auditoría de la H. Cámara de Diputados, cuáles son sus riegos y oportunidades, y se fundamenta plenamente las recomendaciones hechas en cuanto a la implantación de IT dentro del área y diferentes recursos, así como capacitación de personal y actualización de la legislación existente.

Capítulo 1. Descripción del órgano legislativo y de su organo interno de control

En este capítulo se da un vistazo a la historia y conformación de la Cámara de Diputados; asimismo se ubica en qué contexto se encuentra el Órgano de Control Interno y su respectiva área de Auditoría, estructura, objetivos, funciones y la normatividad con la que actualmente se maneja. Lo anterior, a fin de dar un panorama claro de qué es y a qué se dedica, principalmente enfocado a estudiar la Subcontraloría de Auditoría, de esta forma, se encuentra en este apartado el punto de partida de nuestro estudio.

H. Cámara de Diputados

Las paredes de la H. Cámara de Diputados pueden relatar una larga historia de triunfos y fracasos, pero sobretodo de cambios y transformaciones constantes que la han convertido en lo que hoy día es, a continuación se da un repaso de qué es, para qué es y por qué fue creada a H. Cámara de Diputados y como llego a conformarse la Contraloría Interna como órgano de control dentro de este órgano hace 10 años:

"El pueblo ejerce su soberanía por medio del Congreso de la Unión"[1] , éste representa la conformación del Poder Legislativo de los Estados Unidos Mexicanos, mismo que se deposita en dos Cámaras, una de Diputados y otra de Senadores, las cuales ejercen las facultades que la propia Constitución les confiere.

Antecedentes

Poca gente sabe que el 24 de febrero de 1822, el México Independiente tuvo a la Iglesia de San Pedro y San Pablo como el primer escenario del Poder Legislativo, donde nace la primera Cámara de Diputados y el primer Congreso Constituyente en México.

En 1823 el Congreso Constituyente comenzó a esbozar la idea de que el Poder Legislativo se compusiera por dos Cámaras: una integrada con base en el número de habitantes y otra formada por igual número de representantes de los nacientes estados, Diputados y Senadores, respectivamente.

En este mismo año, Fray Servando Teresa de Mier concibe la idea del bicameralismo dando lugar a la creación del Honorable Congreso de la Unión que se plasmó en el Acta Constitutiva de la Federación, que fue la ley fundamental mexicana y base de la creación de la Constitución Política de los Estados Unidos Mexicanos, que ha pasado por innumerables modificaciones hasta llegar a lo que hoy día se conoce como nuestra Carta Magna.

En 1981 se inauguró la construcción de lo que hoy es la sede de la Cámara de Diputados, con sólo 24 años de existencia las paredes de este recinto pueden contar una larga trayectoria de triunfos y fracasos.

Como dato curioso mencionar que las distintas instalaciones que ha tenido la Cámara de Diputados a lo largo de este período han sido incendiadas por lo menos tres veces, a causa de los diferentes movimientos políticos y sociales que se han dado en México.

Nuestro estudio empieza aquí y, no de forma idealista ni inocente este informe trata de comenzar a cambiar la situación de México desde su parte más fuerte, dentro del poder; introduciendo nuevas formas de ver el gobierno.

[1]Constitución Política de los Estados Unidos Mexicanos, Título Segundo, Capítulo 1.- «De la Soberanía Nacional y de la Forma de Gobierno», Artículo 41.

La Cámara de Diputados está compuesta por 500 Diputados, mismos que son los representantes de la Nación electos en su totalidad por la ciudadanía mexicana; divididos en: 300 elegidos, según el principio de votación mayoritaria relativa, mediante sistemas de distritos electorales y 200 según el principio de representación proporcional, mediante el sistema de listas regionales, votadas en 5 circunscripciones plurinominales.

Legislación

En México, nuestra carta magna, habla de la división de poderes para su ejercicio: Legislativo, Ejecutivo y Judicial; el poder legislativo en nuestro país consiste en la elaboración, estudio y aprobación de las leyes que regulan nuestro territorio a nivel nacional, asimismo la *Constitución Política de los Estados Unidos Mexicanos*, establece que "el Poder Legislativo se deposita en un Congreso General, que se divide en dos Cámaras, una de Diputados y otra de Senadores"[2].

La Cámara de Diputados es, por tanto, uno de los dos Órganos Legislativos que está encargado de brindar representatividad a la población de todo el país, por medio del ejercicio del poder legislativo, mediante los 500 diputados que la conforman. Los artículos 51 al 79[3]establecen detalladamente la conformación, funciones, ejercicio, facultades compartidas y exclusivas, etc. de estos dos Órganos, las cuales no se menciona por no ser el objeto de nuestro estudio.

Órganos de gobierno y estructura técnica y administrativa

Como está plasmado en el Estatuto de la Organización Técnica y Administrativa y del Servicio de Carrera de la Cámara de Diputados, ésta cuenta con cuatro Órganos de Gobierno:

- Pleno.
- Mesa Directiva.
- Conferencia para la Dirección y Programación de los Trabajos Legislativos.
- Junta de Coordinación Política.

Y por lo que respecta a la organización técnica y administrativa, está integrada por:

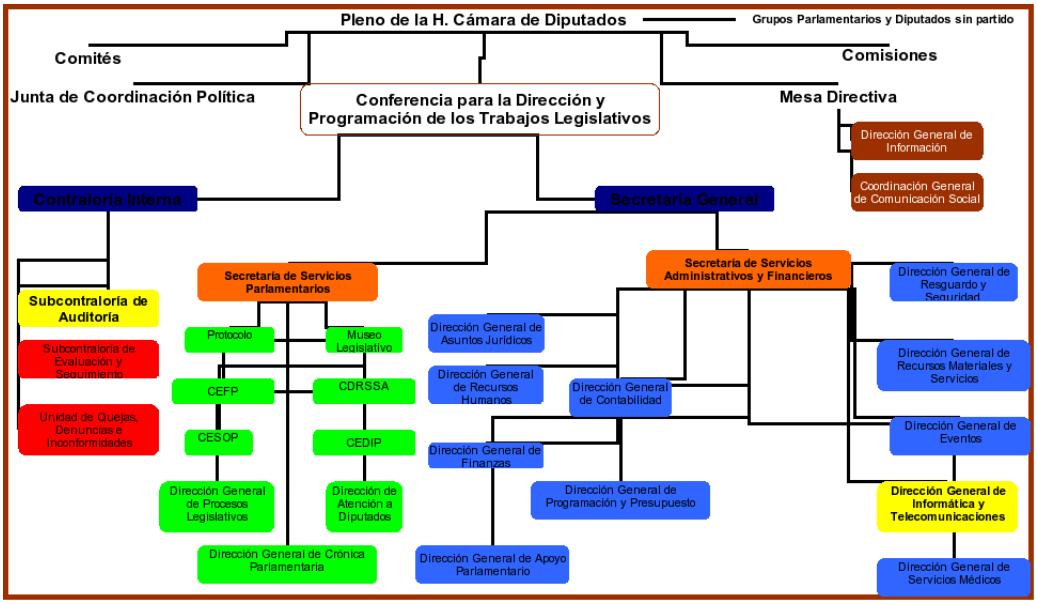
- Secretaría General.
- Secretaría de Servicios Parlamentarios.
- Secretaría de Servicios Administrativos y Financieros.
- Contraloría Interna.
- Coordinación General de Comunicación Social.

Estructura orgánica general

A fin de comprender, la conformación de la Cámara de Diputados y específicamente con el propósito de ubicar tanto de la Contraloría Interna como de la Dirección General de Informática y Telecomunicaciones dentro de este Órgano Legislativo, a continuación se presenta su Estructura Orgánica[4] actual en Figura 1.1, " Estructura orgánica general de la Cámara de Diputados".

[2]Constitución Política de los Estados Unidos Mexicanos, Título Segundo, Capítulo 1.- «De la Soberanía Nacional y de la Forma de Gobierno, Artículos 49 y 50».
[3]Constitución Política de los Estados Unidos Mexicanos, Capítulo II.- «Del Poder Legislativo»
[4][bib-manual-camara-diputados]

Figura 1.1. Estructura orgánica general de la Cámara de Diputados

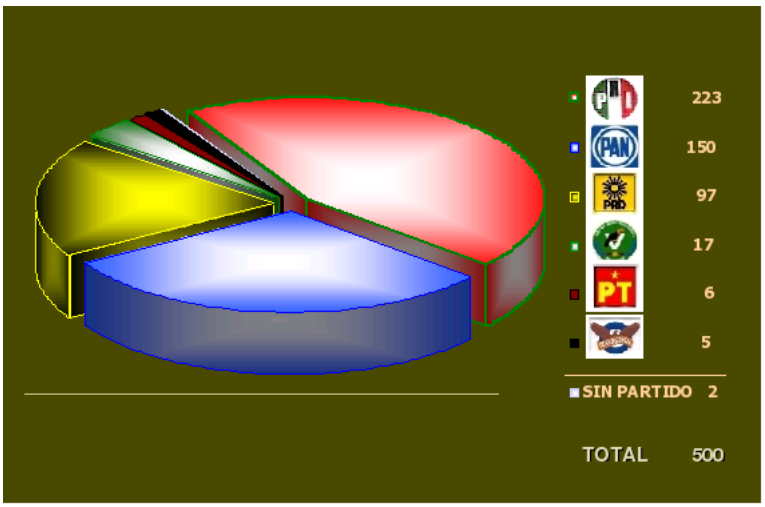


Como se puede ver, la Secretaría General es la cabeza de los servicios técnicos y administrativos (compuesta a su vez por la Secretaría de Servicios Parlamentarios y de Servicios Administrativos y Financieros). Estas últimas articuladas mediante órganos responsables de la gama de servicios específicos, respectivamente en las áreas parlamentaria y administrativo-financiera. Dentro de las áreas que conforman a la Secretaría de Servicios Administrativos y Financieros, se encuentra a la Dirección General de Informática y Telecomunicaciones, misma que se estudia en el siguiente capítulo de este informe.

Conformación actual

Para comprender el funcionamiento de la Cámara de Diputados se menciona su conformación actual en cuanto a los Grupos Parlamentarios, que en conjunto con los respectivos Senadores conforman un Partido Político, los cuales están encargados de las labores puramente legislativas; dentro de la Cámara de Diputados la información publicada al 15 de julio de 2005 en su página oficial[5], arroja la repartición de los actuales 500 Diputados con las siguientes cifras:

Figura 1.2. Conformación de la H. Cámara de Diputados LIX Legislatura



[5][bib-camara-diputados-web]

Contraloría Interna de la Cámara de Diputados

Ya que se conoce como se conforma la Cámara de Diputados, el siguiente escalón para hablar en particular de la Contraloría Interna, éste es el Órgano de Interno de Control que es el encargado de llevar a cabo la gestión del control administrativo y fiscal dentro de esta institución.

Cabe señalar que la Contraloría Interna de la Cámara de Diputados del Honorable Congreso de la Unión se creó mediante Acuerdo de la Gran Comisión del 5 de mayo de 1994, con el objetivo de que la Cámara de Diputados cuente con su propio Órgano Interno de Control que a fin de propiciar el óptimo aprovechamiento de los recursos de la Institución.

Legislación

La formación de la Contraloría Interna se establece en la Ley Orgánica del Congreso General de los Estados Unidos Mexicanos, Artículo 53 que a la letra dice:

La Cámara cuenta con su propia Contraloría Interna, la que tendrá a su cargo recibir quejas, realizar investigaciones, llevar a cabo auditorías y aplicar los procedimientos y sanciones inherentes a las responsabilidades administrativas de los servidores públicos de la misma.

La Contraloría se ubica en el ámbito de la Conferencia para la Dirección y Programación de los Trabajos Legislativos. Su titular es designado a propuesta de dicha Conferencia, y aprobado por las dos terceras partes de los diputados presentes en el pleno.

Importante

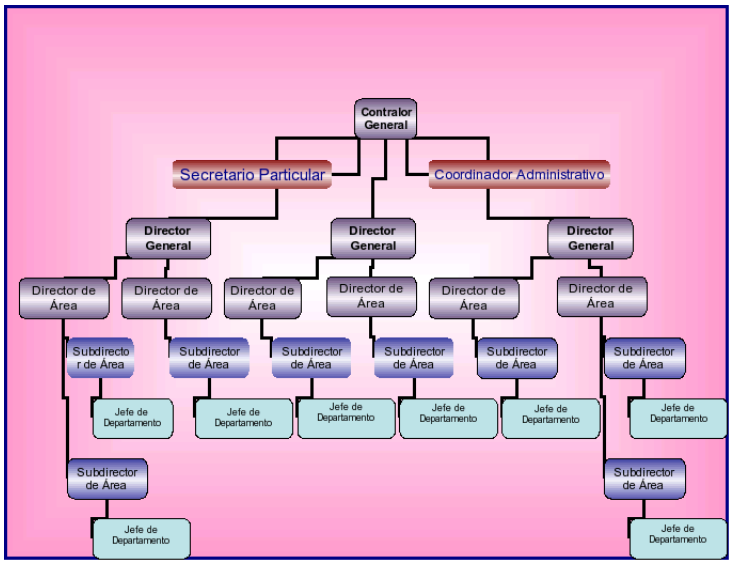
Como puede apreciarse, la creación de la Contraloría Interna dentro de la H. Cámara de Diputados data de hace diez años y paulatinamente ha venido reforzando sus mecanismos e incrementando su actuación, ha tenido avances significativos hasta incorporar en sus revisiones las subvenciones a los grupos parlamentarios, a partir de 2002, lo que representó un arduo esfuerzo y rediseño de funciones.

Para su manejo interno, la Cámara de Diputados cuenta con el *Manual de Organización General de la Cámara de Diputados*, que se expide en cumplimiento a los *Lineamientos para la Organización de los Servicios Parlamentarios, Administrativos y Financiero*s establecidos por la Conferencia para la Dirección y Programación de los Trabajos Legislativos, que en su presentación "...establece el marco de actuación de las unidades sustantivas y adjetivas de la Cámara, así como su estructura orgánica, representada a nivel de jefatura de departamento. Comprende las atribuciones de la Secretaría General, de las Secretarías de Servicios Administrativos y Financieros, y de sus áreas dependientes, así como de otros órganos técnicos de la Cámara como la Contraloría Interna y la Coordinación General de Coordinación Social", y al cual se apega la administración actual.

Estructura orgánica

En el Manual de Organización General de la Cámara de Diputados se establece la estructura orgánica autorizada de la Contraloría Interna, como se ilustra en Figura 1.3, "Estructura orgánica de la Contraloría Interna de la Cámara de Diputados":

Figura 1.3. Estructura orgánica de la Contraloría Interna de la Cámara de Diputados



En la figura anterior, se aprecia en el segundo nivel a tres Direcciones Generales, éstas representan lo que en la práctica son la son las tres Subcontralorías que ya se menciona, con sus respectivas Direcciones de Área.

Este problema está siendo regulado en la actualidad para homogeneizar los nombres de los puestos dentro del organigrama

Habrá que mencionarse que aunque existen autorizados ciertos número de plazas, en la práctica, actualmente la nivelación, regularización y autorización de algunas plazas de más y de menos se encuentra en proceso. Como es el caso de los Jefes de Departamento, entre otros.

En cuanto a los niveles salariales, en Tabla 1.1, “Niveles salariales de la Contraloría Interna de la Cámara de Diputados” se describe su régimen, su nivel según estructura y rango salarial:

Tabla 1.1. Niveles salariales de la Contraloría Interna de la Cámara de Diputados

Denominación	Régimen	Estructura	Rango salarial
Contralor General	1	Base	MD 02 a MD 06
Director General	3	Base	MD 07 a MD 12
Director de Área	6	Base	MG 06 a MG 10
Secretario Particular		Homólogos	MG 02 a MG 12
Subdirector de Área	8	Base	MS 02 a MS 12
Coordinador Administrativo		Homólogos	MS 02 a MS 12
Jefe de Departamento	9	Base	MC 01 a MC 07
Total	27		

Objetivo y funciones

Dentro del Manual de Organización General de la Cámara de Diputados se encuentra también que se plasma el objetivo y funciones de la Contraloría Interna, como sigue:

Objetivo

Establecer los mecanismos de fiscalización, control, auditoría y evaluación para supervisar el funcionamiento de las unidades administrativas dentro de su campo de acción, así como realizar las recomendaciones necesarias orientadas a mejorar los procedimientos administrativos que emplean las áreas, con el propósito de que éstas cumplan con los ordenamientos legales aplicables y así lograr el óptimo aprovechamiento de los recursos de los que dispone la Cámara.

Funciones

Elaborar el Programa Anual de Control y Auditoría de la Cámara de Diputados, someterlo a la aprobación de la Conferencia para la Dirección y Programación de los Trabajos Legislativos y proceder a su ejecución.

Diseñar, implantar y supervisar la operación del Sistema Integral de Control y Evaluación de la Gestión de las unidades administrativas de la Cámara de Diputados.

Evaluar el cumplimiento de los programas y políticas aprobados por la Conferencia para la Dirección y Programación de los Trabajos Legislativos, con objeto de retroalimentar el proceso de planeación, programación y presupuestación.

Establecer los lineamientos y políticas que orienten a la colaboración, que conforme a la ley deba prestar la Contraloría a la Auditoría Superior de la Federación, para el mejor cumplimiento de sus respectivas responsabilidades.

Emitir las disposiciones, reglas y bases de carácter general, normas, lineamientos y políticas en el ejercicio de las atribuciones, que conforme a las leyes, competen a la Contraloría, previa autorización de la Conferencia para la Dirección y Programación de los Trabajos Legislativos.

Opinar previamente a su expedición, sobre los proyectos de disposiciones, reglas, normas, lineamientos y políticas que elaboren las unidades administrativas de la Cámara.

Aplicar las normas que se hubieren fijado por la Conferencia para la Dirección y Programación de los Trabajos Legislativos en materia de control, fiscalización y evolución.

Proporcionar información a la Conferencia para la Dirección y Programación de los Trabajos Legislativos cuando ésta lo requiera.

Recibir y atender las quejas y denuncias que se presenten en contra de los servidores públicos, adscritos a las áreas administrativas y los que realicen funciones de ese carácter en la Cámara de Diputados y en su caso, sustanciar el procedimiento administrativo disciplinario e imponer las sanciones correspondientes en los términos de la ley en la materia.

Subcontraloría de Auditoría

La Subcontraloría de Auditoría se puede apreciar a nivel general en Figura 1.1, “ Estructura orgánica general de la Cámara de Diputados”; asimismo corresponde a una de las Direcciones Generales de Figura 1.3, “Estructura orgánica de la Contraloría Interna de la Cámara de Diputados”. De esta forma se observa al área de interés particular, en este apartado se presenta su legislación, conformación, principales funciones, estructura, etc.

Legislación

La legislación de la Subcontraloría de Auditoría, como ya se mencionó, se estructura desde el *Estatuto de la Organización Técnica y Administrativa y del Servicio de Carrera de la Cámara de Diputados* establece que la “organización y funcionamiento de la estructura técnica y administrativa de este Ór-

gano, entre ellos la Contraloría Interna"[6], en su Título Cuarto habla específicamente de éste órgano, misma que se encarga de recibir quejas, realizar investigaciones, llevar a cabo auditorías y aplicar los procedimientos y sanciones inherentes a las responsabilidades administrativas de los servidores públicos y se ubica en el ámbito de la Conferencia, según lo dispone el artículo 53 de la Ley Orgánica.

Este Título del estatuto establece todas las particularidades de este Órgano de Control Interno, como son: el procedimiento para designar al Contralor Interno, lo sueldos y percepciones que recibirá él y el demás personal del área, sus derechos y obligaciones, su estructura orgánica y funciones[7].

Para realizar estas funciones, se divide en tres Subcontralorías:

- Quejas, Denuncias e Inconformidades
- Evaluación y Seguimiento
- Auditoría[8]

Ésta última, objeto de nuestro estudio, es la encargada en particular de la realización de las auditorías que se plasman dentro del Programa Anual de Control y Auditoría que es sometido a la aprobación de la Conferencia para la Dirección y Programación de los Trabajos Legislativos.

Además de las revisiones por peticiones especiales o por órdenes de la Auditoría Superior de la Federación.

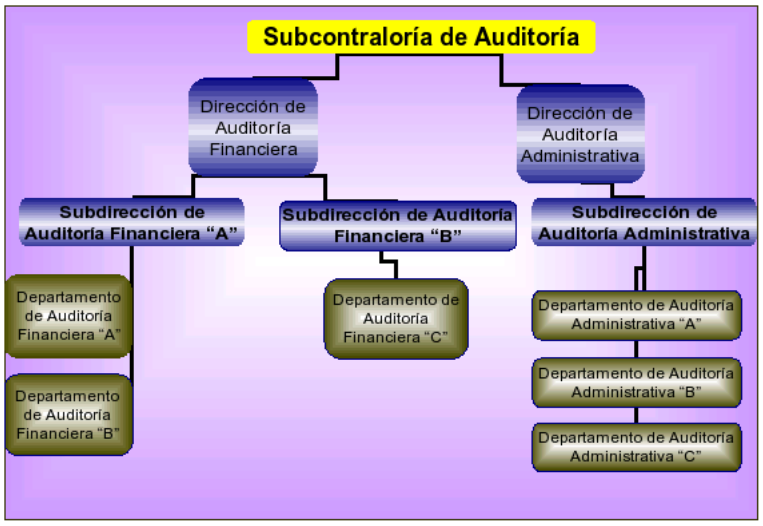
Estructura orgánica general

Además de la estructura general (Figura 1.1, " Estructura orgánica general de la Cámara de Diputados") dentro de la cual se ubica a la Subcontraloría de Auditoría dentro del universo entero de la Cámara de Diputados, a continuación se presenta el Organigrama de la Subcontraloría de Auditoría de forma particular y desglosada (Figura 1.3, "Estructura orgánica de la Contraloría Interna de la Cámara de Diputados"), estos datos se encuentran plasmados también en el Manual de Organización General de la Cámara de Diputados.

Como a continuación se aprecia, la Subcontraloría de Auditoría está compuesta por dos vertientes: la Dirección de Auditoría Financiera y la Dirección de Auditoría Administrativa y a su vez en las Subdirecciones y Departamentos correspondientes.

[6] *Estatuto de la Organización Técnica y Administrativa y del Servicio de Carrera de la Cámara de Diputados*, Título Primero.- "Disposiciones Generales", Artículo 1º, Inciso c).
[7] *Estatuto de la Organización Técnica y Administrativa y del Servicio de Carrera de la Cámara de Diputados*, Título Primero.- "Disposiciones Generales", Artículos del 153 al 158.
[8] *Estatuto de la Organización Técnica y Administrativa y del Servicio de Carrera de la Cámara de Diputados*, Título Primero.- "Disposiciones Generales", Artículo 158.

Figura 1.4. Estructura orgánica de la Subcontraloría de Auditoría



Objetivo

El objetivo general de la Subcontraloría de Auditoría se plasma en el Manual de Organización General de la Cámara de Diputados, que a la letra dice:

Vigilar que las operaciones de la Cámara de Diputados se realicen con apego a los programas y procedimientos establecidos de conformidad a la normatividad aplicable, verificando que el manejo y aplicación de los recursos financieros, humanos y materiales se lleven a cabo de acuerdo con las disposiciones presupuestales en el Presupuesto de Egresos de la Federación.

Adicionalmente, en el *Manual de Organización de la Contraloría General* se establece como su objetivo:

Establecer los mecanismos de fiscalización, control, auditoría y evaluación para supervisar el funcionamiento de las unidades administrativas dentro de su campo de acción, así como realizar las recomendaciones necesarias orientadas a mejorar los procedimientos administrativos que emplean las áreas, con el propósito de que éstas cumplan con los ordenamientos legales aplicables y así lograr el óptimo aprovechamiento de los recursos de los que dispone la Cámara.

Funciones

Las funciones de la Contraloría Interna están plasmadas en primera instancia de forma general en el Estatuto de la Organización Técnica y Administrativa y del Servicio de Carrera de la Cámara de Diputados:

a. Elaborar, aplicar y verificar el cumplimiento del programa anual de control y auditoría;

b. Realizar las auditorías conforme al programa anual de control y auditoría y elaborar los informes de los resultados obtenidos;

c. Vigilar que el manejo y aplicación de los recursos financieros, humanos y materiales se lleven a cabo de acuerdo con las disposiciones aplicables;

d. Convocar y participar en la aclaración de las observaciones con los titulares de las Unidades Administrativas auditadas, así como llevar el seguimiento de las observaciones pendientes de solventar;

e. Participar en los diversos actos de fiscalización conforme a las atribuciones de la Contraloría Interna;

f. Fungir como enlace con la entidad de fiscalización superior de la federación de la Cámara, en la revisión de la Cuenta Pública; y

g. Las demás que se deriven del presente Estatuto y de las normas, disposiciones y acuerdos aplicables.[9]

En segunda instancia, de forma particular las funciones de la Subcontraloría de Auditoría están plasmadas en el *Manual de Organización General de la Cámara de Diputados*:

- Elaborar y verificar el cumplimiento de la aplicación del Programa Anual de Control y Auditoría, autorizado por la Conferencia para la Dirección y Programación de los Trabajos Legislativos.
- Realizar las auditorías conforme al Programa Anual de Control y Auditoría (PACA).
- Convocar y participar en la aclaración de las observaciones con los titulares de las unidades administrativas auditadas, así como llevar el seguimiento de las observaciones pendientes de solventar.
- Elaborar los informes definitivos de los resultados obtenidos de las auditorías realizadas.
- Elaborar trimestralmente el avance del PACA.
- Elaborar las guías y programas detallados de auditorías, correspondiente al PACA.
- Participar en los diversos actos de fiscalización conforme a las atribuciones de la Contraloría Interna.
- Fungir como enlace con la Auditoría Superior de la Federación, cuando así se instruya por las instancias correspondientes, en la revisión de la Cuenta Pública de la Cámara de Diputados.
- Promover la capacitación de los integrantes de la Subcontraloría de Auditoría, a fin de elevar la calidad, eficiencia y eficacia de su presencia fiscalizadora.
- Elaborar, revisar y actualizar los manuales correspondientes al área.
- Representar a la Contraloría Interna conforme a sus atribuciones.

Por otra parte, en el *Manual de Organización de la Contraloría General* se reiteran las mismas funciones plasmadas con anterioridad en el Manual de Organización General de la Cámara de Diputados.

Metas

Las metas de la Subcontraloría de Auditoría no se encuentran plasmadas en ningún documento oficial; sin embargo, en el *Marco conceptual y desempeño de la Contraloría Interna* se plasman sus metas, y a la letra dice:

- Establecer los mecanismos de fiscalización, control, auditoría y evaluación para supervisar el funcionamiento de las unidades administrativas y de los Grupos Parlamentarios dentro de su campo de acción.
- Verificar el ejercicio de los recursos públicos asignados a la Cámara, para que se realice con eficiencia, eficacia y en apego a los ordenamientos legales aplicables, transparencia y racionalidad.
- Fortalecer la mejora continua en la administración y uso de los recursos públicos.
- Dar transparencia al ejercicio del gasto.
- Reforzar la prevención de irregularidades en el desempeño de los servidores públicos.

[9] *Estatuto de la Organización Técnica y Administrativa y del Servicio de Carrera de la Cámara de Diputados*, Título Primero.- “Disposiciones Generales”, Artículo 158.

Misión

La misión de la Subcontraloría de Auditoría no se encuentra plasmada tampoco en ningún documento oficial; pero de igual forma en el *Marco conceptual y desempeño de la Contraloría Interna* se plasma como su misión la siguiente:

Importante

La misión de la Subcontraloría de Auditoría es “Dar transparencia a la gestión de las unidades administrativas y de los servidores públicos de la H. Cámara de Diputados, en el ejercicio del gasto público, previniendo la desviación del mismo”.

Visión

La visión de la Subcontraloría de Auditoría tampoco se encuentra en ningún documento oficial; pero de igual forma en el *Marco conceptual y desempeño de la Contraloría Interna* se plasma como su visión la siguiente:

Importante

La visión de la Subcontraloría de Auditoría es “que la ciudadanía tenga confianza y credibilidad en la administración de la H. Cámara de Diputados”.

Debilidades y fortalezas

En cuanto a las debilidades, fortalezas de la Subcontraloría de Auditoría, derivado del estudio al área, el cual consistió primero en entrevistas con el personal, y asistir a las instalaciones para analizar el área entera en lo que se refiere a tecnologías de información, recursos informáticos, infraestructura y cultura informática, se encuentran las siguientes:

Debilidades

- No cuentan con la debida regulación legal y jurídica actualizada que apoye y sustente sus funciones, ni en las áreas administrativas, mucho menos en lo que respecta a las funciones de auditoría en informática.
- No existe un área ni una persona que desarrolle la función de auditoría en informática.
- En general, el personal de mandos medios, así como operativo, se muestra poco interesado en el avance de las tecnologías de información, así como en la formación de su personal en este sentido.
- Su personal está capacitado para la utilización de equipos de cómputo solo para las funciones más básicas.
- Actualmente la Subcontraloría de Auditoría no ha realizando nunca una auditoría en informática al área de sistemas, mucho menos a las demás áreas administrativas ni Grupos Parlamentarios.
- No cuentan con ningún tipo de software que apoye la función de auditoría cotidiana, mucho menos alguno especializado para la auditoría en informática.
- No aprovechan la infraestructura informática que les proporciona la Cámara de Diputados (red).
- No cuentan con una planeación informática que les permita ir a la vanguardia, mucho menos hacer un planteamiento formal en cuanto a este tema.
- El personal de la Cámara de Diputados muestra en general un grado muy bajo de cultura informática.

- Existe poco equipo de cómputo en el área y está mal repartido entre el personal auditor y los altos mandos.
- El equipo con que cuentan los auditores, en general no cumple con las necesidades básicas de procesamiento para que realicen correctamente su función.
- El procedimiento para la adquisición de tecnologías de información dentro de la Cámara de Diputados es muy burocrático, lleva mucho tiempo el suministro de equipos y bienes de cómputo.
- Hay muy poca participación del personal del área en los constantes cursos de capacitación en informática que se imparten en la Cámara de Diputados.

Fortalezas

- En general existe poca rotación de personal integrante de la Subcontraloría de Auditoría en general, lo que ayuda a comprometer paulatinamente más al personal en sus labores cotidianas.
- La red que tiene la Subcontraloría de Auditoría es la que proporciona la Cámara de Diputados, la cual es de banda ancha y además puede ser adaptada a las necesidades del área si ésta lo fundamenta adecuadamente, asimismo la compra de equipo y demás tecnología.
- De ser correctamente fundamentada la necesidad de adquirir un software o equipo de cómputo para la Subcontraloría de Auditoría en las áreas dedicadas a este proceso, podrán ser adquiridos.
- Regularmente existe reconocimiento del trabajo de los niveles superiores hacia los inferiores.
- Buena motivación del personal que labora en la Subcontraloría de Auditoría.
- Es un “campo fértil” para la implantación de nuevas tecnologías de información, ya que al no haber un sistema actualmente, no será necesario ningún proceso de migración de datos.
- Un planteamiento adecuado y bien pensado de las necesidades presentes y futuras del área resolverá fácilmente la problemática que actualmente enfrenta la Subcontraloría de Auditoría.

Riesgos

Cuando se habla de riesgo, se entiende como: “Los riesgos son condiciones del mundo real en el cual hay una exposición a la adversidad, conformada por una combinación de circunstancias del entorno, donde hay posibilidad de perdidas.[10]”.

Al asistir a las instalaciones de la Subcontraloría de Auditoría para analizarla, se revisaron las tecnologías de información con las que cuentan a la fecha, de lo cual se determinan los siguientes riesgos:

Tabla 1.2. Lógicos

Riesgo	Probabilidad	Impacto	Control
Pérdida de información	Media	Alto	No lo hay
Recomendaciones inadecuadas	Baja	Alto	No lo hay
Fuga de información	Baja	Medio	No lo hay
Descontrol del personal	Medio	Bajo	No lo hay

[10][bib-solis-2002]

Tabla 1.3. Físicos

Riesgo	Probabilidad	Impacto	Control
Incendio	Baja	Bajo	Sistemas contra incendio
Robo	Media	Alta	Controles de acceso, resguardos e inventarios
Desastres naturales	Baja	Alta	Programas de capacitación en caso de desastres naturales

Controles

El personal de la Subcontraloría de Auditoría no cuenta con un documento formal que establezca sus funciones; sin embargo, cuentan con un documento llamado *Marco conceptual y desempeño de la Contraloría Interna*, que fue se proporcionó para este estudio y en el cual se muestran como controles, los siguientes:

Preventivo:

Una de las prioridades de la Contraloría Interna ha sido y es la de fortalecer los sistemas de control interno, a fin de contribuir al ejercicio transparente del gasto y a evitar irregularidades por parte de las diversas áreas administrativas, para lo cual se ha venido promoviendo la revisión, actualización y complementación de la normatividad.

En este sentido destaca lo siguiente:

- Expedición de la Norma de Adquisiciones, Arrendamientos, Obra Pública y Servicios.
- Actualización del Manual para los eventos de Entrega-Recepción.
- Actualización de los Lineamientos Generales para la Administración de Recursos.
- Manual de Bases y Políticas para la Prestación de Servicios.
- Actualización de Manuales de Procedimientos.

Otro aspecto al que se le ha dado importancia es a la participación en los diferentes actos de fiscalización relacionados con adquisiciones, tales como licitaciones públicas, concursos por invitación restringida, selección entre 5 cotizaciones, etc, participando desde la revisión de bases hasta el fallo de los eventos.

Esta actividad ha permitido obtener importantes ahorros para la Institución, además de hacer más transparentes los procesos de adquisición.

Se tuvo participación relevante en los actos de Entrega-Recepción de los Grupos Parlamentarios, Comisiones y Comités realizados por primera vez, con motivo del cambio de la LVIII a la LIX Legislatura.

Como se puede ver, los controles a los que se refiere son puramente administrativos.

En cuanto a tecnologías de información, actualmente el único control que se lleva dentro de la Subcontraloría de Auditoría es como máximo el inventario físico de los equipos de cómputos, resguardos individuales de los mismos y relación del software que maneja cada equipo.

La Dirección General de Tecnologías de Información cuenta con sus propios controles de acceso lógico y sellos de seguridad en cuanto a la seguridad física, además de los ya mencionados resguardos físicos personales de equipo de cómputo.

Además de eso, no existe control alguno sobre ningún aspecto del ámbito informático, tampoco sobre la capacitación del personal y actualmente hay total desconocimientos de las mejores prácticas y/o software que pueda auxiliar a los auditores en su desempeño y cumplimiento de funciones.

Tecnología informática actual de la Subcontraloría de Auditoría

La Subcontraloría de Auditoría tiene un inventario de equipo limitado y mal repartido, hay personal que necesita máquinas más adecuadas para su trabajo, algunos incluso podría hacer uso de herramientas informáticas que apoyarán su labor, mientras que hay personal con equipos más completos y modernos que en realidad no utilizan.

En los siguientes puntos se detalla su infraestructura, su tecnología actual en cuanto a hardware y software.

Hardware

En la Subcontraloría de Auditoría se utiliza la red que proporciona la propia Cámara de Diputados, misma que funciona por medio de un anillo lógico de fibra óptica, sobre la cual corren la mayoría de las áreas administrativas, órganos técnicos y buena parte de los Grupos Parlamentarios. Sobre la red que provee el área de sistemas se habla en el siguiente capítulo, por el momento concretamente se menciona la tecnología con la que cuenta únicamente la Subcontraloría de Auditoría:

- Tres equipos DELL, Pentium IV.
- 7 HP Pentium IV
- 8 HP Pentium III
- Tres equipos en desuso modelo 486.
- Tres impresoras en red:
- 1 DELL blanco y negro
- 1 Xerox Phaser 4400 blanco y negro
- 1 Laser Jet 400 blanco y negro
- 2 HP Laser Jet 5500 a color (Propiedad privada)

Software

Los equipos con Pentium IV, tiene instalado Windows XP, con sesión para usuario limitado y office XP con los componentes básicos.

Los equipos de Pentium III para abajo tienen instalado Windows 98 ó 95 y office de la misma versión, con paquetería básica.

Recursos humanos y capacitación

La Subcontraloría de Auditoría tiene como personal una plantilla de 29 empleados entre los regímenes fiscales de mandos Medios y Superiores, Honorarios Asimilados a Sueldos y Supernumerarios, mismos que a continuación se enuncian:

- 1 Subcontralor de Auditoría,
- 1 Auxiliar.
- 2 Subdirectores (Director de Auditora Financiera y Director de Auditoría Administrativa),
- 4 Jefes de Departamento (Dos para cada Dirección),

- 17 Auditores (Rotan según las necesidades de auditoría entre las dos áreas),
- 2 Secretarias,
- 1 Chofer

ya se mencionó que existe un conflicto entre los nombres de los puestos que se plasman en el Estatuto de la Organización Técnica y Administrativa y del Servicio de Carrera de la Cámara de Diputados y la estructura orgánica de la Subcontraloría de Auditoría, adicionalmente existen inconsistencias en los tramos de control, entre otras, pero no se ahonda más en este tema por no ser objeto de este estudio; por otra parte, esta situación ya está siendo regularizada ante las instancias correspondientes.

Nota

Como ya se mencionó, uno de los grandes problemas de la Subcontraloría de Auditoría es la poca capacitación de persona, aproximadamente el 30% sabe usar con agilidad la paquetería de office, un 40% la usa pero con dificultades, mientras que el 30% tiene conocimientos muy básicos de computación.

Capítulo 2. Descripción del área de sistemas

Una vez que se conoce al área de auditoría del órgano, es necesario ahora que se conozca su contraparte: la Dirección General de Tecnologías de Información; misma que existe dentro de la Cámara de Diputados, para la administración y control de sus recursos informáticos, misma que se estudia en este capítulo. Parte importante de este estudio es definir los controles y riesgos del área de sistemas y darle dimensión respecto de la auditoría; así como las debilidades propias a fin de determinar el objetivo a seguir. Por ello, en este capítulo, se hace un estudio de la conformación actual del área de sistemas, su normatividad, recursos, estrategias y servicios actuales, estructura, misión, visión y funciones.

Las debilidades y fortalezas dirán cuáles son los requerimientos del área de auditoría y cuáles serán sus dimensiones. Sobretodo, recordando que toda falla o carencia de control genera una *situación de riesgo*, éstos serán estudiados a fin de conocer su funcionamiento actual y posibles mejoras.

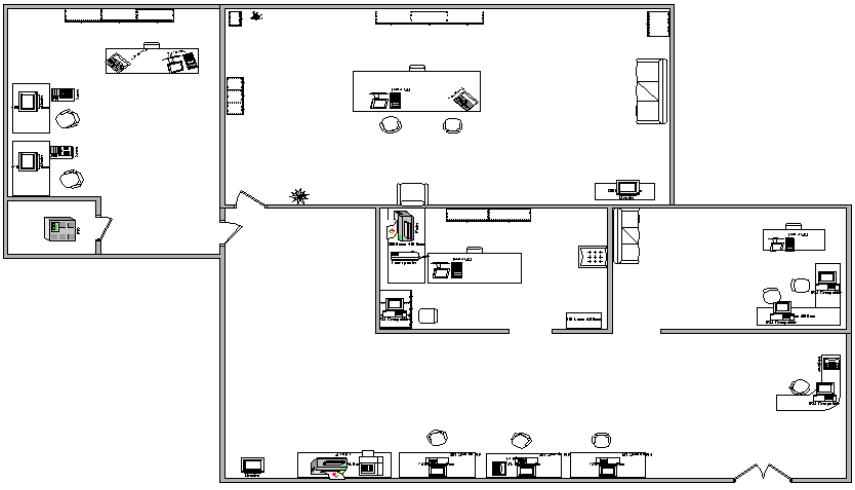
Normatividad actual

En la actualidad la Cámara de Diputados en su Área de sistemas no se rige bajo ninguna norma o certificación externa nacional o internacional. Tampoco cuentan con ningún tipo de manual de procedimientos u organización que les permita realizar sus labores de forma sistemática y ordenada. De igual forma la falta de metas y objetivos genera desorganización y falta de control, mala administración e inclusive representa un riesgo latente ante las posibles fallas del sistema.

Tampoco cuentan con ningún tipo de plan de contingencia en caso de que la red falle, mucho menos con medidas para minimización de riesgos por posibles ataques, desastres de ningún tipo, etc.

A fin de conocer mejor el área de sistemas se presenta en la Figura 2.1, “Conformación actual del área de sistemas” su conformación actual:

Figura 2.1. Conformación actual del área de sistemas



Recursos informáticos existentes del área de sistemas

Hardware.

Actualmente el área de sistemas cuenta con un total de 45 máquinas de escritorio, 20 impresoras conectadas en red y 3 tipos de servidores, aunque dentro del área se cuentan con algunos otros servidores, los 3 que se describen a continuación son exclusivos del área de sistemas:

Tabla 2.1. Equipos de escritorio

Cantidad	Marca	Características
22	DELL	Pentium IV, 512 MB Ram 60 GBD.D., Quemador 48x, Pantalla LCD 15" Floppy 3½, Tarjeta de fibra óptica, Tarjeta de red
18	HP	Pentium III, 256 MB Ram, 40 GB D.D., CD-Rom, Monitor 15", Floppy 3½, Tarjeta de fibra óptica, Tarjeta de red
5	Compaq	Pentium III, 128 MB D.D., CD-Rom, Monitor 15" Flopy 3½, Tarjeta de red

Tabla 2.2. Impresoras

Cantidad	Marca	Características
5	Impresora Dell	Laser a color
10	Impresora HP	Inyección de tinta color
5	Impresora Epson	Inyección de tinta color

Tabla 2.3. Servidores

Cantidad	Marca	Características
2	Servidores Sun	1 servidor de Correo 1 servidor Web
1	Servidor Dell	Antivirus (McAfee)

Software

Para el área de sistemas todos los equipos incluyendo Pentium III cuentan con Windows XP Professional, Office XP, antivirus McAfee. Todos los equipos cuentan con la paquetería básica, solo algunos de los equipos Dell cuentan con Visio 2003, Corel ó Photoshop.

Todo el software tiene licencia, las licencias adquiridas para cualquier software es de tipo corporativa.

Infraestructura informática

La infraestructura con la que cuenta tanto el área de sistemas como toda la Cámara de Diputados incluyendo cada una de sus áreas dentro de cada edificio se describe de la siguiente manera:

Debajo de toda la infraestructura de los edificios de encuentra una red de anillo lógico de fibra óptica, la cual esta conectada a un servidor central (Web) el cual esta tiene salida a Internet por medio de un firewall físico.

En cada uno de los edificios en la planta baja se encuentra un switch que a su vez funciona como router, estos son de alta capacidad, cada unos de estos switch/router se conectan a otros switch también de alta capacidad que se encuadran en cada piso por cableado UTP categoría 6 ó 5, estos últimos se co-

nectan a un switch más, que es de una capacidad menor que se encuentra dentro de cada área de cada edificio por medio de cableado UTP categoría 6 ó 5, cada uno de estos switch se encarga de distribuir los servicios de red a cada una de las PC dentro del área.

En cada piso se maneja una topología de bus para la distribución de servicios.

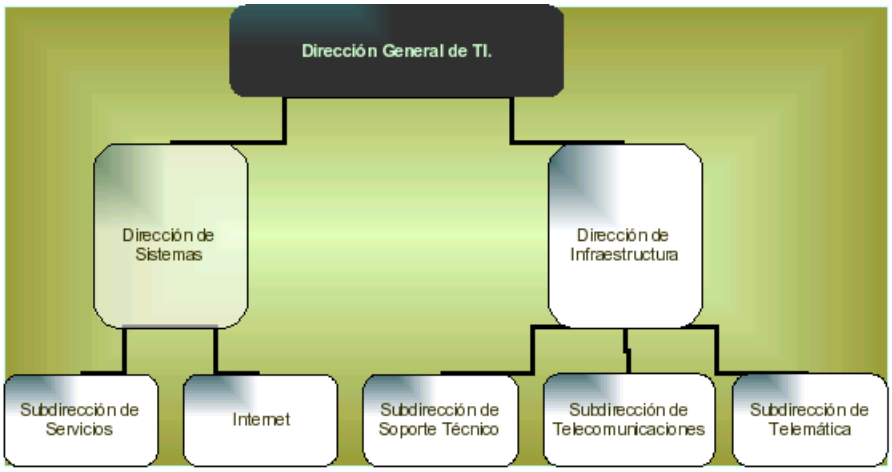
Recursos humanos y capacitación

El área de sistemas cuenta con un total de 60 empleados los cuales están distribuidos de la siguiente manera:

- 1 Director general de tecnologías de información.
- 1 Director de sistemas.
- 1 Subdirector de servicios.
- 1 Subdirector de Internet.
- 1 Director de infraestructura.
- 1 Subdirector de soporte técnico.
- 1 Subdirector de telemática.
- 1 Subdirector de telecomunicaciones
- 1 Jefe de telemática.
- 12 Ingenieros de soporte técnico.
- 10 Ingenieros de comunicaciones.
- 5 Ingenieros de desarrollo Web.
- 5 Ingenieros de desarrollo de aplicaciones.
- 1 Webmaster.
- 10 Secretarias.
- 5 Ingenieros de sistemas.
- 3 Auxiliares.

Estructura orgánica

Figura 2.2. Estructura orgánica de la Dirección General de S.I.



Misión

Una misión en el área de sistemas ayuda a establecer la finalidad o el propósito para la cual fue creada y este debe de ir ligado al objetivo de la organización, también se deben de comprender unos o más objetivos y las tareas que deben de realizarse para alcanzar dicho objetivo.

En la actualidad el área de sistemas de la Cámara de Diputados no cuenta con una misión que ayude a establecer el propósito para la cual fue creada esta área, esto representa un riesgo para el área ya que al no contar con una misión bien establecida crea confusión en las personas que operan dentro del área.

Visión

Una visión ayuda al área de sistemas a proyectarse en el futuro en una situación deseada, es decir hacía donde va o que es lo que quiere lograr. El área de sistemas de la Cámara de Diputados aún no cuenta con una visión establecida.

Objetivos y metas

Un objetivo para el área de sistemas es una situación deseada que el esta intenta lograr, esta es una imagen que el área pretende para el futuro. Al alcanzar el objetivo, la imagen deja de ser un ideal y se convierte en real y actual, por lo tanto, el objetivo deja de ser deseado y se busca otro para ser alcanzado.

Las funciones de establecer objetivos son las siguientes:

- Presentación de una situación futura: se establecen objetivos que sirven como una guía para la etapa de ejecución de las acciones.
- Fuente de legitimidad: los objetivos justifican las actividades del área.
- Sirven como estándares: sirven para evaluar las acciones y la eficacia del área.
- Unidad de medida: para verificar la eficiencia y comparar la productividad del área.

En la actualidad el área de sistemas de la H. Cámara de Diputados no cuenta con objetivos ni metas.

Funciones y servicios

En base a la plática realizada con el los gerentes de las diferentes subáreas que conforman al área de sistemas, actualmente estas son las funciones que realizan:

- Instalación y configuración de equipos.
- Altas y bajas de usuarios.
- Instalación y configuración de aplicaciones.
- Mantenimiento de equipos de usuarios.
- Administración de las listas de correo.
- Copias de seguridad de los datos de los usuarios y recuperación de los mismos en caso de pérdida.
- Instalación, configuración y mantenimiento de servicios como correo electrónico.
- Desarrollo de nuevas aplicaciones que permitan el mejor uso de los equipos.
- Administrar y mantener la disponibilidad y funcionamiento de los servidores (hardware y software).
- Elaborar proyectos e informes para la implementación de software y hardware, y analizar y proponer nuevos programas y equipamientos.
- Mantener y controlar las licencias de software adquiridas por el Organismo.
- Intervenir en proyectos especiales en los cuales resulte necesaria la asistencia informática.

- Coordinar la capacitación del personal de la Cámara de Diputados en materia informática, en el uso de los programas, manejo de Intranet e Internet.
- Asegurar la disponibilidad de las comunicaciones.
- Mejorar la funcionalidad del software asociado a las comunicaciones e incorporarle novedades.

Estrategias

Una estrategia es un plan que integra las principales metas u objetivos y políticas de una organización y a la vez, establece una secuencia coherente de las acciones a realizar. Una estrategia puede ayudar a un área de sistemas a poner orden y asignar recursos con el fin de lograr una situación viable y estable, así como a anticiparse a los posibles cambios en el entorno.

En base a las platicas sostenidas con los gerentes de la subáreas de sistemas y debido a que en los puntos anteriores ya se definió que el área de sistemas no cuenta con políticas ni objetivos establecidos a su vez esta tampoco cuenta con estratégicas.

Fortalezas y debilidades

De las visitas que se hicieron al área de la Dirección General de Tecnologías de Información, se detectaron las fortalezas y debilidades más importantes dentro del área de sistemas de la Cámara de Diputados, mismas que se muestran a continuación:

Fortalezas
Capacidad del personal de trabajo
Infraestructura de punta
Motivación hacía el personal de trabajo por parte de los Jefes
Ganas de crecer

Debilidades	**Riesgo**	**Impacto**
Bajo presupuesto dirigido al área	Poco crecimiento del área de sistemas, poca implantación de sistemas que impulsen al área a ser un área de servicios y a establecer controles para una mejor administración de la información	ALTO
Mala distribución de personal	No se pueden aprovechar al 100% las capacidades del personal	MEDIO
Poco tiempo de creación (3 años)	No se le da la importancia necesaria pensando que es un área sin experiencia	BAJO
No hay procesos	Las actividades no se realizan de acuerdo a estandares	ALTO
Mala rotación de personal	El personal realiza actividades que no conoce	MEDIO
Poca comunicación con los usuarios finales	Los usuarios no ven resultados por parte del área de sistemas como un área de servicios	MEDIO
Los sud-departamentos no trabajan en conjunto	Mala administración de las tecnologías, mala identificación de problemas	ALTO
Pocas posibilidades de crecimiento personal (influyentismo).	No se pueden aprovechar al 100% las capacidades del personal	MEDIO
No cuentan con las herramientas (software) necesarias para la buena administración del área.	No pueden anticiparse a los posibles problemas, perdida de información, caída de sistemas.	ALTO

Riesgos

El área de Tecnologías de Información fue analizada mediante entrevista al Ing. Omar Hash Pereyda, Director de Soporte Técnico, quien permitió dar un recorrido a las instalaciones, asimismo, proporcionó la normatividad autorizada con la que se cuenta, se realizó un análisis del área y basándonos en la experiencia de trabajo en diferentes áreas de TI en la actualidad en el área de sistemas de la H. Cámara de Diputados se detectaron los siguientes riesgos:

Tabla 2.4. Lógicos

Riesgo	Probabilidad	Impacto
Caída de la red	Media	Alto
Caída de servicios de producción	Media	Bajo
Extracción, modificación y destrucción de información confidencial	Baja	Alto
Uso inadecuado de las instalaciones	Alta	Media
Ataques de virus informáticos	Alta	Alto
Fuga de información	Media	Alto
Inadecuados controles de acceso lógicos	Baja	Alto
Pérdida de información	Baja	Medio
Falta de disponibilidad de aplicaciones críticas	Baja	Alto
Descontrol del personal	Medio	Bajo

Tabla 2.5. Físicos

Riesgo	Probabilidad	Impacto
Inadecuados controles de acceso físico	Alta	Bajo
Vulnerabilidad	Media	Alto
Incendio	Baja	Bajo
Robo	Media	Alto
Desastres naturales	Baja	Alto

Teniendo en cuenta que una de las principales causas de los problemas dentro del área de sistemas, es la inadecuada administración de riesgos informáticos, se debe hacer una buena administración de riesgos, basándose en los siguientes aspectos:

- La evaluación de los riesgos inherentes a los procesos informáticos.
- La evaluación de las amenazas ó causas de los riesgos.
- Los controles utilizados para minimizar las amenazas a riesgos.
- La asignación de responsables a los procesos informáticos.
- La evaluación de los elementos del análisis de riesgos.

Controles y mecanismos de seguridad

Los controles en un área de TI permiten monitorear acciones y tomar medidas para hacer correcciones inmediatas o preventivas para evitar eventos indeseables en el futuro. Existen diferentes tipos de controles que se deben establecer en un área de sistemas en donde hasta el momento en el área de sistemas

de la H. Cámara de Diputados solo cuenta con los que a continuación se mencionan y los cuales aun no están totalmente maduros.

Los controles con los que cuenta el área de sistemas son los siguientes:

- Controles de acceso físico a las instalaciones
- Controles de acceso lógico a las computadoras de todas las áreas (por medio de directorio activo)
- Definición de roles para equipos de computo todas las áreas
- Uso de firewall físico
- Políticas de seguridad para el uso de equipos de cómputo (actualmente es un proyecto de Manual que aún no está autorizado oficialmente, pero ya está en uso en la práctica), entre las más importantes está la prohibición del uso de programas no autorizados o software pirata, políticas de seguridad en el área de sistemas y áreas administrativas y parlamentarias.

Capítulo 3. Legislación informática, mejores prácticas y técnicas de auditoría informática

Legislación informática

En este punto se describen la regulación de las mejores prácticas de Auditoría en Informática como administrar los riesgos en tecnología Informática, la auditoría en el sector público en base a los organismos nacionales e internacionales.

Institute of System Audit and Association, ISACA

La Information Systems Audit and Control Association –Asociación de Auditoría y Control de Sistemas de Información– ISACA, comenzó en 1967. En 1969, el grupo se formalizó, incorporándose bajo el nombre de EDP Auditors Association –Asociación de Auditores de Procesamiento Electrónico de Datos. En 1976 la asociación formó una fundación de educación para llevar a cabo proyectos de investigación de gran escala para expandir los conocimientos y el valor del campo de gobernación y control de TI.

«Actualmente, los miembros de ISACA –más de 28.000 en todo el mundo– se caracterizan por su diversidad ya que están presentes en más de 100 países y cubren una variedad de puestos profesionales relacionados con TI, como son los Auditores de SI, Consultores, Educadores, Profesionales de Seguridad de SI, Reguladores, Directores Ejecutivos de Información y Auditores Internos, por mencionar sólo algunos.

»En las tres décadas transcurridas desde su creación, ISACA se ha convertido en una organización global que establece las pautas para los profesionales de gobernación, control, seguridad y auditoría de información.

»Su certificación Certified Information Systems Auditor –Auditor Certificado de Sistemas de Información– CISA, es reconocida en forma global y ha sido obtenida por más de 30.000 profesionales. Su nueva certificación Certified Information Security Manager –Gerente Certificado de Seguridad de Información– CISM, se concentra exclusivamente en el sector de gerencia de seguridad de la información. Publica un periódico técnico líder en el campo de control de la información, el Information Systems Control Journal –Periódico de Control de Sistemas de Información.» [1]

Organiza una serie de conferencias internacionales que se concentran en tópicos técnicos y administrativos pertinentes a las profesiones de gobernación de TI y aseguración, control, seguridad de SI. Juntos, ISACA y su IT Governance Institute –Instituto de Gobernación de TI– asociado lideran la comunidad de control de tecnología de la información y sirven a sus practicantes brindando los elementos que necesitan los profesionales de TI en un entorno mundial en cambio permanente

Las empresas públicas y privadas están valorando cada día más la creciente importancia que representa mantener sistemas informáticos seguros, confiables y confidenciales, que eviten o prevengan la ocurrencia de errores u operaciones ilegales a partir de debilidades en los sistemas de control.

Certified Information Security Auditor, CISA

La Asociación de Auditoría y Control de Sistemas de Información (ISACA) provee una Certificación en Auditor en Sistemas de Información (CISA), por medio de un examen anual que realiza el Instituto

[1] [bib-isaca-mx]

a los candidatos, el cual cubre el conocimiento de actividades requeridas para la función de Auditoría en TI, para lo cual presenta un Manual de Información Técnica para la preparación de los candidatos.

La certificación de CISA (Certified Information Systems Auditor) es otorgada por la (ISACA), desde 1978 y es considerada en la actualidad como un reconocimiento de que se cuenta con los conocimientos teóricos y prácticos necesarios para desempeñarse como Auditor de Sistemas siguiendo los estándares y directrices definidos para una mejor preparación.

La designación de CISA, se considera hoy en día, una ventaja competitiva y resulta de beneficio no solo para las organizaciones que deben cumplir con requerimientos de certificación profesional de sus colaboradores, sino para las personas que buscan un desarrollo profesional y la obtención de certificaciones que ofrecen oportunidades a nivel internacional.

Certified Information Security Manager, CISM

También ISACA provee la Certificación para la Administración de la Seguridad de la Información del cual intenta garantizar que existan administradores de seguridad de TI que tengan los conocimientos necesarios para reducir el riesgo y proteger a la organización.

La certificación CISM está diseñada para dar la certeza de que los individuos certificados tengan los conocimientos para ofrecer una eficaz administración y consultoría de seguridad.

Esta orientada a profesionales que administran la seguridad de la información en una organización y tienen el conocimiento y la experiencia para montar, implementar y dirigir una estructura de seguridad para administrar el riesgo con eficacia y tienen la responsabilidad de entender la relación entre las necesidades comerciales y la seguridad de TI.

Para obtener esta certificación, los profesionales deben aprobar el examen, adherirse a un código ético y presentar pruebas verificadas de que tienen una experiencia laboral de cinco años en seguridad de la información.

Según la ISACA, menciona los principales objetivos de esta certificación como a continuación se mencionan:

- Desarrollar modelos de riesgos que midan mejor los riesgos de seguridad y los potenciales impactos sobre el negocio.
- Aumentar la calidad de la gestión ejecutiva de las nuevas amenazas y las ya existentes, a través de la convergencia entre la organización y las medidas de seguridad
- Impulsar la unificación del enlace entre la seguridad de las organizaciones y los organismos gubernamentales y legislativos, informándoles de las mejores prácticas en seguridad.
- Continuar definiendo la cualificación, certificación y formación de los Directores de Seguridad - Chief Security Officer (CSO)/Chief Information Security Officer (CISO)- y otros puestos.

Instituto Mexicano de Auditores Internos, IMAI

El Instituto Mexicano de Auditores Internos, A.C. (IMAI) fue constituido en 1984, está dedicado a la capacitación e investigación en de Auditoría Interna y Control.

A través del IMAI los profesionales de la auditoría interna permanecen actualizados para cumplir con las responsabilidades que tienen a su cargo en diferentes sectores de la industria, el comercio y los servicios, tanto en el sector público como privado y social.

De acuerdo al IMAI su misión es “promover el mejoramiento constante de la Práctica Profesional de la Auditoría Interna, para fortalecer el prestigio de esta profesión y de quienes la practican”.

El objetivo principal del Instituto es “la superación profesional de sus miembros”, mediante lo siguiente:

El mejoramiento de la práctica Profesional de la Auditoría Interna.

Desarrollar y mantener la unión y cooperación efectiva entre los profesionales de la Auditoría Interna.

Promover la difusión de las normas de actuación profesional a través de las cuales los auditores internos puedan medir y regular su propio desempeño y las organizaciones puedan esperar servicios de calidad.

Establecer y mantener el prestigio de la Auditoría Interna a través de la investigación y la divulgación de conocimientos técnicos de enfoques conceptuales relativos al ejercicio profesional de esta disciplina y materias afines.

Establecer y mantener vínculos con otros organismos profesionales o docentes y entidades públicas o privadas, para identificación y desarrollo de aspectos que permitan elevar la calidad de la práctica de la Auditoría Interna y el Control en general, dentro de las organizaciones.

Institute of Internal Auditors, IIA

El Institute of Internal Auditors (IIA) –organización profesional con sede en Estados Unidos, con más de 70.000 miembros en todo el mundo y 60 años de existencia– anualmente organiza su Conferencia Internacional, la que habitualmente congrega a más de un millar de auditores de todos los continentes.

EI IIA es reconocido mundialmente como una autoridad, pues es el principal educador y el líder en la certificación, la investigación y la guía tecnológica en la profesión de la audítoría interna.

El desarrollo de los Estándares de la Práctica Profesional de Auditoría Interna, así como las Certificaciones de Auditor Interno (CIA), de Auto evaluación de Control (CCSA) y de Auditor Interno Gubernamental (CGAP), y su participación en el diseño del Enfoque COSO son sólo algunos de los hitos que han transformado al IIA en la entidad internacional señera en la profesión.

Establecen el IIA como el recurso de conocimiento primario sobre las mejores prácticas y publicaciones(cuestiones) que afectan la profesión interna de auditoría. Encuentran las necesidades de desarrollo de profesional que se desarrollan de médicos internos de auditoría.[2]

Certified Internal Auditor, CIA

El IIA cuenta con su propia Certificación de Auditores Internos CIA, la cual se da tanto a proveedores de estos servicios.

Contar con profesionales certificados en auditoría interna, para la organización significa contar con un valioso recurso para la dirección y el consejo de administración, que ayuda a garantizar el avance en la dirección correcta para el logro de sus metas y objetivos. La certificación como auditor interno la otorga el Institute of Internal Auditors que es una asociación internacional de profesionales especialistas en auditoría interna, administración de riesgos, gobierno corporativo. control interno, auditoría a tecnología de información, educación y seguridad[3].

La Certificación CIA (Certified Internal Auditor) cumplió 30 años como un reconocimiento mundial que demuestra la capacidad profesional, el dominio de los estándares y de las normas internacionales de la práctica de auditoría interna, el manejo de los principios y controles de la tecnología de información, y las estrategias emergentes para mejorar a la organización y a su gobierno corporativo.

Para obtener la certificación CIA además de los requisitos educacionales y de experiencia sino el apego al Código de Ética, y el desarrollo profesional continuo.

[2]http://www.theiia.org/ [http://www.theiia.org/]http://www.theiia.org/index.cfm?doc_id=5119 http://www.facpece.org.ar/boletines/37/60a-confederacion.htm.
[3]http://www.isaca.com.mx/ [http://www.isaca.com.mx]

Los rigurosos requerimientos de este programa, aseguran que los auditores internos que logran la certificación, están armados con herramientas invaluables que pueden ser aplicadas globalmente en cualquier organización o industria.[4]

Para mantener la certificación CIA se requiere que los CIA mantengan y actualicen sus habilidades y conocimientos. Los CIA practicantes deben completar e informar cada dos años, 80 horas de educación profesional continua.

Mejores prácticas de la auditoría en informática

Las mejores prácticas son directrices que permiten a las empresas modelar sus procesos para que se ajusten a sus propias necesidades, proporcionan a las empresas y/o organizaciones métodos utilizados para estandarizar procesos y administrar de una mejor manera los entornos de TI.

Las empresas que deseen utilizar un enfoque basado en mejores prácticas para la estandarización de estas directrices, tienen como opción varias metodologías que serán descritas a lo largo de este capítulo.

A continuación se presenta un marco en el que se pueden encerrar las mejores prácticas de la auditoría, dado que todas responden al siguiente esquema[5]:

Identificación	Identificación Buscan definir las necesidades de la organización que deben ser identificadas respecto de la auditoría, así como las debilidades propias, a fin de determinar el objetivo a seguir.
Administración de calidad total	Administración de calidad total Incorporan conceptos de calidad total aplicada a la auditoría sobre la base de la mejora continua, con el pertinente concepto de medición y evaluación de resultados.
Comunicación	Comunicación Buscan establecer un proceso de comunicación interna que propenda a informar lo actuado, lo planeado y las mejoras obtenidas.
Tecnología	Tecnología Recomiendan emplear recursos de tecnología informática al proceso de auditorías privilegiando la eficacia, eficiencia y oportunidad en los resultados de las revisiones.
Interrelación externa	Interrelación externa Proponen mantener estrechas relaciones profesionales con otras gerencias de auditoría a fin de intercambiar estrategias, criterios y resultados.
Agente de cambio	Agente de cambio Proporcionan las bases para posicionar a la Auditoría como un agente de cambio en la organización a fin de implementar la auto evaluación del control.

[4] http://www.theiia.org/index.cfm?doc_id=56
[5] [bib-ti-complejos]

Reingeniería de auditoría	Reingeniería de auditoría Proponen el cambio funcional proyectando a los auditores como facilitadores de la auto evaluación del control.

Aseguramiento de la información

El aseguramiento de la información es la base sobre la que se construye la toma de decisiones de una organización. Sin aseguramiento, las empresas no tienen certidumbre de que la información sobre la que sustentan sus decisiones es confiable, segura y está disponible cuando se le necesita.

Definimos Aseguramiento de la Información como “la utilización de información y de diferentes actividades operativas, con el fin de proteger la información, los sistemas de información y las redes de forma que se preserve la disponibilidad, integridad, confidencialidad, autenticación y el no repudio, ante el riesgo de impacto de amenazas locales, o remotas a través de comunicaciones e Internet”[6].

Una tarea de aseguramiento puede darse a cualquier nivel, por lo que a continuación se describe brevemente las más importantes.

Aseguramiento de los Datos	Aseguramiento de los Datos Referente la información histórica o prospectiva, probabilística e indicadores de desempeño.
Aseguramiento de los Procesos	Aseguramiento de los Procesos Basado principalmente en controles internos y procedimientos establecidos para la protección de intereses.
Aseguramiento del Comportamiento	Aseguramiento del Comportamiento Conformidad con normas, regulaciones o mejores prácticas.
Aseguramiento del Sistema de Gestión	Aseguramiento del Sistema de Gestión En la que los objetivos del negocio son establecidos para proteger a todos los involucrados: directivos y empleados.

Aseguramiento de la calidad de la información

La administración del aseguramiento de la calidad valida que los sistemas de información producidos por la función de sistemas de información logren las metas de calidad y que el desarrollo, implementación, operación, y mantenimiento de los sistemas de información, cumplan con un conjunto de normas de calidad[7].

En la actualidad es más común ver que los usuarios se están haciendo más exigentes en términos de la calidad del software que emplean para realizar su trabajo, por ello actualmente el aseguramiento de la calidad ha tomado mayor importancia en muchas organizaciones.

Las organizaciones se están comprometiendo en proyectos de sistemas de información que tienen requerimientos de calidad más estrictos y se preocupan cada vez más sobre sus responsabilidades legales al producir y vender software defectuoso.

Debido a esto, mejorar la calidad del software es parte de una tendencia universal entre las organizaciones proveedoras para mejorar la calidad de los productos y los servicios que ofrecen, agregando valor a los controles de producción, implementación, operación y mantenimiento del software.

[6] [bib-guia-17799]
[7] [bib-guia-17799]

Control Objectives for Information and related Technology, COBIT

COBIT, lanzado en 1996, es una herramienta de gobierno[8] de TI que ha cambiado la forma en que trabajan los profesionales de TI.

De acuerdo a ISACA, COBIT es:

Una herramienta que permite evaluar la calidad del soporte de TI actual de la organización, vinculando los distintos procesos del negocio con los recursos informáticos que los sustentan.

COBIT establece un diagnóstico que permite definir las metas desde el punto de vista de seguridad y control que le serán de utilidad para la organización para cada uno de sus procesos, pudiendo entonces establecer un plan de acción para lograr estas mejoras, y posteriormente identificar los lineamientos para sustentar un proceso de monitoreo y mejora continua sobre las soluciones implementadas.

La manera en que COBIT provee este marco para el control y la gobernabilidad de TI se puede presentar en forma sintética a partir de sus principales características, que a continuación serán descritas.

Estructura de CUBO

La estructura de cubo es la capacidad que brinda COBIT de poder trabajar (con sus objetivos de control) desde tres puntos de vista diferentes; los procesos, los recursos de TI, y las características que debe reunir la información para ser considerada adecuada a las necesidades de la organización.

Esta estructura, al vincular estos tres puntos de vista brinda un enfoque global que apoya a la planificación estratégica, fundamentalmente a través de promover las funciones ligadas a la gobernabilidad de TI, la cual es básica para asegurar el logro de las metas de la organización.

Esta estructura permite vincular las expectativas de la Dirección con las de la Gerencia de TI, manejando lineamientos entendibles por las Gerencias de negocio y los dueños de los procesos.

Dominios

Permite agrupar los objetivos de control de COBIT en distintas áreas de actividad de la organización. Los cuatro dominios principales son:

- Planificación y organización,
- Adquisición e implantación,
- Soporte y servicios, y
- Monitoreo.

Como su nombre indica, cada uno de estos dominios están enfocados a los diferentes niveles y departamento que pueden existir en una organización.

Modelo de madurez (Maturity Model)

Ofrece las bases para el entendimiento y la evaluación de las condiciones actuales de seguridad y control de los procesos del ambiente de TI de una organización. Este modelo provee las bases para la evaluación de las principales funciones del área de TI, a través de la consideración de cada uno de sus procesos clave, a los cuales se les asignará un valor de cero a cinco, según las definiciones siguientes:

Inexistente	Inexistente

[8] http://www.monografias.com/trabajos4/derpub/derpub.shtml

	Ausencia total de cualquier proceso o control reconocible.
1. Inicial	1. Inicial Existe evidencia de que la organización ha reconocido la necesidad de mejorar los procesos o controles.
2. Repetible	2. Repetible Se han desarrollado procesos donde se siguen procedimientos similares por diferentes personas para la misma tarea.
3. Definido	3. Definido Los procedimientos han sido estandarizados y documentados y son comunicados a través de la capacitación.
4. Gestionado o administrado	4. Gestionado o administrado Es posible monitorear y medir el cumplimiento de los procedimientos y tomar acciones cuando los procesos no están funcionando efectivamente.
5. Optimizado	5. Optimizado Los procesos han sido redefinidos al nivel de las mejores prácticas, basados en los resultados de mejoras continuas y el modelo de madurez con otras organizaciones.

Information Technology Infraestructure Library, ITIL

ITIL es un conjunto de las mejores prácticas para la gestión de servicios de TI que ha evolucionado desde 1989, comenzó como un conjunto de procesos que utilizaba el gobierno del Reino Unido para mejorar la gestión de los servicios de TI y ha sido adoptado por la industria, como base de una gestión satisfactoria de los servicios de TI[9].

ITIL describe las mejores prácticas que se pueden utilizar y mejor se adecuan a una organización, incluye cinco disciplinas que proporcionan las empresas flexibilidad y estabilidad para ofrecer servicios de TI[10] , estas son:

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

Incluye también cinco disciplinas que soportan los servicios TI de calidad y bajo costo de las empresas 6, estas son:

- Gestión del nivel de servicio,
- Gestión de la disponibilidad,

[9] [bib-sun-itil]
[10] [bib-conceptos-itil]

- Gestión de la capacidad,
- Gestión financiera para servicios TI, y
- Gestión de la continuidad de los servicios TI.

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

BS 7799 e ISO 17799

En 1995 el British Standard Institute (BSI) publica la norma BS 7799, un código de buenas prácticas para la gestión de la seguridad de la información. En 1998 también el BSI publica la norma BS 7799-2 con especificaciones para los sistemas de gestión de la seguridad de la información. Tras una revisión de ambas partes de BS 7799, la primera es adoptada como norma ISO en el año 2000 y denominada ISO/IEC 17799.

Actualmente las empresas deben asegurar que sus recursos y la propiedad intelectual estén protegidos y que los clientes se sientan seguros de realizar negocios.

De acuerdo al BSI[11]:

BS CIA 7799 es una guía de auditoría del Sistema de Gestión de Seguridad de la Información (ISMS) basada en los requisitos que deben ser cubiertos por la organización. Contiene especificaciones para certificar los dominios individuales de seguridad para poder registrarse a esta norma.

ISO 17799 define la seguridad de la información como la preservación de la confidencialidad, la integridad y la disponibilidad de la misma. Esta norma global basada en la norma BS 7799 que define las mejores prácticas para gestión de la seguridad de la información, consta de las siguientes partes:

Define un conjunto de objetivos principales e identifica un conjunto de controles de seguridad, que son medidas que se pueden adoptar para cumplir los objetivos de la norma.

Especifica los controles de seguridad que se pueden utilizar, basándose en los resultados de una evaluación de gestión de riesgos, como base para una certificación formal d una empresa TI bajo la norma BS 7799.

ISO 17799 establece la base común para desarrollar normas de seguridad de control de las organizaciones, definiendo diez dominios de control que cubren por completo la Gestión de la Seguridad de la Información.

Dominios:

- Política de seguridad,
- Aspectos organizativos para la seguridad,
- Clasificación y control de activos,
- Seguridad ligada al personal,
- Seguridad física y del entorno,
- Gestión de comunicaciones y de operaciones,
- Control de accesos,

[11] *Gestión de la seguridad de la información ISO 17799*- S2 Grupo –Antonio Villalón Huerta

- Desarrollo y mantenimiento de sistemas,
- Gestión de continuidad del negocio, y
- Conformidad.

British Standard BS 15000

El estándar fue creado por el Grupo de Gestión de Servicio de BSI, este grupo está conformado por expertos de la industria que representan distintas organizaciones e industrias, todos ellos con prácticas de excelencia en la Gestión de Servicio.

En la década de 1980 se inició su estudio con la publicación de un código de prácticas que cubría cuatro procesos centrales. En 1998 se sustituyó con los 13 procesos de la figura anterior, así la primer edición como estándar se publicó en el año 2000. Al mismo tiempo también se publicó el libro *IT Service Management* (PD 0015), este libro de trabajo es utilizado para la revisión de la calidad del proceso de servicio.[12]

Es el primer estándar mundial para la gestión de servicios de TI. Se dirige tanto a proveedores de la gestión de servicios, así como a empresas que subcontratan o gestionan sus propios requisitos.

BS 15000 especifica un conjunto de procesos de gestión interrelacionados basados en gran medida en el marco de trabajo ITIL y se pretende que formen una base de una auditoría del servicio gestionado.

En esencia, la norma BS 15000 contiene conceptos cuidadosamente concebidos que definen y demarcan los elementos que una organización debe tener en cuenta para estructurar y soportar los Servicios de IT a sus clientes, ya sean internos o externos.

El estándar BS 15000 consiste de 2 partes[13]:

La Parte 1 son las especificaciones del sistema de gestión, y contiene alrededor de 14 páginas de requisitos normativos. Está estructurado de acuerdo a las reglas para especificaciones fijadas por el BSI.

En general BS 15000 define lo que requiere hacer y cumplir una organización para alcanzar su certificación respecto al estándar. Cubre el cumplimiento de requisitos para:

- El Sistema de Gestión (Management Systems),
- El Planeamiento del servicio (Service Planning),
- Las Relaciones entre procesos (Process Reationships),
- La Estructuración del Servicio (Delivery Service),
- El Control, y
- La Liberación de Servicios (Release).

La Parte 2 del BS 15000 es conocida como el *Code of Practice* y se extiende en detalle sobre cada requisito, ofreciendo dirección y guía al Proveedor del Servicio que desee alcanzar el estándar.

Sigue la misma estructura de la Parte 1, pero es un poco menos formal en terminología. Provee guía y dirección practica respecto a como debe ser considerado el proceso, como debe ser documentado, que debería ser realizado, y que debería monitorearse para lograr una efectividad real del proceso en la práctica.

Su estructura y vocabulario está cuidadosamente manejado, logrando que las dos partes de la norma manejen los mismos conceptos y sean totalmente complementarias.

[12] http://www.nhmadrid.com/itil_bs15000.htm
[13] Miguel Díaz S.: Ingeniero de Sistemas. / Socio consultor de AUDISIS / Líder de proyectos de adopción de ITL en Argentina y Venezuela

Committee of Sponsoring Organizations, COSO

El informe es un manual de control interno que publica el Instituto de Auditores Internos de España en colaboración con la empresa de auditoría Coopers & Lybrand. En control interno lo último que ha habido es el informe COSO (Sponsoring Organizations of the Treadway Commission), es denominado así, porque se trata de un trabajo que encomendó el Instituto Americano de Contadores Públicos, la Asociación Americana de Contabilidad, el Instituto de Auditores Internos que agrupa a alrededor de cincuenta mil miembros y opera en aproximadamente cincuenta países, el Instituto de Administración y Contabilidad, y el Instituto de Ejecutivos Financieros. Ha sido hecho para uso de los consejos de administración de las empresas privadas en España y en los países de habla hispana.[14]

Normalmente en organizaciones medianas o grandes el implantar o monitorear un sistema de control interno sano se enfrentan a todo un desafío.

COSO[15] es una herramienta que puede asistirlo en la evaluación, auditoría, documentación, mejora y seguimiento del sistema de control interno.

COSO permite facilitar las actividades de los encargados del control interno, auditores internos y externos, y gerencias de las organizaciones preocupadas por mejorar sus resultados.

Esta herramienta permite construir o mejorar en sistema de control interno (total o parcial por ejemplo solo acotado al objetivo información contable) y de este modo recibir con tranquilidad la evaluación de los auditores externos que podrán así efectuar su tarea de atestiguamiento en forma más rápida y eficaz.

Según el informe COSO, los componentes que se interrelacionan para alcanzar los objetivos son los siguientes[16].

Ambiente de control

Elemento que proporciona disciplina y estructura, el ambiente de control se denomina en función de la integridad y competencia del personal de una organización; los valores éticos son un elemento esencial que afectan otros elementos del control

Evaluación de riesgos

Es la identificación y análisis de os riesgos que se relacionan con el logro de los objetivos; la administración debe cuantificar la magnitud, proyectar su probabilidad y sus posibles consecuencias:

En la dinámica actual de los negocios se debe prestar atención a diversos factores, entre ellos los avances tecnológicos.

Actividades de control

Ocurren a lo largo de la Organización en todos los niveles y en todas las funciones, incluyendo los procesos de aprobación, autorización, conciliaciones, etc. Las actividades de control se clasifican en:

- Controles preventivos,
- Controles detectivos,
- Controles correctivos,
- Controles manuales y de usuarios,

[14] http://www.info.ccss.sa.cr
[15] Instituto de Auditores Internos de España 1985 [http://www.datasec.com.uy/]
[16] V Reunión de Auditores Internos de Banca Central Exposición de Banco de México

- Controles de cómputo o de tecnología de información, y
- Controles administrativos.

Monitoreo y aprendizaje

Los controles internos deben ser “monitoreados” constantemente para asegurar que el proceso se encuentra operando como se planeó y comprobar que son efectivos ante los cambios de las situaciones que les dieron origen.

Las actividades de monitoreo constante pueden ser implantadas en los propios procesos del negocio a través de evaluaciones separadas de la operación, es decir, mediante la auditoría interna o externa.

Información y comunicación

Se debe generar información relevante y comunicarla oportunamente de tal manera que permita a las personas entenderla y cumplir con sus responsabilidades.

Metodología de análisis y gestión de riesgos de los sistemas de información, MAGERIT

MAGERIT[17] es una metodología de análisis y gestión de riesgos de los sistemas de información de las administraciones públicas, emitida en el año 1997 por el Consejo Superior de Informática[18] y recoge las recomendaciones de las directivas de la Unión Europea en materia de seguridad de sistemas de información.

Esta metodología presenta un objetivo definido en el estudio de los riesgos que afectan los sistemas de información y el entorno de ellos haciendo unas recomendaciones de las medidas apropiadas que deberían adoptarse para conocer, prevenir, evaluar y controlar los riesgos investigados.

MAGERIT desarrolla el concepto de control de riesgos en las guías de procedimientos, técnicas, desarrollo de aplicaciones, personal y cumplimiento de normas legales.

MAGERIT persigue los siguientes objetivos:

- Concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de atenderlos a tiempo,
- Ofrecer un método sistemático para analizar tales riesgos,
- Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control, y
- Apoyar la preparación a la organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

Asimismo, se ha cuidado la uniformidad de los informes que recogen los hallazgos y las conclusiones de un proyecto de análisis y gestión de riesgos: modelo de valor, mapa de riesgos, evaluación de salvaguardas, estado de riesgo, informe de insuficiencias, y plan de seguridad.

Sarbanes-Oxley, SOX

Actualmente las organizaciones están expuestas a ataques que propicien la pérdida de información y fraudes, para minimizar los riesgos de fraude, las empresas se requieren revisar, evaluar y fortalecer sus propios controles internos.

[17] Ministerio de Administraciones Públicas, Madrid, 16 de junio de 2005
[18] http://www.csi.map.es/csi

La ley Sarbanes-Oxley, emitida por el gobierno estadounidense el 30 de julio de 2002, fue preparada a partir de los escándalos financieros de los últimos años y establece una serie de nuevos requisitos tanto para las empresas estadounidenses como para las extranjeras, tenedoras y subsidiarias, que cotizan en la bolsa de valores estadounidense (New York Stock Exchange, NYSE), con la idea de regular el gobierno corporativo.

Estos requerimientos deberían estar cumplidos a partir del 15 de diciembre de 2003, pero la Comisión de Valores de Estados Unidos (Security Exchange Commision,SEC) ya dio, el pasado mes de mayo, una prórroga para las empresas extrajeras de dos años, no más allá del 31 de julio de 2005. Para las empresas estadounidenses la prórroga es de sólo un año, no más allá del 31 de octubre de 2004.[19]

La ley Sarbanes-Oxley, tiene como objetivo crear un marco transparente para las actividades de las empresas multinacionales que cotizan en la Bolsa.

Esta ley estadounidense contempla una revisión mucho más rigurosa de los datos financieros que una empresa declara en sus estados financieros y que utiliza para sus controles internos[20].

Sin embargo, el control interno es un proceso efectuado por los niveles directivos y gerenciales, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos dentro de sus áreas, teniendo como principales objetivos:

- Efectividad y eficiencia de las operaciones,
- Confiabilidad de la información financiera,
- Cumplimiento de las normas y leyes que sean aplicables, y
- Salvaguardia de los recursos.

Esta ley lleva mucho más lejos las disposiciones sobre la obligación de la gerencia de asegurar adecuados controles internos por lo que cuenta con una sección de normas y reglas que dispone que los auditores deben incluir lo siguiente:

- El alcance de las pruebas del auditor de la estructura de control interno,
- Los hallazgos del auditor con respectos a dicha pruebas, y
- Una evaluación sobre dicha estructura de control.

Dentro de esta ley existen 3 secciones que involucran directamente al departamento de TI y que son la 302, 404 y 409, cuyo contenido se explica brevemente a continuación[21].

La cláusula 302. Habla de la obligación de generar reportes donde muestren el resultado financiero de la empresa[22] y que este debe de estar avaluado en cuanto a su integridad.

La cláusula 404 nos dice que deben existir procedimientos[23] y políticas [24] que aseguren la integridad de la información así como la disponibilidad de ella.

Por último la cláusula 409 indica que toda organización debe de notificar en menos de 48 hrs. cuando uno de los procesos de la cadena de proveedores no va a ser entregado a tiempo[25] y esto afecte de manera seria a las ventas[26] de la organización.

[19] [bib-rusbacki-2004]
[20] http://www.datasec.com.uy/ oxely-coso.pdf
[21] [bib-novell-sarbanes-oxley]
[22] http://www.monografias.com/trabajos11/empre/empre.shtml
[23] http://www.monografias.com/trabajos13/mapro/mapro.shtml
[24] http://www.monografias.com/trabajos10/poli/poli.shtml
[25] http://www.monografias.com/trabajos6/meti/meti.shtml
[26] http://www.monografias.com/trabajos12/evintven/evintven.shtml

Normas, técnicas y procedimientos de auditoría en informática.

El desarrollo de una auditoría se basa en la aplicación de normas, técnicas y procedimientos de auditoría. Para nuestro caso, estudiaremos aquellas enfocadas a la auditoría en informática.

Es fundamental mencionar que para el auditor en informática conocer los productos de software que han sido creados para apoyar su función aparte de los componentes de la propia computadora resulta esencial, esto por razones económicas y para facilitar el manejo de la información.

El auditor desempeña sus labores mediante la aplicación de una serie de conocimientos especializados que vienen a formar el cuerpo técnico de su actividad. El auditor adquiere responsabilidades, no solamente con la persona que directamente contratan sus servicios, sino con un número de personas desconocidas para él que van a utilizar el resultado de su trabajo como base para tomar decisiones.

La auditoría no es una actividad meramente mecánica, que implique la aplicación de ciertos procedimientos cuyos resultados, una vez llevados a cabo son de de carácter indudable. La auditoría requiere el ejercicio de un juicio profesional, sólido maduro, para juzgar los procedimientos que deben seguirse y estimar los resultados obtenidos[27].

Normas.

Según se describe en [bib-imcp], las normas de auditoría son los requisitos mínimos de calidad relativos a la personalidad del auditor, al trabajo que desempeña ya la información que rinde como resultado de este trabajo.

Las normas de auditoría se clasifican en:

a. Normas personales.
b. Normas de ejecución del trabajo.
c. Normas de información.

Normas personales	Normas personales son cualidades que el auditor debe tener para ejercer sin dolo una auditoría, basados en un sus conocimientos profesionales así como en un entrenamiento técnico, que le permita ser imparcial a la hora de dar sus sugerencias.
Normas de ejecución del trabajo	Normas de ejecución del trabajo son la planificación de los métodos y procedimientos, tanto como papeles de trabajo a aplicar dentro de la auditoría.
Normas de información	Normas de información son el resultado que el auditor debe entregar a los interesados para que se den cuenta de su trabajo, también es conocido como informe o dictamen.

[27] [bib-imcp]

Técnicas.

Se define a las técnicas de auditoría como “los métodos prácticos de investigación y prueba que utiliza el auditor para obtener la evidencia necesaria que fundamente sus opiniones y conclusiones, su empleo se basa en su criterio o juicio, según las circunstancias”.

Al aplicar su conocimiento y experiencia el auditor, podrá conocer los datos de la empresa u organización a ser auditada, que pudieran nesecitar una mayor atención.

Las técnicas procedimientos están estrechamente relacionados, si las técnicas no son elegidas adecuadamente, la auditoría no alcanzará las normas aceptadas de ejecución, por lo cual las técnicas así como los procedimientos de auditoría tienen una gran importancia para el auditor.

Según el IMCP en su libro *Normas y procedimientos de auditoría* las técnicas se clasifican generalmente con base en la acción que se va a efectuar, estas acciones pueden ser oculares, verbales, por escrito, por revisión del contenido de documentos y por examen físico.

Siguiendo esta clasificación las técnicas de auditoría se agrupan específicamente de la siguiente manera:

- Estudio General
- Análisis
- Inspección
- Confirmación
- Investigación
- Declaración
- Certificación
- Observación
- Cálculo

Procedimientos.

Al conjunto de técnicas de investigación aplicables a un grupo de hechos o circunstancias que nos sirven para fundamentar la opinión del auditor dentro de una auditoría, se les dan el nombre de procedimientos de auditoría en informática.

La combinación de dos o más procedimientos, derivan en programas de auditoría, y al conjunto de programas de auditoría se le denomina plan de auditoría, el cual servirá al auditor para llevar una estrategia y organización de la propia auditoría.

El auditor no puede obtener el conocimiento que necesita para sustentar su opinión en una sola prueba, es necesario examinar los hechos, mediante varias técnicas de aplicación simultánea.

En General los procedimientos de auditoría permiten:

- Obtener conocimientos del control interno.
- Analizar loas características del control interno.
- Verificar los resultados de control interno.
- Fundamentar conclusiones de la auditoría.

Por esta razón el auditor deberá aplicar su experiencia y decidir cuál técnica o procedimiento de auditoría serán los mas indicados par obtener su opinión.

Análisis de datos.

Dentro de este trabajo, desarrollaremos diversos tipos de técnicas y procedimientos de auditoría, de los cuales destacan el análisis de datos, ya que para las organizaciones el conjunto de datos o información son de tal importancia que es necesario verificarlos y comprobarlos, así también tiene la misma importancia para el auditar ya que debe de utilizar diversas técnicas para el análisis de datos, basados en [bib-solis-2002], las cuales se describen a continuación.

Comparación de programas	Comparación de programas esta técnica se emplea para efectuar una comparación de código (fuente, objeto o comandos de proceso) entre la versión de un programa en ejecución y la versión de un programa piloto que ha sido modificado en forma indebida, para encontrar diferencias.
Mapeo y rastreo de programas	Mapeo y rastreo de programas esta técnica emplea un software especializado que permite analizar los programas en ejecución, indicando el número de veces que cada línea de código es procesada y las de las variables de memoria que estuvieron presentes.
Análisis de código de programas	Análisis de código de programas Se emplea para analizar los programas de una aplicación. El análisis puede efectuarse en forma manual (en cuyo caso sólo se podría analizar el código ejecutable).
Datos de prueba	Datos de prueba Se emplea para verificar que los procedimientos de control incluidos los programas de una aplicación funcionen correctamente. Los datos de prueba consisten en la preparación de una serie de transacciones que contienen tanto datos correctos como datos erróneos predeterminados.
Datos de prueba integrados	Datos de prueba integrados Técnica muy similar a la anterior, con la diferencia de que en ésta se debe crear una entidad, falsa dentro de los sistemas de información.
Análisis de bitácoras	Análisis de bitácoras Existen varios tipos de bitácoras que pueden ser analizadas por el auditor, ya sea en forma manual o por medio de programas especializados, tales como bitácoras de fallas del equipo, bitácoras de accesos no autorizados, bitácoras de uso de recursos, bitácoras de procesos ejecutados.

Simulación paralela	Simulación paralela Técnica muy utilizada que consiste en desarrollar programas o módulos que simulen a los programas de un sistema en producción. El objetivo es procesar los dos programas o módulos de forma paralela e identificar diferencias entre los resultados de ambos.

Monitoreo.

Dentro de las organizaciones todos los procesos necesitan ser evaluados a través del tiempo para verificar su calidad en cuanto a las necesidades de control, integridad y confidencialidad, este es precisamente el ámbito de esta técnica, a continuación se muestran los procesos de monitoreo:

- M1 Monitoreo del proceso.
- M2 Evaluar lo adecuado del control Interno.
- M3 Obtención de aseguramiento independiente.
- M4 Proveer auditoría independiente.

M1 Monitoreo del proceso

Asegura el logro de los objetivos para los procesos de TI, lo cual se logra definiendo por parte de la gerencia reportes e indicadores de desempeño y la implementación de sistemas de soporte así como la atención regular a los reportes emitidos.

Para ello la gerencia podrá definir indicadores claves de desempeño y factores críticos de éxito y compararlos con los niveles propuestos para evaluar el desempeño de los procesos de la organización.

M2 Evaluar lo adecuado del control Interno

Asegura el logro de los objetivos de control interno establecidos para los procesos de TI, para ello se debe monitorear la efectividad de los controles internos a través de actividades administrativas, de supervisión, comparaciones, acciones rutinarias, evaluar su efectividad y emitir reportes en forma regular[28].

M3 Obtención de aseguramiento independiente

Incrementa los niveles de confianza entre la organización, clientes y proveedores, este proceso se lleva a cabo a intervalos regulares de tiempo.

Para ello la gerencia deberá obtener una certificación o acreditación independiente de seguridad y control interno antes de implementar nuevos servicios de tecnología de información que resulten críticos, así como para trabajar con nuevos proveedores de servicios de tecnología de información, luego la gerencia deberá adoptar como trabajo rutinario tanto hacer evaluaciones periódicas sobre la efectividad de los servicios de tecnología de información, de los proveedores de estos servicios así como también asegurarse el cumplimiento de los compromisos contractuales de los servicios de tecnología de información y de los proveedores de dichos servicios.

[28] Http://Ilustrados.com/Publicaciones/Epyfapup.php

M4 Proveer auditoría independiente.

Incrementa los niveles de confianza de recomendaciones basadas en mejores prácticas de su implementación, lo que se logra con el uso de auditorías independientes desarrolladas a intervalos regulares de tiempo.

Para ello la gerencia deberá establecer los estatutos para la función de auditoría, destacando en este documento la responsabilidad, autoridad y obligaciones de la auditoría.

El auditor deberá ser independiente del auditado, esto significa que los auditores no deberán estar relacionados con la sección o departamento que esté siendo auditado y en lo posible deberá ser independiente de la propia empresa, esta auditoría deberá respetar la ética y los estándares profesionales, seleccionando para ello auditores que sean técnicamente competentes, es decir que cuenten con habilidades y conocimientos que aseguren tareas efectivas y eficientes de auditoría informática.

La función de la auditoría informática deberá proporcionar un reporte que muestre los objetivos, período de cobertura, naturaleza y trabajo de auditoría realizado, así como también la organización, conclusión y recomendaciones relacionadas con el trabajo de auditoría informática llevado a cabo.

Análisis de bitácoras.

Hoy en día los sistemas de cómputo se encuentran expuestos a distintas amenazas, las vulnerabilidades de los sistemas aumentan, al mismo tiempo que se hacen más complejos, el número de ataques también aumenta, por lo anterior las organizaciones deben reconocer la importancia y utilidad de la información contenida en las bitácoras de los sistemas de computo así como mostrar algunas herramientas que ayuden a automatizar el proceso de análisis de las mismas.

El crecimiento de Internet enfatiza esta problemática, los sistemas de cómputo generan una gran cantidad de información, conocidas como bitácoras o archivos logs, que pueden ser de gran ayuda ante un incidente de seguridad, así como para el auditor.

Una bitácora puede registrar mucha información acerca de eventos relacionados con el sistema que la genera los cuales pueden ser:

- Fecha y hora.
- Direcciones IP origen y destino.
- Dirección IP que genera la bitácora.
- Usuarios.
- Errores.

La importancia de las bitácoras es la de recuperar información ante incidentes de seguridad, detección de comportamiento inusual, información para resolver problemas, evidencia legal, es de gran ayuda en las tareas de cómputo forense.

Las Herramientas de análisis de bitácoras mas conocidas son las siguientes:

- Para UNIX, Logcheck, SWATCH.
- Para Windows, LogAgent

Las bitácoras contienen información crítica es por ello que deben ser analizadas, ya que están teniendo mucha relevancia, como evidencia en aspectos legales.

El uso de herramientas automatizadas es de mucha utilidad para el análisis de bitácoras, es importante registrar todas las bitácoras necesarias de todos los sistemas de cómputo para mantener un control de las mismas.

Técnicas de auditoría asistida por computadora

La utilización de equipos de computación en las organizaciones, ha tenido una repercusión importante en el trabajo del auditor, no sólo en lo que se refiere a los sistemas de información, sino también al uso de las computadoras en la auditoría.

Al llevar a cabo auditorías donde existen sistemas computarizados, el auditor se enfrenta a muchos problemas de muy diversa condición, uno de ellos, es la revisión de los procedimientos administrativos de control interno establecidos en la empresa que es auditada.

La utilización de paquetes de programas generalizados de auditoría ayuda en gran medida a la realización de pruebas de auditoría, a la elaboración de evidencias plasmadas en los papeles de trabajo.

Según [bib-zavaro-martinez] las técnicas de auditoría Asistidas por Computadora (CAAT) son la utilización de determinados paquetes de programas que actúan sobre los datos, llevando a cabo con más frecuencia los trabajos siguientes:

- Selección e impresión de muestras de auditorías sobre bases estadísticas o no estadísticas, a lo que agregamos, sobre la base de los conocimientos adquiridos por los auditores.
- Verificación matemática de sumas, multiplicaciones y otros cálculos en los archivos del sistema auditado.
- Realización de funciones de revisión analítica, al establecer comparaciones, calcular razones, identificar fluctuaciones y llevar a cabo cálculos de regresión múltiple.
- Manipulación de la información al calcular subtotales, sumar y clasificar la información, volver a ordenar en serie la información, etc.
- Examen de registros de acuerdo con los criterios especificados.
- Búsqueda de alguna información en particular, la cual cumpla ciertos criterios, que se encuentra dentro de las bases de datos del sistema que se audita.

Consecuentemente, se hace indispensable el empleo de las CAAT que permiten al auditor, evaluar las múltiples aplicaciones específicas del sistema que emplea la unidad auditada, el examinar un diverso número de operaciones específicas del sistema, facilitar la búsqueda de evidencias, reducir al mínimo el riesgo de la auditoría para que los resultados expresen la realidad objetiva de las deficiencias, así como de las violaciones detectadas y elevar notablemente la eficiencia en el trabajo.

Teniendo en cuenta que se hacía imprescindible auditar sistemas informáticos; así como diseñar programas auditores, se deben incorporar especialistas informáticos, formando equipos multidisciplinarios capaces de incursionar en las auditorías informáticas y comerciales, independientemente de las contables, donde los auditores que cumplen la función de jefes de equipo, están en la obligación de documentarse sobre todos los temas auditados.

De esta forma los auditores adquieren más conocimientos de los diferentes temas, pudiendo incluso, sin especialistas de las restantes materias realizar análisis de esos temas, aunque en ocasiones es necesario que el auditor se asesore con expertos, tales como, ingenieros industriales, abogados, especialistas de recursos humanos o de normalización del trabajo para obtener evidencia que le permita reunir elementos de juicio suficientes.

Evaluación del control interno.

En un ambiente de evolución permanente, determinado por las actuales tendencias mundiales, las cuales se centran en el plano económico soportadas por la evolución tecnológica, surge la necesidad de que la función de auditoría pretenda el mejoramiento de su gestión.

La práctica de nuevas técnicas para evaluar el control interno a través de las cuales, la función de auditoría informática pretende mejorar la efectividad de su función y con ello ofrecer servicios más eficientes y con un valor agregado.

La evolución de la teoría del control interno se definió en base a los principios de los controles como mecanismos o prácticas para prevenir, identificar actividades no autorizadas, más tarde se incluyó el concepto de lograr que las cosas se hagan; la corriente actual define al control como cualquier esfuerzo que se realice para aumentar las posibilidades de que se logren los objetivos de la organización.

En este proceso evolutivo se considera actualmente, y en muchas organizaciones que el director de finanzas, contralor o al director de auditoría como los responsables principales del correcto diseño y adecuado funcionamiento de los controles internos.

Benchmarking

Las empresas u organizaciones deben buscar formas o fórmulas que las dirijan hacia una mayor calidad, para poder ser competitivos, una de estas herramientas o fórmulas es el Benchmarking.

Existen varios autores que han estudiado el tema, y de igual manera existen una gran cantidad de definiciones de lo que es benchmarking, a continuación se presentan algunas definiciones.

Benchmarking es el proceso continuo de medir productos, servicios y prácticas contra los competidores o aquellas compañías reconocidas como líderes en la industria.[29]

Esta definición presenta aspectos importantes tales como el concepto de continuidad, ya que benchmarking no sólo es un proceso que se hace una vez y se olvida, sino que es un proceso continuo y constante.

Según la definición anterior podemos deducir que se puede aplicar benchmarking a todas las facetas de las organizaciones, y finalmente la definición implica que el benchmarking se debe dirigir hacia aquellas organizaciones y funciones de negocios dentro de las organizaciones que son reconocidas como las mejores.

Entre otras definiciones tenemos la extraída del libro *Benchmarking* de Bengt, la cual es: “benchmarking es un proceso sistemático y continúo para comparar nuestra propia eficiencia en términos de productividad, calidad y prácticas con aquellas compañías y organizaciones que representan la excelencia”.

Como vemos en esta definición se vuelve a mencionar el hecho de que benchmarking es un proceso continuo, también se presenta el término de comparación y por ende remarca la importancia de la medición dentro del benchmark.

Estos autores se centran, a parte de la operaciones del negocio, en la calidad y en la productividad de las mismas, considerando el valor que tienen dichas acciones en contra de los costos de su realización lo cual representa la calidad, y la relación entre los bienes producidos y los recursos utilizados para su producción, lo cual se refiere a la productividad.

Por lo que podemos ver existen varias definiciones sobre lo que es benchmarking, y aunque difieren en algunos aspectos también se puede notar que concuerdan o presentan una serie de elementos comunes.

Para empezar en la mayoría de ellas se resalta el hecho de que benchmarking es un proceso continuo que al aplicarla en nuestra empresa resuelva los problemas de la misma, sino que es un proceso que se aplicará una y otra vez ya que dicho proceso está en búsqueda constante de las mejores prácticas de la industria, y como sabemos la industria está en un cambio constante y para adaptarse a dicho cambio desarrolla nuevas practicas, por lo que no se puede asegurar que las mejores prácticas de hoy lo serán también de mañana.

También se vio en las diferentes definiciones que este proceso no sólo es aplicable a las operaciones de producción, sino que puede aplicarse a todas la fases de las organizaciones, por lo que benchmarking

[29] [bib-kearns-1994]

es una herramienta que nos ayuda a mejorar todos los aspectos y operaciones del negocio, hasta el punto de ser los mejores en la industria, observando aspectos tales como la calidad y la productividad en el negocio.

De igual manera podemos concluir que es de suma importancia como una nueva forma de administrar ya que cambia la práctica de compararse sólo internamente a comparar nuestras operaciones en base a estándares impuestos externamente por las organizaciones conocidas como las de excelencia dentro de la industria.

Dentro del benchmarking existen los siguientes tipos:[30]

Benchmarking interno	Benchmarking interno en la mayor parte de las grandes organizaciones con múltiples divisiones o internacionales hay funciones similares en diferentes unidades de operación, una de las investigaciones de benchmarking más fácil es comparar estas operaciones internas, también debe contarse con facilidad con datos e información y no existir problemas de confidencialidad y los datos ser tan amplios y completos como se desee. Este primer paso en las investigaciones de benchmarking es una base excelente no sólo para descubrir diferencias de interés sino también centrar la atención en los temas críticos a que se enfrentara o que sean de interés para comprender las practicas provenientes de investigaciones externas, también pueden ayudar a definir el alcance de un estudio externo.
Benchmarking competitivo	Benchmarking competitivo los competidores directos de productos son contra quienes resulta más obvio llevar a cabo el benchmarking, ellos cumplirían, o deberían hacerlo, con todas las pruebas de comparabilidad, en definitiva cualquier investigación de benchmarking debe mostrar cuales son las ventajas y desventajas comparativas entre los competidores directos. Uno de los aspectos más importantes dentro de este tipo de investigación a considerar es el hecho que puede ser realmente difícil obtener información sobre las operaciones de los competidores, quizá sea imposible obtener información debido a que está patentada y es la base de la ventaja competitiva de la empresa.
Benchmarking genérico	Benchmarking genérico algunas funciones o procesos en las organizaciones son las mismas, el beneficio de esta forma de benchmarking, es que se

[30] http://Monografias.com/Trabajos4.html

pueden descubrir prácticas y métodos que no se implementan en la organización propia del investigador. Este tipo de investigación tiene la posibilidad de revelar lo mejor de las mejores prácticas, la necesidad de objetividad y receptividad por parte del investigador.

Que mejor prueba que la posibilidad de ponerlo en práctica si se pudiera obtener que el hecho de que la tecnología ya se ha probado y se encuentra en uso en todas partes, el benchmarking genérico requiere de una amplia conceptualización, pero con una comprensión cuidadosa del proceso genérico.

Computer Assisted Audit Techniques CAAT

Las técnicas de auditoría asistidas por computadora son de suma importancia para el auditor de TI cuando realiza una auditoría. CAAT (Computer Audit Assisted Techniques) incluyen distintos tipos de herramientas y de técnicas, las que más se utilizan son los software de auditoría generalizado, software utilitario, los datos de prueba y sistemas expertos de auditoría. Las CAAT se pueden utilizar para realizar varios procedimientos de auditoría incluyendo:

- Prueba de los detalles de operaciones y saldos.
- Procedimientos de revisión analíticos.
- Pruebas de cumplimiento de los controles generales de sistemas de información.
- Pruebas de cumplimiento de los controles de aplicación.

A continuación se enuncian algunas de las normas que el auditor de sistemas de información debe conocer. El ajustarse a estas normas no es obligatorio, pero el auditor de sistemas de información debe estar preparado para justificar cualquier incumplimiento a éstas.

Normas Internacionales de Auditoría emitidas por IFAC (International Federation of Accountants) en la NIA (Norma Internacional de Auditoría o International Standards on Auditing, ISA) 15 y 16, donde se establece la necesidad de utilizar otras técnicas además de las manuales.

Norma ISA 401, sobre Sistemas de Información por Computadora. SAS No. 94 (The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement audit) dice que en una organización que usa Tecnologías de Información, se puede ver afectada en uno de los siguientes cinco componentes del control interno: el ambiente de control, evaluación de riesgos, actividades de control, información, comunicación y monitoreo además de la forma en que se inicializan, registran, procesan y reporta las transacciones.

La norma *SAP 1009 (Statement of Auditing Practice)* denominada Computer Assisted Audit Techniques (CAATs) o Técnicas de Auditoría Asistidas por Computador, plantea la importancia del uso de CAAT en auditorías en un entorno de sistemas de información por computadora.

SAP 1009 los define como programas de computadora y datos que el auditor usa como parte de los procedimientos de auditoría para procesar datos de significancia en un sistema de información.

SAP 1009 describe los procedimientos de auditoría en que pueden ser usados los CAAT:

1. Pruebas de detalles de transacciones y balances (recálculos de intereses, extracción de ventas por encima de cierto valor, etc.)

2. Procedimientos analíticos, por ejemplo identificación de inconsistencias o fluctuaciones significativas.

3. Pruebas de controles generales, tales como configuraciones en sistemas operativos, procedimientos de acceso al sistema, comparación de códigos y versiones.

4. Programas de muestreo para extraer datos.

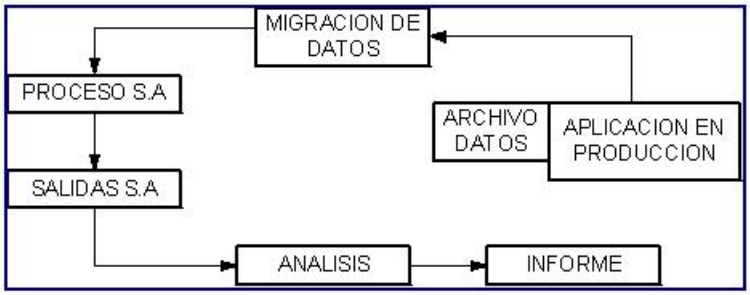
5. Pruebas de control en aplicaciones.

6. Recálculos.

Según SAP1009, en su párrafo 26 y como se muestra en la Figura 3.1, “Flujo de un CAAT”:

El software de auditoría consiste en programas de computadora usados por el auditor, como parte de sus procedimientos de auditoría, para procesar datos de importancia de auditoría del sistema de contabilidad de la entidad. Puede consistir en programas de paquete, programas escritos para un propósito, programas de utilería o programas de administración del sistema. Independientemente de la fuente de los programas, el auditor deberá verificar su validez para fines de auditoría antes de su uso.

Figura 3.1. Flujo de un CAAT



Técnicas para analizar programas

Existen diferentes técnicas para analizar programas la cuales ayudan al auditor en el trabajo de campo y de las cuales las más importantes se mencionan a continuación:

Traceo	Traceo Indica por donde paso el programa cada vez que se ejecuta una instrucción. Imprime o muestra en la pantalla el valor de las variables, en una porción o en todo el programa.
Mapeo	Mapeo Característica del programa tales como tamaño en bytes, localización en memoria, fecha de última modificación, etc.
Comparación de código	Comparación de código Involucra los códigos fuentes y códigos objetos.
Job Accounting Software. Informe de Contabilidad del Sistema	Job Accounting Software. Informe de Contabilidad del Sistema Utilitario del sistema operativo que provee el medio para acumular y registrar la in-

formación necesaria para facturar a los usuarios y evaluar el uso del sistema.

Planificación de CAAT

En este punto se mencionarán cuales son los factores que influyen en la adecuada selección de una herramienta CAAT, así como los pasos que se deben tomar en cuenta para la planificación y selección de la misma.

Cuando se planifica la auditoría, el auditor de sistemas de información debe considerar una combinación apropiada de las técnicas manuales y las técnicas de auditoría asistidas por computadora. Cuando se determina utilizar CAAT los factores a considerar son los siguientes:

- Conocimientos computacionales, pericia y experiencia del auditor de sistemas de información.
- Disponibilidad de los CAAT y de los sistemas de información.
- Eficiencia y efectividad de utilizar los CAAT en lugar de las técnicas manuales
- Restricciones de tiempo

Los pasos más importantes que el auditor de sistemas de información debe considerar cuando prepara la aplicación de los CAAT seleccionados son los siguientes:

- Establecer los objetivos de auditoría de los CAAT: Determinar accesibilidad y disponibilidad de los sistemas de información, los programas/sistemas y datos de la organización.
- Definir los procedimientos a seguir (por ejemplo: una muestra estadística, recálculo, confirmación, etc).
- Definir los requerimientos de output.
- Determinar los requerimientos de recursos.
- Documentar los costos y los beneficios esperados.
- Obtener acceso a las facilidades de los sistemas de información de la organización, sus programas/sistemas y sus datos.
- Documentar los CAAT a utilizar incluyendo los objetivos, flujogramas de alto nivel y las instrucciones a ejecutar.
- Acuerdo con el cliente (auditado): Los archivos de datos, tanto como los archivos de operación detallados (transaccionales, por ejemplo), a menudo son guardados sólo por un período corto, por lo tanto, el auditor de sistemas de información debe arreglar que estos archivos sean guardados por el marco de tiempo de la auditoría.
- Organizar el acceso a los sistemas de información de la organización, programas/sistemas y datos con anticipación para minimizar el efecto en el ambiente productivo de la organización

El auditor de sistemas de información debe evaluar el efecto que los cambios a los programas/sistemas de producción puedan tener en el uso de los CAAT. Cuando el auditor de sistemas de información lo hace, debe considerar el efecto de estos cambios en la integridad y utilidad de los CAAT, tanto como la integridad de los programas/sistemas y los datos utilizados por el auditor de sistemas de información. Probando los CAAT el auditor de sistemas de información debe obtener una garantía razonable de la integridad, confiabilidad, utilidad y seguridad de los CAAT por medio de una planificación, diseño, prueba, procesamiento y revisión adecuados de la documentación. Ésto debe ser hecho antes de depender de los CAAT. La naturaleza, el tiempo y extensión de las pruebas depende de la disponibilidad y la estabilidad de los CAAT.

La seguridad de los datos y de los CAAT pueden ser utilizados para extraer información de programas/sistemas y datos de producción confidenciales. El auditor de sistemas de información debe guardar la información de los programas/sistemas y los datos de producción con un nivel apropiado de confidencialidad y seguridad. Al hacerlo el auditor debe considerar el nivel de confidencialidad y seguridad que exige la organización a la cual pertenecen los datos. El auditor de sistemas de información debe utilizar y documentar los resultados de los procedimientos aplicados para asegurar la integridad, confiabilidad, utilidad y seguridad permanentes de los CAAT. Por ejemplo, debe incluir una revisión del mantenimiento de los programas y controles de los cambios de programa de auditoría para determinar que sólo se hacen los cambios autorizados al CAAT.

Cuando los CAAT están en un ambiente que no está bajo el control del auditor de sistemas de información, un nivel de control apropiado debe ser implementado para identificar los cambios a los CAAT Cuando se hacen cambios a los CAAT el auditor de sistemas de información debe asegurarse de su integridad, confiabilidad, utilidad y seguridad por medio de una planificación, diseño, prueba, procesamiento y revisión apropiados de la documentación, antes de confiar en ellos.

Utilizar CAAT (realización de auditoría)

Cuando se toma la decisión de hacer una auditoría de sistemas con al ayuda de CAAT es importante tomar en cuenta los pasos que a continuación se describen.

El uso de los CAAT debe ser controlado por el auditor de sistemas de información para asegurar razonablemente que se cumple con los objetivos de la auditoría y las especificaciones detalladas de los CAAT. El auditor debe:

- Realizar una conciliación de los totales de control.
- Realizar una revisión independiente de la lógica de los CAAT
- Realizar una revisión de los controles generales de los sistemas de información de la organización que puedan contribuir a la integridad de los CAAT (por ejemplo: controles de los cambios en los programas y el acceso a los archivos de sistema, programa y/o datos).

El software de auditoría generalizado, también conocidos como paquetes de auditoría s on programas de computadora diseñados para desempeñar funciones de procesamiento de datos que incluyen leer archivos de computadora, seleccionar información, realizar cálculos, crear archivos de datos e imprimir informes en un formato especificado por el auditor.

Cuando el auditor de sistemas de información utiliza el software de auditoría generalizado para acceder a los datos de producción, se deben tomar las medidas apropiadas para proteger la integridad de los datos de la organización. Además, el auditor de sistemas de información tendrá que conocer en el diseño del sistema y las técnicas que se utilizaron para el desarrollo y mantenimiento de los programas/sistemas de aplicación de la organización.

El software utilitario es usado para desempeñar funciones comunes de procesamiento de datos, como clasificación, creación e impresión de archivos. Estos programas generalmente no están diseñados para propósitos de auditoría y, por lo tanto, pueden no contener características tales como conteo automático de registros o totales de control.

Cuando el auditor de sistemas de información utiliza el software utilitario debe confirmar que no tuvieron lugar ninguna intervención no planificada durante el procesamiento y que éste software ha sido obtenido desde la biblioteca de sistema apropiado, mediante una revisión del log de la consola del sistema o de la información de contabilidad del sistema. El auditor de sistemas de información también debe tomar las medidas apropiadas para proteger la integridad del sistema y programas de la organización, puesto que estos utilitarios podrían fácilmente dañar el sistema y sus archivos.

Los datos de prueba consisten en tomar una muestra del universo de datos del sistema que se encuentra en producción para analizarlos.

Cuando el auditor de sistemas de información utiliza los datos de prueba debe estar consiente de que pueden existir ciertos puntos potenciales de errores en el procesamiento; dado que esta técnica no evalúa los datos de producción en su ambiente real. El auditor de sistemas de información también debe estar consiente de que el análisis de los datos de prueba pueden resultar muy complejos y extensos, dependiendo de el número de operaciones procesadas, el número de programas sujetos a pruebas y la complejidad de los programas/sistemas.

Cuando el auditor de sistemas de información utiliza el software de aplicación para sus pruebas CAAT, debe confirmar que el programa fuente que está evaluando es lo mismo que se utiliza actualmente en producción. El auditor de sistemas de información debe estar consiente de que el software de aplicación sólo indica el potencial de un proceso erróneo, no evalúa los datos de producción en su ambiente real. Cuando el auditor de sistemas de información utiliza los sistemas de auditoría especializados debe conocer profundamente las operaciones del sistema.

Documentación de CAAT (worksheets)

Una descripción del trabajo realizado, seguimiento y las conclusiones acerca de los resultados de los CAAT deben estar registrados en los papeles de trabajo de la auditoría. Las conclusiones acerca del funcionamiento del sistema de información y de la confiabilidad de los datos también deben estar registrados en los papeles de trabajo de la auditoría. El proceso paso a paso de los CAAT debe estar documentado adecuadamente para permitir que el proceso se mantenga y se repita por otro auditor de sistemas de información. Específicamente los papeles de trabajo deben contener la documentación suficiente para describir la aplicación de los CAAT incluyendo los detalles que se mencionan en los párrafos siguientes:

- Planificación
- Los objetivos de los CAAT
- Los CAAT a utilizar
- Los controles a implementar
- El personal involucrado, el tiempo que tomará y los costos.

La documentación debe incluir:

- Los procedimientos de la preparación y la prueba de los CAAT y los controles relacionados.
- Los detalles de las pruebas realizadas por los CAAT.
- Los detalles de los input (ejemplo: los datos utilizados, esquema de archivos), el procesamiento (ejemplo: los flujogramas de alto nivel de los CAAT, la lógica).
- Evidencia de auditoría: el output producido (ejemplo: archivos log, reportes).
- Resultado de la auditoría.
- Conclusiones de la auditoría.
- Las recomendaciones de la auditoría.

Informe/reporte descripción de los CAAT

La sección del informe donde se tratan los objetivos, la extensión y metodología debe incluir una clara descripción de los CAAT utilizados. Esta descripción no debe ser muy detallada, pero debe proporcionar una buena visión general al lector. La descripción de los CAAT utilizados también debe ser incluida en el informe donde se menciona el hallazgo específico relacionado con el uso de los CAAT. Si se puede aplicar la descripción de los CAAT a varios hallazgos o si es demasiado detallado debe ser

descrito brevemente en la sección del informe donde se tratan los objetivos, extensión y metodología y una referencia anexa para el lector, con una descripción más detallada.

Tipos de herramientas CAAT

A continuación se mencionan y se describe el funcionamiento de las principales herramientas CAAT, cuales son sus beneficios y que es lo que ofrecen.

IDEA[31].

A través de la herramienta IDEA, se puede disminuir costos de análisis, realzar la calidad del trabajo y adquirir nuevos roles. Con esta herramienta se puede leer, visualizar, analizar y manipular datos; llevar a cabo muestreos y extraer archivos de datos desde cualquier origen ordenadores centrales a PC, incluso reportes impresos.

IDEA es reconocido en todo el mundo, como un estándar en comparaciones con otras herramientas de análisis de datos, ofreciendo una combinación única en cuanto a poder de funcionalidad y facilidad de uso.

Áreas de uso de la herramienta

Auditoría externa de estados financieros.

- Precisión: comprobación de cálculos y totales.
- Revisión analítica: comparaciones, perfiles, estadísticas.
- Validez: duplicados, excepciones, muestreos estadísticos.
- Integridad: omisiones y coincidencias.
- Cortes: análisis secuencial de fechas y números.
- Valuación:provisiones de inventario.

Auditoría interna.

- Conformidad de políticas.
- Valor del dinero.
- Pruebas de excepción.
- Análisis.
- Comparaciones y coincidencias.

Detección de fraudes.

- Compras y pagos: validación de proveedores, análisis contables.
- Nómina: coincidencias cruzadas, cálculos.
- Lavado de dinero: valores elevados, cifras redondeadas, movimientos frecuentes.

Informes y análisis de gestión.

- Análisis y cálculos de porcentajes.

[31] www.cynthus.com.mx [http://www.cynthus.com.mx]

- Sumarización y categorías (por ejemplo: por cliente, producto o región).
- Establecimiento de medidas de actuación (por ejemplo: tiempos de respuesta en un proceso de pedidos).
- Perfiles.
- Análisis de Inventario.
- Análisis de flujo de caja.
- Revisiones de Seguridad.
- Registros del sistema.
- Derechos de acceso.
- Registro de teléfonos.
- Firewalls.

Transferencias de archivos.

- Importación de datos desde el sistema central y exportación a un nuevo sistema en un formato más adecuado.

Bancos e instituciones financieras.

- Verificación de cálculos de interés.
- Identificación de cuentas inactivas.
- Análisis de préstamos por índices de riesgo.
- Corroboración de provisiones para pérdidas por préstamos.
- Análisis de reclamos de seguros.

Industrias.

- Verificación de costos de inventarios.
- Análisis de movimientos de inventario.
- Comprobación de diferencias entre el mayor general y las cuentas de inventario.
- Análisis y anticuación del trabajo en curso.

Organizaciones de ventas al por menor.

- Análisis de utilidad bruta.
- Análisis por región, departamento o línea de producto.
- Análisis de precios.

Entes gubernamentales (prestadores de ayudas y beneficios).

- Comprobación de cálculos.
- Análisis y acumulación de estadísticas de pago.
- Búsqueda de duplicados: coincidencias cruzadas de nombres, direcciones e información bancaria.

Funciones

Importación de datos. IDEA permite importar casi todo tipo de archivos desde cualquier tipo de origen, mediante la utilización del Asistente de importación. IDEA ofrece también el editor de Definiciones de Registro (RDE, Record Definition Editor), que lo ayudará en la importación de archivos complejos, registros de longitud variable, y archivos con múltiples tipos de registros. Este producto también puede ser utilizado para modificar definiciones de registros creadas y guardadas por el Asistente de Importación.

Manejo de archivos y clientes. IDEA utiliza un Explotador de Archivos que proporciona un manejo sencillo y estandarizado de los mismos. Esta ventana puede cambiarse de posición en la pantalla y puede modificarse su tamaño. En ella se visualiza, ya sea en forma jerárquica u ordenada, toda la información referente a los archivos de IDEA que pertenecen a la carpeta de trabajo (cliente) activa. IDEA utiliza el concepto de Carpetas de Cliente para facilitar el manejo de los archivos. Tanto el nombre del cliente o proyecto como el período de análisis pueden ser asociados a una Carpeta de Cliente. Esta información aparecerá en todos los informes que se impriman dentro de esta carpeta. La Barra de Herramientas del Explorador de Archivos proporciona un acceso sencillo a las funciones de manejo de archivos incluyendo la posibilidad de marcar un archivo.

Estadísticas de campo. Pueden generarse estadísticas para todos los campos numéricos y de fecha pertenecientes a una base de datos. Se pueden calcular, para cada campo numérico, el valor neto, los valores máximos y mínimos, el valor medio, así como también la cantidad de registros positivos y negativos y la cantidad de registros de valor cero. Para los campos de fecha se proporcionan estadísticas tales como la fecha más temprana y fecha más tardía y el análisis de transacciones diarias y mensuales.

Historial. Dentro de la Ventana de Base de Datos, la pestaña Historial muestra todas y cada una de las operaciones realizadas en la Base de Datos presentadas en una lista que puede expandirse fácilmente. Cada prueba o función realizada genera, en forma automática, un código IDEAScript que puede ser copiado en el Editor de IDEAScript. IDEAScript es un lenguaje de programación compatible con Visual Basic.

Extracciones. La Extracción o prueba de excepción, es la función más comúnmente utilizada en IDEA para identificar elementos que satisfacen una determinada condición como por ejemplo pagos mayores a $10,000 o transacciones efectuadas con anterioridad a una fecha dada. Los criterios de extracción son ingresados utilizando el Editor de Ecuaciones y todos los registros que satisfagan el criterio ingresado son extraídos a una nueva base de datos. Se puede realizar una sola extracción de registros a una base de datos o hasta 50 extracciones diferentes a través de un solo paso por la base de datos.

Extracción indexada. La Extracción Indexada permite limitar el ámbito de los datos a ser buscados por IDEA en la base de datos. Una extracción indexada ahorra tiempo al trabajar con bases de datos extensas.

Extracción por valor clave. La Extracción por Valor Clave brinda la posibilidad de generar una serie de bases de datos secundarias en forma rápida mediante valores comunes encontrados en la base de datos primaria. La extracción por valor clave no requiere de la creación de ecuaciones para ejecutar la extracción. Una clave es un índice creado en una base de datos y un valor clave es uno de los posibles valores que puede tomar esa clave.

@Funciones. Las @Funciones son utilizadas para realizar cálculos complejos y pruebas de excepción. IDEA proporciona más de 80 funciones las cuales pueden utilizarse para llevar a cabo aritmética de fechas, manipulaciones de texto, así como cálculos estadísticos, numéricos, financieros y de conversión. En IDEA las funciones comienzan, ortográficamente, con el símbolo “@”, y son muy similares a las funciones proporcionadas por el programa Microsoft Excel.

Conector Visual. El conector Visual le permite generar una única base de datos a través de otras bases de datos que comparten un campo “clave” en común. Para crear una conexión visual entre diferentes bases de datos, se debe seleccionar una base de datos primaria y luego conectar bases de datos que posean registros coincidentes. La relación creada por el Conector Visual entre las bases de datos es uno a muchos, es decir que la base de datos primaria puede contener diversos registros coincidentes

en las bases de datos conectadas. Todos los registros de las bases de datos conectadas que coincidan con los registros de la base de datos primaria son incluidos en la base de datos resultante.

Uniones. IDEA, a través de la opción Unir Bases de Datos, permite combinar dos campos de bases de datos distintas dentro de una única base de datos, comprobando la existencia o no de datos coincidentes en ambos archivos. Las uniones entre bases de datos pueden realizarse si las mismas contienen un campo en común denominado campo clave.

Agregar. La función Agregar Bases de Datos se utilizar para concatenar dos o más archivos dentro de una única base de datos. Por ejemplo se pueden agregar todos los archivos mensuales de nóminas para obtener una base de datos con todas las nóminas del año. Luego esta base de datos podría ser sumarizada por empleado obteniendo el bruto, el neto anual y las deducciones anuales. Pueden concatenarse hasta 32,768 archivos en una única base de datos.

Comparar. La opción Comparar Bases de Datos identifica las diferencias que existen en un campo numérico dentro de dos archivos para una clave en común. Estos archivos pueden ser comparados en diferentes momentos, por ejemplo, en el caso de la nómina al principio y al final del mes para identificar cambios en los salarios de cada empleado. Se puede comparar también un campo numérico en sistemas distintos, por ejemplo, la cantidad de inventario existente para un ítem tanto en el archivo maestro de inventario como en el archivo inventarios.

Duplicados. IDEA puede identificar elementos duplicados dentro de una base de datos donde existen hasta 8 campos con la misma información. Por ejemplo, números de cuenta duplicados, direcciones, pólizas de seguros, etc.

Omisiones. IDEA le permite buscar omisiones o huecos en secuencias numéricas y de fechas dentro de un archivo, así como también dentro de secuencias alfanuméricas a través de una máscara previamente definida. Para omisiones de fecha, se pueden elegir las opciones fines de semana e ignorar vacaciones. Como ocurre con muchas de las funciones de IDEA, se pueden establecer criterios antes de realizar la búsqueda, tales como importes superiores a $1,000, e incluso se puede modificar el incremento si se desea buscar, por ejemplo, omisiones múltiplos de 10.

Omisiones. La opción Ordenar se utilizar para crear una base de datos físicamente ordenada de acuerdo a un orden previamente especificado. El ordenar bases de datos puede mejorar significativamente el desempeño de determinadas funciones.

Gráficos. La opción Graficar Datos puede utilizarse para graficar archivos de datos o resultados de pruebas realizadas, ya sea en gráficos de barras, barras agrupadas, áreas, líneas o sectores. El Asistente de Gráficos lo guiará paso a paso en la creación del gráfico proporcionándole opciones para incluir títulos, efectos 3D, leyendas, colores, formas y estilos de rejillas. Los gráficos pueden ser impresos, guardados como archivos de mapa de bits o pueden ser copiados en otra aplicación de Windows.

Ley de Benford. Mediante la aplicación del análisis de la ley de Benford podrá identificar posibles errores, fraudes potenciales y otras irregularidades. Esta ley determina que los dígitos y las secuencias de dígitos persiguen un patrón predecible. El análisis cuenta las apariciones de valores en los dígitos en una serie de datos y compara los totales con un resultado predeterminado de acuerdo a la ley de Benford. Los dígitos distintos de cero son contados de izquierda a derecha.

Estratificación. La Estratificación Numérica, la Estratificación de Carácter y la Estratificación de Fecha son una poderosa herramienta para totalizar la cantidad y el valor de los registros dentro bandas específicas. Permiten analizar, por ejemplo, elementos por código postal o por código alfanumérico de producto o activos por fecha de adquisición.

Sumarización. La Sumarización de Campo Rápida se utiliza para totalizar valores de campos numéricos por cada clave única, sumarizando un único campo clave. La Sumarización por Campo Clave se utiliza cuando la clave esta formada por uno o más campos. Los resultados de las sumarizaciones pueden ser graficados y puede accederse en detalle a los registros asociados a cada clave.

Antigüedad. La función antigüedad realiza una anticuación del archivo desde una fecha específica en hasta seis intervalos definidos. Por ejemplo, al final del año pueden anticuarse los créditos a cobrar para determinar si se deben realizar provisiones. La función antigüedad produce un Informe de Antigüedad y dos bases de datos opcionales: la base de datos de antigüedad detallada y la base de datos totalizada por clave.

Tabla pivot. La Tabla Pívot le permite crear análisis variables y multi-dimensionales en archivos de datos extensos. Al momento de diseñar una tabla pívot en IDEA, podrá seleccionar la ubicación de los distintos campos en la tabla para visualizar la información en el modo en que usted desea. La posición de los campos en la tabla definirá como estarán organizados y cómo serán sumarizados los datos.

Agrupador de procesos. Cuando se ejecuta una serie de tareas sobre una base de datos de IDEA, cada tarea requiere de un paso a través de la base de datos. El Agrupador de Procesos analiza las tareas a efectuar y ejecuta las diferentes tareas realizando un solo paso por la base de datos, siempre y cuando esto sea posible. El Agrupador de Procesos ejecuta cada tarea en forma independiente y crea una salida para cada proceso realizando un solo paso por la base de datos.

Muestreo. IDEA proporciona cuatro métodos de muestreo junto con la posibilidad de calcular tamaños de muestras basadas en parámetros ingresados, y evaluar los resultados de las muestras efectuadas. Los métodos de muestreo disponibles son: sistemático (ej. cada 1000 registros); aleatorio (número de elementos elegidos al azar); aleatorio estratificado (un número específico de elementos seleccionados de acuerdo al azar de acuerdo a intervalos); y unidad monetaria (ej. De cada 1,000 dólares u otra unidad monetaria).IDEA proporciona también una opción de Planificación y Evaluación de Atributos, la cual puede ser utilizada para calcular tamaños de muestras, niveles de confianza, límites de errores o desvíos y cantidad de errores de la muestra. Estos cálculos son utilizados para planificar y luego evaluar los resultados de las muestras.

Agregar campos. Los datos importados a IDEA son protegidos y no pueden ser modificados. Sin embargo, pueden agregarse campos adicionales editables ya sea para detallar comentarios, para tildar elementos o para corregir datos. Por otro lado, se pueden agregar campos virtuales (calculados) para probar cálculos en una base de datos, para realizar nuevos cálculos, para obtener porcentajes a través de otros campos de la base de datos, o para convertir datos de un tipo a otro. Los campos editables pueden estar “vacíos” para ingresar comentarios o datos, o pueden basarse en una expresión como ocurre en el caso de los campos virtuales. Los campos booleanos y triestado permiten etiquetar o marcar los campos de acuerdo a 2 o 3 estados respectivamente.

IDEAScript. IDEAScript es un lenguaje de programación orientada a objetos, compatible con Microsot Visual Basic para Aplicaciones TM y LotusScript TM. Los IDEAScripts, también denominados macros, pueden ser creados ya sea grabando una serie de pasos, copiándose desde otros scripts, copiándose desde el Historial, siendo ingresados en la Ventana de Macro o mediante una combinación de cualquiera de todas estas posibilidades. Los Scripts pueden incorporarse al menú Herramientas o a la Barra de Herramientas de Macro, o ejecutarse simplemente desde el menú Herramientas. Los IDEAScript poseen una serie de herramientas complementarias tales como el Editor de Diálogos, el Explorador de Lenguaje y las herramientas de Depuración para asistirlo en la creación de los scripts.

Requerimientos del sistema

- Windows NT4/98/ME/2000/XP
- 128 MB para NT4/2000/XP y 64 MB para Windows 98/ME
- 80 MB de Disco Duro

ACL[32]

ACL es una herramienta CAAT enfocada al acceso de datos, análisis y reportes para auditores y profesionales financieros.

[32] www.acl.com [http://www.acl.com]

Una de las ventajas de esta herramienta es que no es necesario ser un especialista en el uso de CAAT ya que su uso es muy amigable, esta herramienta reduce el riesgo y asegura el retorno de la inversión, también posee una poderosa combinación de accesos a datos, análisis y reportes integrados, ACL lee y compara los datos permitiendo a la fuente de datos permanecer intacta para una completa integridad y calidad de los mismos. ACL permite tener una vista inmediata de la transacción de datos críticos en la organización.

ACL permite:

- Análisis de datos para un completo aseguramiento.
- Localiza errores y fraudes potenciales.
- Identifica errores y los controla.
- Limpia y normaliza los datos para incrementar la consistencia de los resultados.
- Realiza un test analítico automático y manda una notificación vía e-mail con el resultado.

ACL brinda una vista de la información de la organización y habilita directamente el acceso a búsquedas de cualquier transacción, de cualquier fuente a través de cualquier sistema.

Ahorra tiempo y reduce la necesidad de requerimiento de información a departamentos de TI muy ocupados, incrementa el nivel de datos hospedados en múltiples ERP o aplicaciones especializadas. Permite examinar el 100 por ciento de las transacciones de datos, cada campo, cada registro.

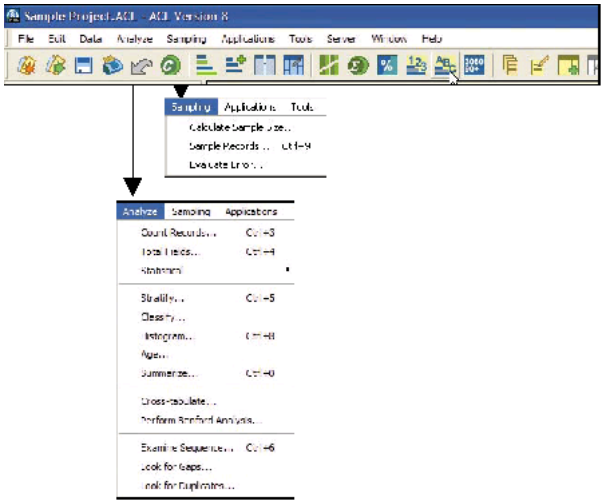
Accesa a diversos tipo de de datos con facilidad incluyendo bases de datos ODBC. Esta herramienta proporciona una completa integridad de datos, ACL solo tiene acceso de lectura a los datos de los sistemas que se están monitoreando, esto significa que la fuente de datos nunca será cambiando, alterada o borrada.

Una de las ventajas de esta herramienta es que tiene un tamaño ilimitado en el monitoreo de datos y puede procesar rápidamente millones de transacciones de datos ya que permite leer mas de 10,000 y hasta 100,000 registros por segundo

ACL destaca por ser de fácil uso: selecciona, identifica y da formato a los datos fácilmente gracias al Data Definition Wizard con esta librería permite importar y exportar datos directamente a Excel, Access y XML, otra mas de las ventajas es que no es necesario tener conocimientos de programación para el uso de ACL.

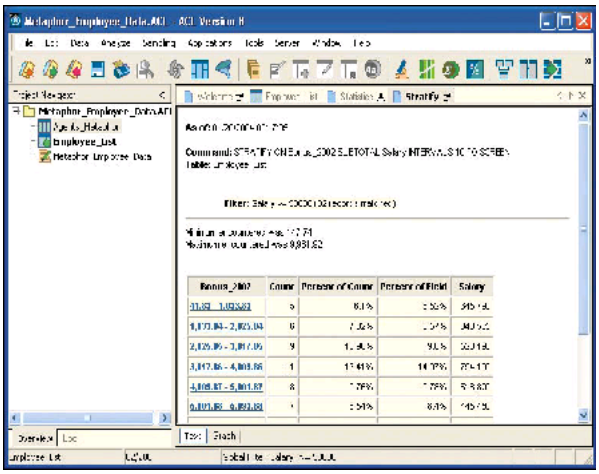
La herramienta tiene comandos pre-programados para análisis de datos, pero también puede analizar datos adaptándose a una metodología y excepciones de investigación en cualquier momento, se pueden implementar continuos monitoreos haciendo análisis automáticos a través de scripts y habilitando la notificación en tiempo real. Explora los datos rápida y completamente, como se muestra en Figura 3.2, “Comandos pre-cargados”

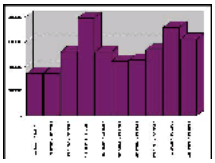
Figura 3.2. Comandos pre-cargados



Otra ventaja es los resultados se pueden ver fácilmente y entenderlos en formatos tabulares, posee graficas precargadas, también posee un log de actividad de los registros ésto permite analizar y comprar registros pasados con los nuevos, posee vistas de reportes precargadas de Crystal Reports, como se muestra en Figura 3.3, “Visor de Cristal Reports”

Figura 3.3. Visor de Cristal Reports





Especificaciones técnicas:

- PC con procesador Pentium o superior.
- Windows 98/ME o Windows NT (SP6), 2000 (SP2), XP.
- 32MB de RAM (Mínimo).
- 26MB de espacio en disco duro para ACL (Mínimo) y 44 MD extras si se desea instalar la librería de Crystal Reports.

Otros componentes requeridos:

- Internet Explorer 5.5 o mayor.
- Windows Installer
- MDAC 2.6
- MsJet 4.0 SP3 o mayor.
- MSXML 4.0 o mayor.

Auto Audit

Auto Audit es un sistema completo para la automatización de la función de Auditoría, soportando todo el proceso y flujo de trabajo, desde la fase de planificación, pasando por el trabajo de campo, hasta la preparación del informe final.

Además del manejo de documentos y papeles de trabajo en forma electrónica, Auto Audit permite seguir la metodología de evaluación de riesgos a nivel de entidad o de proceso, la planificación de auditorías y recursos, seguimiento de hallazgos, reportes de gastos y de tiempo, control de calidad, y cuenta con la flexibilidad de un módulo de reportes “ad hoc”. Todos estos módulos están completamente integrados y los datos fluyen de uno a otro automáticamente. Su pantalla principal se muestra en la Figura 3.4, “Ventana principal”.

Figura 3.4. Ventana principal

Beneficios

Eficiencia en el trabajo	Eficiencia en el trabajo Aumenta la eficiencia en la conducción de la evaluación de riesgos y planificación anual. El incremento está entre 20% y 45%.
Base de conocimiento	Base de conocimiento Acceso inmediato a toda la documentación de auditorías pasadas, en ejecución o planeadas.
Flexibilidad	Flexibilidad Permite que los auditores puedan trabajar en lugares distantes con sus réplicas locales de la auditoría en curso y su posterior sincronización a la base de datos centralizada.
Estandarización y control	Estandarización y control Garantiza el seguimiento de metodologías de trabajo de acuerdo a las mejores prácti-

	cas de la organización con el uso de una biblioteca de documentos estándares (memoranda, programas, papeles de trabajo, cuestionarios, evaluaciones, informe final y otros).
Adaptabilidad	Adaptabilidad Provee una herramienta de reportes “ad hoc” para la generación de informes, tablas y gráficos con los formatos requeridos para el Comité de Auditoría o Auditor General.
Comunicación	Comunicación Mejora la comunicación con los auditados en el seguimiento de los hallazgos y planes de acción.
Reducción de costos y aprovechamiento del recurso más valioso (el auditor):	Reducción de costos y aprovechamiento del recurso más valioso (el auditor): Se reducen los costos y el tiempo de documentación y revisión de papeles, logrando invertir más tiempo en la auditoría, añadiendo así valor a la labor de auditoría.
Seguridad y confidencialidad	Seguridad y confidencialidad Permite la creación de usuarios definiendo perfiles según su rol dentro de la auditoría para controlar el acceso de documentos e integridad de la información. Con sus algoritmos de cifrado (encriptación) Auto Audit garantiza la confidencialidad de información.
Facilidad de uso	Facilidad de uso Auto Audit se aprende e implementa en menos de una semana.
Integración con ACL	Integración con ACL Es posible integrar los procesos de análisis de datos que se efectúan con ACL en los papeles de trabajo de Auto Audit.

Funcionalidad de Auto Audit for Windows

- Planificación de Auditorías en función de la Evaluación de Riesgos, siguiendo la metodología de evaluación vertical y/o por proceso.
- Programación de auditorías y asignación de auditores para el trabajo de campo.
- Flexibilidad máxima para la numeración e índice de los programas y papeles de trabajo, enlaces y referencias cruzadas de documentos.
- Mantenimiento de una Biblioteca de Estándares de programas de auditoría, papeles de trabajo, memos, listas de chequeo, hallazgos, informes y otros.
- Establecimiento de usuarios con perfiles definidos para crear, modificar, eliminar, revisar o aprobar documentos específicos, de acuerdo a su rol dentro del flujo de trabajo en el proceso de auditoría (Gerente, Encargado, Staff).

- Creación automática del Informe Final de Auditoría extrayendo información clave de los hallazgos registrados durante el trabajo de campo.
- Monitoreo de hallazgos para todas las auditorías visualizado por status, fecha de seguimiento, auditoría, nivel de riesgo y otros.
- Registro de tiempos y gastos para la generación de reportes.
- Elaboración de encuestas post-auditoría así como también evaluaciones de los auditores.
- Disponibilidad de reportes estándares ya listos para su uso y posibilidad de crear reportes “ad hoc” según las necesidades.
- Mantiene un registro histórico de todas las actualizaciones, revisiones y aprobaciones de documentos.
- Permite personalizar áreas de la aplicación para reflejar el ambiente de trabajo único de cada organización tales como: áreas de negocio, factores de riesgo, calificaciones de hallazgos, entre otros y se adapta a cualquier estructura de auditoría (COSO, COCO, CSA).
- Tiene un algoritmo propio que encripta los datos asegurando la confidencialidad de la información y su acceso únicamente a través de la aplicación.

Audicontrol APL (AUDISIS)[33]

La metodología *Audicontrol APL versión 2005* y el software en el que ésta se apoya, proveen ayudas para asistir a los diseñadores de controles, analistas de seguridad y analistas de riesgos, en el desarrollo de todas las etapas de proyectos de Gestión de Riesgos y Diseño de Controles Internos o de Rediseño, Reingeniería del Sistema de Control Interno existente para procesos de negocio, sistemas de información (Aplicaciones de Computador) y la Infraestructura de Tecnología de Información de la organización.

Audicontrol APL es una herramienta para asistir en la construcción de sistemas de gestión de riesgos y controles internos en los procesos de la cadena de valor y los sistemas de información de las empresas. Para este fin, utiliza la técnica de *Autoevaluación del Control (CSA: Control Self Assessment)*, también conocida con el nombre de *Autoaseguramiento del Control (CSA: Control Self Assurance)*. Esta es una extensión de los mecanismos de control interno que tiene por objeto el asegurar a los clientes, accionistas y organismos gubernamentales de control y vigilancia, que los controles necesarios están establecidos y son efectivos para mitigar los riesgos importantes.

Desde la perspectiva administrativa, CSA asiste en la determinación de si la organización está satisfaciendo sus objetivos. Las ventajas claves de implementar un CSA incluyen la detección temprana de riesgos y el desarrollo de planes de acción concretos que salvaguarden los programas organizacionales contra riesgos del negocio significativos. Los objetivos del CSA son:

- Reducir o eliminar los controles costosos e inefectivos.
- Define con precisión las áreas de riesgo, mientras se desarrollan adecuadas medidas de control.
- Evalúa los estándares de control utilizados.
- Enfatiza las responsabilidades de la administración por el desarrollo y monitoreo efectivo de los sistemas de control interno.
- Comunicar los resultados a otros.

CSA es una técnica que implica la conducción de talleres (workshops) con todos los miembros del staff que intervienen en un proceso o sistema de información, en el cual se discuten los riesgos y problemas de control y se aconsejan planes de acción para solucionar esos problemas. Este proceso ofrece

[33] http://www.audisis.com

un medio de identificar los problemas de control y las recomendaciones de mejoramiento. Los facilitadores ayudan al grupo a ponerse de acuerdo.

Audicontrol-APL automatiza las metodologías de diseño y documentación de controles en operaciones de negocios y procesos de TI, utilizando tres alternativas de escenarios de riesgo:

- Subprocesos o componentes de los procesos de la Cadena de Valor de las Empresas (misionales o de apoyo administrativo), definidos de acuerdo con las condiciones de funcionamiento reales de cada Organización.
- Diez escenarios de riesgos claves para la Infraestructura de TI. La metodología es aplicable para desarrollar el enfoque de diseño de gestión de riesgos para procesos de los cuatro dominios del Modelo COBIT (Control Objectives for Information and Related Technology, tercera edición en el año 2000).
- Quince escenarios de Riesgo agrupados de manera natural, que representan el ciclo de vida del control de los datos en las aplicaciones de computador.

Audicontrol-APL provee una herramienta de software orientada al usuario final, para apoyar el desarrollo de todas las fases y etapas de la metodología de Diseño de Controles y Gestión de Riesgos Operacionales. Las 2 fases y 10 etapas de la metodología son las siguientes:

Fase I: fase estática o estructural del control interno.

1. Identificar la Seguridad Requerida.
2. Evaluar Riesgos Potenciales e identificar Riesgos Críticos.
3. Elaborar Mapa de Riesgos.
4. Seleccionar Controles Necesarios y evaluar la protección que ofrecen.
5. Definir Especificaciones para Implantar los Controles (Documentar los Controles).

Fase II: dinámica u operativa del control interno.

1. Sensibilizar y Concientizar a los propietarios del proceso para el mejorar cultura de Control de la Organización.
2. Elaborar e Implantar Guías de Autocontrol.
3. Elaborar e Implantar de Guías de Monitoreo de la Protección Existente y del Riesgo Residual.
4. Generar el Manual de Controles y Administración de Riesgos Operacionales.
5. Mantenimiento y Actualización del Manual de Controles.

Audicontrol-APL es un software para Windows, que opera en ambientes monousuario o en Red local.

La metodología AUDICONTROL APL fue creada para apoyar el trabajo de:

- Analistas y Desarrolladores de Sistemas.
- Departamentos de Organización y Métodos.
- Auditores de Sistemas.
- Departamentos de Control Interno.
- Administradores de Seguridad en Procesamiento electrónico de datos.
- Administradores de Riesgos.

Funciones.

- Para cada proceso o sistema objeto de estudio, Audicontrol-APL ayuda a personalizar las bases de datos de conocimientos de las organizaciones, con conceptos y elementos modernos de control aportados por los modelos COBIT (Control Objectives for Information and Related Technology ISACA, 2000) y COSO y las normas ISO 9000, ISO 9126, ISO 12207, ISO 14000, ISO 18000 e ISO 17799.

- En las actividades de diseño, rediseño, documentación e implantación de los controles, Audicontrol-APL apoya a los diseñadores con guías, cuestionarios estándar y bases de conocimientos sobre procesos de tecnología de información, riesgos, causas del riesgo, controles y objetivos de control.

- Identificar y categorizar los riesgos inherentes a los negocios o servicios de las empresas, como lo recomienda el modelo COSO.

- Ayuda a elaborar el Mapa de Riesgos con la ubicación física, lógica y funcional de los riesgos en las dependencias y procesos que intervienen en los negocios o servicios de las empresas.

- Seleccionar los controles necesarios para mitigar el impacto o reducir la probabilidad de ocurrencia de las amenazas que podrían originar cada uno de los riesgos potenciales críticos.

- Mide (califica) el grado de protección que aportan los controles seleccionados, por cada amenaza (causa del riesgo), punto de control, dependencia y objetivo de control de cada proceso de negocio y servicio soportado en tecnología de información.

- Elaborar Guías de Autocontrol que asignan responsabilidades por la ejecución y/o supervisión de cada control clave en las dependencias que intervienen en los procesos de negocios automatizados.

- Elaborar Guías de Autoevaluación del Control o Autoaseguramiento del Control, para medir (determinar) periódicamente los niveles del riesgo residual en las dependencias de la empresa.

- Diseñar e implantar el Plan de Mitigación de Riesgos no protegidos apropiadamente por los controles establecidos en la organización.

- Elaborar los Manuales de Control Interno y Gestión de Riesgos para los procesos, las aplicaciones y la infraestructura de TI y permite su actualización permanente.

- Para los procesos y sistemas en proceso de desarrollo, Audicontrol-APL ayuda a diseñar e implantar la estructura de control requerida, desde su inicio hasta su implantación definitiva.

- Ofrece la posibilidad de personalizar y reutilizar las bases de datos generadas con circunstancias propias de la empresa, como base para el diseño de controles en otras áreas o procesos automatizados.

- Provee ayudas y herramientas para valorar y medir el riesgo potencial (RP), la protección ofrecida (PO) por los controles establecidos y el riesgo residual (RR) que están asumiendo las organizaciones en cada proceso o sistema de información.

- Audicontrol-APL cuenta con el soporte y asesoría permanente de AUDISIS, que es una firma de Consultores Gerenciales especializados en control y auditoría de sistemas, estable y de reconocido prestigio profesional en Colombia y el exterior.

En síntesis, Audicontrol-APL p roporciona un esquema de trabajo seguro y eficiente para:

- Identificar y evaluar los riesgos potenciales y residuales asociados con las operaciones de negocio y de soporte administrativo de las empresas.

- Definir e implantar controles manuales y automatizados que sean efectivos para reducir a niveles aceptables la exposición al riesgo en los sistemas automatizados de las empresas, con su respectiva documentación.

- Facilitar la implantación de un Sistema de Gestión de Riesgos Operacionales.
- Implantar técnicas y procedimientos de Autocontrol y de Prevención del Riesgo en las empresas.

AuditMaster[34]

AuditMaster de Pervasive, es una solución de supervisión de transacciones a nivel de base de datos. Este sistema controla e informa de toda la actividad que tiene lugar en una base de datos Pervasive.SQL.

La tecnología de AuditMaster consiste en capturar las operaciones que se realizan en la base de datos y escribirlas en un archivo de registro. AuditMaster se divide en tres componentes:

Gestor de eventos (Log event handler)	Gestor de eventos (Log event handler) Es un plugin que se instala fácilmente en la base de datos. Actúa como una especie de “caja negra” que captura y escribe en un registro de seguimiento todas las actividades que se llevan a cabo en la base de datos. Se instala en el nivel de la base de datos, de forma que siempre que ésta funciona, también lo hace el gestor de eventos, manteniendo al día el registro de seguimiento. El gestor de eventos se instala en el sistema con el motor para servidores Pervasive.SQL.
Base de datos de registro (Log database)	Base de datos de registro (Log database) Es un conjunto de archivos de Pervasive.SQL residente en el directorio de datos de AuditMaster. El archivo principal de registro contiene toda la información de seguimiento, por ejemplo, la identificación de usuario, la identificación de la estación de red, el tiempo y la fecha de la operación, el nombre de aplicación, el nombre de la tabla de la base de datos y el tipo de operación. Además, el archivo crea imágenes, antes y después de la transacción, a efectos de actualización de los registros. Cada vez que un usuario modifica algún dato, AuditMaster escribe en el registro tanto el valor antiguo como el nuevo.
Visor de registros (Log viewer)	Visor de registros (Log viewer) Permite hacer consultas a la base de datos de registro, lo que permite que un administrador de seguridad compruebe las actividades realizadas y analice patrones y tendencias. Las consultas se realizan con rapidez gracias a una sencilla interfaz gráfica. Los informes de AuditMaster también pueden evidenciar si se utilizan las prácticas requeridas o buenas prácticas generales. Asimismo, el visor de registros también se emplea para mantener y configurar el sistema AuditMaster, lo que incluye la

[34] http://www.pervasive.com

creación de alertas que ejercen una vigilancia dinámica de las actividades realizadas con datos futuros. Una vez definidas las alertas en AuditMaster, esperan a que se lleve a cabo alguna operación de interés perteneciente al espectro de acciones de los usuarios, tales como la creación, la actualización, la eliminación o simplemente la lectura de datos. Cuando se produce algún evento de interés, el gestor de eventos activa inmediatamente una alerta, bien a través de un correo electrónico enviado a uno o más destinatarios, bien a través de una llamada a otra aplicación o mediante el inicio de una nueva aplicación. El visor de registros puede instalarse en cualquier máquina con acceso al servidor Pervasive.SQL y a los archivos de la base de datos de registro.

Ventajas

AuditMaster no exige modificar el código de la aplicación actual o de la base de datos Pervasive.SQL, ya que es independiente de la aplicación y se instala en la propia base de datos, muy por debajo del nivel de las aplicaciones clientes. AuditMaster puede supervisar varias aplicaciones e incluso identificar la fuente original de cada evento en el registro de seguimiento, permitiendo de esta manera llevar a cabo un análisis interno del sistema y un control detallado de la aplicación.

Además de presentar informes y activar alertas, el registro de seguimiento detallado ofrece otras ventajas. Al almacenar imágenes de todos los cambios antes y después de la transacción, es posible recuperar registros individuales de la base de datos deshaciendo los cambios capturados en el registro de seguimiento. Además, como el registro está almacenado en tablas de Pervasive.SQL, las aplicaciones pueden acceder directamente a los datos de registro, lo que permite integrar AuditMaster en otras aplicaciones.

Trabaja con todos los datos de Pervasive.SQL, tanto transaccionales como relacionales, también puede mantener automáticamente en los registros de datos múltiples archivos de metadatos que faciliten actualizaciones a nuevas versiones de la aplicación cliente, incluso aunque cambien los archivos de definición de datos (DDF). Los metadatos de AuditMaster pueden ser auditados aunque falten los archivos DDF o estén incompletos. Además, si el sistema utiliza registros variantes, AuditMaster sigue realizando las mismas funciones de captura, informe y alerta.

Especificaciones.

Plataformas soportadas.

- Windows NT 4.0 (SP3 o superior)
- Windows 2000
- Windows 2003
- Windows XP

Bases de datos soportadas.

- Pervasive.SQL V8
- Pervasive.SQL V8 SP1

- Pervasive.SQL V8.5
- Pervasive.SQL V9

Delos [35]

Delos es un sistema experto que posee conocimientos específicos en materia de auditoría, seguridad y control en tecnología de información.

Este conocimiento se encuentra estructurado y almacenado en una base de conocimiento y puede ser incrementado y/o personalizado de acuerdo con las características de cualquier organización y ser utilizado como una guía automatizada para el desarrollo de actividades específicas.

Para la utilización del sistema hemos identificado cuatro roles o que tienen relación con el control en una organización:

- El responsable de diseñar e implementar el control en la organización, quien puede ser un analista de sistemas, un oficial de seguridad, un diseñador de procesos de trabajo o alguien quien realice trabajos de reingeniería.
- El responsable de evaluar el correcto funcionamiento del control de la organización, quien normalmente es un auditor, un representante de aseguramiento de calidad o cualquier persona que se le asigne en forma temporal o definitiva la función de evaluación
- El usuario del control, quien realiza sus actividades cotidianas con la seguridad de que cuenta con los elementos suficientes para desarrollar sus funciones de forma eficiente, efectiva, segura y consistente y
- Los beneficiarios del control, quienes reciben los beneficios de que una organización opere con adecuados procedimientos de control. Los beneficiarios pueden ser tanto internos como externos a la organización, los primeros representados por la administración y los accionistas y los segundos representados normalmente por clientes, proveedores, gobierno, inversionistas, etc.

Delos es una herramienta que fue diseñada pensando en empresas, organizaciones y profesionistas que deseen incrementar los beneficios derivados de la tecnología de información a través de actividades relacionadas con auditoría, seguridad y control en TI.

Ventajas

Delos presenta una serie de características que lo distinguen de otras herramientas.

Orientación al negocio. A diferencia de otros productos de auditoría de software, Delos tiene una orientación al negocio, es decir, parte de un marco de referencia estratégico formado por los objetivos de negocio y factores críticos de éxito de la empresa y lo relaciona con elementos de control interno en tecnología de información. Consecuentemente, su empleo promueve el cumplimiento de los objetivos institucionales de la empresa, permitiendo alinear sus elementos de tecnología de información con la estrategia de negocio. De manera indirecta, Delos ayuda a estructurar los objetivos, metas y factores críticos de éxito de la empresa, así como los indicadores que permiten su medición.

Base de conocimientos. Delos cuenta con una extensa base de conocimientos que contiene tanto elementos de negocio (objetivos, metas y factores críticos de éxito) como elementos de control, seguridad y auditoría en TI, utilizando relaciones puntuales entre dichos elementos para ofrecer un nivel de “inteligencia”. Esta base de conocimientos, no solo permite establecer un marco de referencia para las funciones de auditoría, sino que ofrece la posibilidad de ampliar su alcance y sus beneficios a otras áreas de la empresa que tienen relación con el concepto de control, tales como el área de tecnología de información y, en caso de que exista, el área de contraloría (responsable del control en la empresa).

[35] http://www.cynthus.com.mx

Fundamento metodológico. El funcionamiento de Delos se basa en una metodología estructurada que ofrece al usuario una orientación detallada sobre las actividades y la secuencia necesaria para desarrollar auditorías o evaluaciones en ambientes de TI. Esta característica diferencia y posiciona favorablemente a Delos con respecto a otros productos, los cuales primordialmente ofrecen un conjunto de "diagramadores," técnicas y/o "reporteadores" cuya utilización queda supeditada a la experiencia individual de cada usuario o al empleo de una metodología adicional que no necesariamente corresponde a las características del software.

Personalizable a las características y requerimientos de cada empresa. Adicionalmente a contar con una robusta base de conocimientos, Delos permite incorporar nuevos elementos, modificar los existentes y definir nuevas relaciones entre los objetos que integran dicha base. Esto permite complementar el cuerpo de conocimientos y adecuarlo a los requerimientos específicos de cada empresa.

Multicompañía y multiproyecto. La estructura de Delos permite crear modelos de diversas compañías definiendo proyectos con diferentes enfoques, objetivos y alcances. Esta capacidad proporciona gran flexibilidad para la realización de auditorías en empresas o instituciones con requerimientos plurales, como pueden ser: corporativos, entidades de supervisión y vigilancia, organismos gubernamentales o firmas de auditoría externas.

Incluye COBIT. Delos utiliza la estructura y los objetivos de control definidos por COBIT para diseñar programas de auditoría basados en dicha estructura y/o interpretar los resultados de evaluaciones realizadas con el propio enfoque de Delos, con base en el estándar internacional sobre control en tecnología de información emitido por la ISACA (Information Systems Audit and Control Association).

Beneficios

En forma concreta podemos decir que Delos genera los siguientes beneficios:

- Ayuda al logro de objetivos de negocio al apoyar el alineamiento de los recursos de TI con la estrategia de la entidad y al incrementar el retorno sobre la inversión en tecnología.
- Apoya la planeación estratégica de TI, al identificar elementos indispensables para desarrollar la estrategia tecnológica y alinearla a los intereses institucionales.
- Promueve la eficiencia y efectividad de la auditoría al hacer uso de medios automatizados para procesar información e incorporar a los programas de trabajo sólo las actividades que cada auditoría requiere en forma específica.
- Capitaliza el conocimiento de la organización y lo materializa en un patrimonio institucional, al conservar el conocimiento en un repositorio de software, minimizando en gran medida los efectos de rotación de personal.
- Permite capacitar a personal de nuevo ingreso, tanto de la compañía en general como de las funciones relacionadas con auditoría y control en TI.
- Estandariza el trabajo de auditoría al utilizar una metodología automatizada incorporada al sistema de software.

Características.

Además de la descripción antes mencionada Delos se divide en 5 módulos mas, los cuales se describen a continuación:

- DelosCognos: es el módulo responsable de la administración del conocimiento de Gobierno de Tecnología de Información. Este conocimiento se almacena en una completa base de conocimientos. Este módulo permite personalizar, consultar y mantener actualizada la base de conocimientos del sistema y se integra tanto por elementos de negocio como: estrategias, fortalezas, stakeholders, objetivos, metas y factores críticos de éxito, como por elementos de tecnología de información, tales cómo: Aplicaciones, procesos, recursos, colaboradores y elementos de auditoría /aseguramiento, como: Objetivos de control, procedimientos de control y procedimientos de auditoría entre otros.

En esta base de conocimientos también se encuentran los elementos de COBIT. Estos elementos se encuentran interrelacionados, lo cual permite establecer los sistemas de control requeridos por la organización y su relación con elementos de la estrategia institucional.

- Delos Mentor: es el módulo encargado de guiar las actividades de auditoría, es decir, funge como consejero o guía virtual que proporciona apoyo para la realización de tareas específicas de auditoría con base en una metodología de trabajo estructurada. Delos Mentor permite elaborar programas de revisión personalizados de acuerdo con las características de la organización y al alcance y objetivos específicos de cada auditoría.

- Delos Tutor: Este módulo tiene el propósito de ofrecer capacitación a sus usuarios, emulando, como su nombre lo indica, la labor de un tutor, que es proporcionar educación y orientación a sus alumnos en alguna materia en particular. Delos Tutor tiene incorporados los conceptos teóricos de auditoría en TI, lo cual es utilizado para proporcionar instrucción autodidacta a sus usuarios.

- Delos Control: Este módulo esta enfocado a la otra perspectiva del control, es decir, no a la de quien debe evaluar el control, sino del que es responsable de diseñar e implantar controles en una empresa u organización. La misma base de conocimientos de control de Delos es utilizada para identificar los procedimientos que una organización debería tener establecidos en un ambiente de tecnología de información, ya sea en sus procesos de trabajo relacionados con el desarrollo de soluciones informáticas (como desarrollo de sistemas, implantación de paquetes de software, planeación estratégica de sistemas, adquisición de tecnología, etc), como en los procesos de administración de recursos informáticos.

- DelosCentinel: Este módulo permite administrar la seguridad de acceso a Delos. Esto incluye tanto la administración de usuarios del sistema, como la asignación de distintos niveles de seguridad para acceder a cada una de las organizaciones dadas de alta en Delos. Los niveles de seguridad permiten otorgar privilegios de acceso de manera específica, inclusive para restringir los tipos de acciones que cada usuario puede ejercer sobre cada uno de los tipos de objetos en la base de conocimientos de la organización.

Requerimientos.

- Windows 95, 98, 2000, NT y XP.

- 150 MB en disco duro.

- 32 MB en memoria RAM

- Procesador pentium a 100 megahertz.

Capítulo 4. Análisis de información

En el presente capitulo, se realiza el análisis de la información que se presentó en los capítulos anteriores, comenzando por el análisis de consecuencias y riesgos en cuanto a la implantación del área de auditoría en informática dentro de la H. Cámara de Diputados. En seguida, se habla de las mejores prácticas y por último del análisis de las CAAT que más se adaptan a las necesidades específicas del área, ya que la implantación de una mejor práctica y la adquisición de una herramienta de auditoría asistida por computadora, se consideran herramientas básicas para el desarrollo erices del área de auditoría en informática, mismas que deben cubrir las necesidades de del personal.

Análisis de consecuencias y riesgos

(implantación del área de auditoría informática)

Al crear un área nueva dentro de una organización trae consigo cambios importante, que pueden resultar riesgosos si no se realiza aplicando la metodología adecuad y se hace un buen análisis, para el caso específico de implantar un área de auditoría en informática dentro de la Subcontraloría de Auditoría los riesgos se componen de los siguientes:

Riesgos de Implantación del área	**Consecuencias**
Poca aceptación por las áreas de Tecnologías de Información ya que se les establecerán controles los cuales no son aceptados de una buena manera por el personal involucrado.	No podrá trabajar en conjunto con el área de Tecnologías de la información que es hacia donde está enfocada el área de auditoría.
Falta de capacitación del personal de la Subcontraloría de Auditoría	Mal uso de las herramientas y los procedimientos.
Falta de una mejor cultura informática en el personal de la Subcontraloría de Auditoría	Uso inadecuado de los equipos, herramientas, procedimientos e ignorar normas y controles.
Falta de una visión general por parte de las áreas de TI como una problemática la falta de un área de auditoría informática	Ver al área de auditoría como un área que produce y que no sirve así como no poder trabajar en conjunto.
Resistencia al cambio.	Inadaptabilidad a la implantación de las técnicas y herramientas propustas.

Al no implantar el área de auditoría informática también se corren riesgos potenciales, ya que el atraso que generaría eventualmente aumentará los rezagos en los trabajos de auditoría y la ineficiencia del personal, a continuación describimos los que detectamos de acuerdo a las visitas realizadas al área de la Subcontraloría de Auditoría y en base a los cuestionarios aplicados, se determina lo siguiente:

Riesgos de no Implantación del área	Consecuencias
Pérdida de información.	Aumento de costos para la organización, indisponibilidad de la información.
Recomendaciones inadecuadas.	Ineficacia en los procesos de auditoría.
Fuga de información.	Mal manejo de la información por personal interno del área.
Inadecuado desarrollo del área de sistemas.	El área de TI seguirá siendo vista como un área que no ofrece servicios y un desarrollo y crecimiento lento.
Robo	Perdida de información por la falta de controles y procedimientos que regulen su uso y redunde su mal uso malintencionado de externos.
Falta de preparación del personal.	Incapacidad de afrontar contingencias graves.

Selección de mejores prácticas

Se ha comentado en el capítulo anterior la importancia del uso de las mejores prácticas dentro de las organizaciones, por ello se determina que es indispensable el manejo de las mismas para que el área de auditoría informática que se implante pueda realizar sus funciones de forma óptima, mismas que se definen específicamente en el siguiente capítulo.

Se propone el uso de COBIT como mejor práctica de la auditoría, debido a que ésta herramienta como tal, permite evaluar los procesos de la organización que a su vez se relacionan con las tecnologías de información.

El uso de COBIT con sus cuatro dominios principales permitirá a la nueva área de auditoría en informática establecer diagnósticos a todos los niveles, tanto administrativa y operacionalmente ya que proporciona las bases para el establecimiento de controles para la planificación, porcesos y la información utilizada.

Es importante recordar que DELOS by Cynthus como propuesta de herramienta CAAT para la automatización de los procesos de auditoría, está basada en el estándar de COBIRT, por lo que se puede decir que son complementarias.

Análisis de la aplicación de CAAT

En esta parte del capitulo se habla específicamente de las CAAT que serían más útiles dentro de la Subcontraloría de Auditoría para el desarrollo de sus actividades, para lo cual se compararán las siguientes herramientas: Auto Audit (Grupo XopanTech), Working Papers (Grupo Cynthus) y Delos (Grupo Cynthus).

A continuación se hace un análisis de los beneficios de cada una de ellas, así como de sus costos, necesidades de capacitación de personal y equipo de software requerido adicional al ya existente, el criterio de selección obedece a la posible utilización del peronal y hardware ya existente.

Para este efecto, se organizaron presentaciones de demos de estas tres herramientas al personal de la Subcontraloría de Auditoría, de estos tres proveedores obtuvimos también la cotización de implantación de éstas y las necesidades de software y hardware (Apéndice A, *Cotización de proveedores*). Con esta información a continuación se presenta el estudio comparativo de costo beneficio de estas tres herramientas.

En base a la experiencia en la implantación de herramientas (software y hardware) que ayuden a la automatización de procesos y/o información se determina que pueden existir algunos riesgos y más si la herramienta es implementada en un área nueva como es el caso de la H. Cámara de Diputados, en la implementación de un área de auditoría informática, a continuación se mencionan los riesgos que pueden existir en la implementación de una herramienta que ayude a la automatización de las tareas de el área de auditoría informática.

Riesgos de implantación de la herramienta	Consecuencias
Mal análisis para la implantación de la herramienta.	Mal funcionamiento de la herramienta
Costo muy elevado.	Implantar una herramienta más barata que no cumpla con los requisitos necesarios para ayudar a automatizar los procesos del área de auditoría informática.
Mala selección de la herramienta.	Implantar una herramienta que no ayude a automatizar los procesos del área de auditoría Informática.
Mala capacitación en el uso de la herramienta.	Mala explotación de la herramienta.

Los procesos y el flujo de trabajo no están bien definidos.	Mala implantación de la herramienta, así como un mal funcionamiento de la misma.
Arquitectura tecnológica no soportada por la herramienta.	Mal funcionamiento de la herramienta, caídas de sistema, perdido de información, poca disponibilidad de la herramienta.
Sobreautomatización de los procesos.	Que no se conozca como realizar los procesos en caso de que falle el sistema, detección retardada de fallas.

Estudio de costo-beneficio

El Costo-Beneficio, tiene como objetivo fundamental proporcionar una medida de los costos en que se incurren en la realización de la propuesta de implementación de un área de Auditoría en Informática en el Órgano Legislativo, a su vez comparar dichos costos previstos con los beneficios esperados de la realización del proyecto, definiendo la factibilidad de las alternativas a seguir para llevar a cabo la propuesta.

Una función muy importante de los costos es servir de guía para determinar cuál puede ser la combinación de productos más rentable y los gastos en que se puede incurrir sin afectar los beneficios.[1]

Es importante detallar los costos, ya que se considera que entre mayor sea el costo de la técnica de auditoría asistida por computadora que se seleccione, mayores deberán ser los beneficios que conlleve; esto es que la expectativa crece.

A continuación se detallan los costos que se relacionan con la evaluación a las necesidades de la propuesta de implementación.

Costos indirectos

De acuerdo a las características de cada herramienta y en entrevista con el personal de la Subcontraloría de Auditoría se determinó que del software de Auto Audit sería necesario adquirir 20 licencias, para Working Papers 5 y para Delos entre 3 y 5, con estos datos proporcionados por el proveedor, proseguimos nuestro análisis, como sigue:

Tabla 4.1. Costos de adquisición

	Auto Audit	Working Papers	Delos [a]
	(20 usuarios)	(5 usuarios)	(5 usuarios)
Licencia	21,600.00	2,800.00	26,000.00
Implementación	1,440.00		
Hora/especialista			
Capacitación	7,200.00	4,800.00	
Mantenimiento		1,025.00	
Soporte		700.00	
Total	30,240.00	9,325.00	26,000.00

[a]El costo de las Licencias de Delos incluyen la licencia de uso, manual digital, disco de instalación y Dongle de protección por usuario, así como una licencia para uso del software IDEA (para análisis de datos que incluye Dongle de protección, manual de uso y disco de instalación) capacitación para seis personas y una año de mantenimiento e implementación del software en sitio.

La herramienta más económica es Working Papers y la más cara es Delos.

[1]Técnicas de los Costos, Sealtiel Alatriste http://www.inei.gob.pe/web/metodologias/attach/lib604/cap3-6.htm

Tabla 4.2. Costos de inversión

	Auto Audit	Working Papers	Delos
Equipo de cómputo	6 laptop	6 laptop	2 laptop
Costo unitario	160.00	160.00	160.00
Total	960.00	960.00	320.00
Hardware	Ya existe	Ya existe	Ya existe
Software	30,240.00	9,325.00	26,000.000
Total	31,200.00	10,225.00	26,320.00

Una vez más la implementación más económica resulta ser la de Working Papers y la más cara es Auto Audit, estos son dos factores importantes a considerar para la elección de la herramienta adecuada; sin embargo, no son determinantes, ahora que se conoce el costo habrá de realizarse un análisis de la utilidad que estas herramientas traen consigo, cuales son más accesibles de implementar de acuerdo a su funcionalidad y que su ambiente sea amigable para el auditor a fin de que esta propuesta no contemple la contratación de nuevo personal, sino la capacitación del actual, para lo cual posteriormente se analizan los resultados de la aplicación de cuestionarios al personal que asistió a las demostraciones de los proveedores, de cada una de las técnicas de auditoría asistidas por computadora.

La implantación del área no implica necesariamente a aplicación de una CAAT así como la aplicación de una CAAT no necesariamente sucede sí y solo sí se implanta el área, esto es, no son indispensables una sin la otra; sin embargo el modelo óptimo de desarrollo de la Contraloría Interna de acuerdo a este informe de seminario de titulación contempla la implantación del área de auditoría en informática y además reforzar a toda la Subcontraloría de Auditoría con la utilización de la herramienta seleccionada.

Costos de oportunidad

Los costos de oportunidad son los que se derivan de hacer una cosa en lugar de otra.

La herramienta más barata es Working Papers, con un costo de $9,325.00 Dlls, contra la más cara que es Auto Audit de $30,240.00, por lo tanto la diferencia de $20,915.00 representa el costo de oportunidad de tomar esta alternativa.

A continuación, se presenta un análisis del equipo que se usaría en las actividades de esta área y el personal estimado que realizaría estas labores sin el uso de una herramienta de auditoría asistida por computadora para compararla contra el equipo y el personal que se requerirá al implantar una de estas herramientas.

ACTIVIDADES	**Sin uso de herramienta CAAT**		**Con uso de herramienta CATT**	
	Equipo	**Personal**	**Equipo**	**Personal**
1. Elaboración de planes de trabajo	3	6	1	1
2. Elaboración de cuestionarios, encuestas, matrices, etc.	6	12	1	1
3. Trabajo de campo.	6	12	3	12
4. Control de actividades a realizar en tiempos estimados reales.	3	6	1	1
5. Evaluación de resultados de los programas operativos.	3	6	1	1

ACTIVIDADES	Sin uso de herramienta CAAT		Con uso de herramienta CATT	
	Equipo	Personal	Equipo	Personal
6. Evaluación de la problemática de las áreas que cuenten con un sistema informático.	3	6	1	3
7. Elaboración de papeles de trabajo e informes de auditoría.	6	12	3	12
8. Comunicar los resultados y recomendaciones que resulten de sus evaluaciones.	12	12	2	12
9. Comprobar que el área de Sistemas ha tomado las medidas correctivas de los informes de la Auditoría Interna así como de las omisiones que al respecto se verifiquen en el seguimiento de informes.	3	6	1	1
10. Evaluación de los controles de seguridades lógicas y físicas.	2	2	1	1
11. Evaluación de los riegos y controles.	6	12	3	6
12. Evaluar la existencia de políticas[a], objetivos[b], normas[c], metodologías[d], así como la asignación de tareas y adecuada administración[e] de los recursos, humanos e informáticos.	6	12	1	1

[a]http://www.monografias.com/trabajos10/poli/poli.shtml
[b]http://www.monografias.com/trabajos16/objetivos-educacion/objetivos-educacion.shtml" [http://www.monografias.com/trabajos16/objetivos-educacion/objetivos-educacion.shtml]
[c]http://www.monografias.com/trabajos4/leyes/leyes.shtml
[d]http://www.monografias.com/trabajos11/metods/metods.shtml
[e]http://www.monografias.com/Administracion_y_Finanzas/index.shtml

Diagnóstico de personal

Deben seguirse procedimientos sistemáticos para identificar, seleccionar, programar, implantar, mantener, usar y controlar el software adquirido.

Uno de los esquemas generalmente aceptado para tener un adecuado control es que el personal que intervenga esté debidamente capacitado, con alto sentido de moralidad, al cual se le exija la optimización de recursos (eficiencia). Para complementar el grupo, como colaboradores directos en la realización de la auditoría se debe tener personas con las siguientes características:

- Técnico en informática
- Conocimientos de administración, contaduría y finanzas
- Experiencia en el área de Informática
- Experiencia en operación y análisis de sistemas
- Conocimientos y experiencia en psicología industrial
- Conocimiento de los sistemas más importantes

En cuanto a las certificaciones que se expusieron en Capítulo 3, *Legislación informática, mejores prácticas y técnicas de auditoría informática* se determina que la certificación CISA (Certified Information Systems Auditor) que la Asociación de Auditoría y Control de Sistemas de Información (ISACA), es la más conveniente para que el personal cumpla con la calidad de trabajo requerida, ya que esta certificación cubre el conocimiento tanto de auditoría como de Sistemas.

Análisis de la aplicación de cuestionarios

Por último, se aplicó un cuestionario al personal de la Subcontraloría de Auditoría, el formato lo encontraremos en Apéndice B, *Formato de cuestionario*, y los cuestionarios respondidos en Apéndice C, *Cuestionarios respondidos* , los resultados son los siguientes:

1. Consideras que es importante que la Subcontraloría de Auditoría adopte una técnica de auditoría asistida por computadora que apoye tu labor como auditor? ¿Por qué?

   - Sí 15
   - No Ninguno

   Motivos principales : Mejora el tiempo, calidad y presentación del trabajo, dando más tiempo al análisis y oportunidad en las auditorías, la supervisión sería más eficaz.

2. ¿Qué beneficios personales (como auditor) crees que tendría la adopción de una de estás herramientas?

   Beneficios principales: Principalmente ayuda para la elaboración de informes y papeles de trabajo, superación personal al conocer programas y herramientas que coadyuven a optimizar el trabajo, aprovechamiento de tiempos con ello mayor productividad, reducir errores e incongruencias, mayor control de la información, facilita la consulta de documentos, mantener una base de conocimiento actualizada

3. ¿Qué beneficios institucionales (para la H. Cámara de Diputados) crees que tendría la adopción de una de estás herramientas?

   Beneficios principales : Contar con una base de datos donde se almacene y documente toda la información generada en las auditorías, reducción de costos, aprovechamiento de tiempos, mejor presentación de reportes, más y mejores auditorías, información oportuna para toma de decisiones oportuna, estar a la vanguardia en técnicas de auditoría y de esta forma lograr el correcto desempeño de todas las áreas de la Cámara de Diputados

4. ¿Consideras que una de estas herramientas contribuiría al mejor cumplimiento de metas y objetivos de la Subcontraloría de Auditoría?

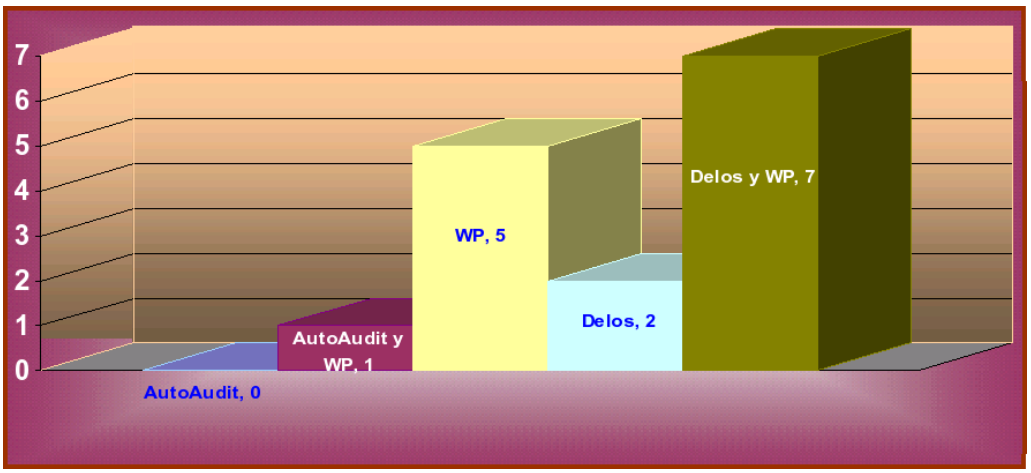
   - Sí: 15
   - No: Ninguno

5. ¿Consideras que sería muy complicado el aprendizaje necesario para que apliques este tipo de técnicas a tu trabajo?

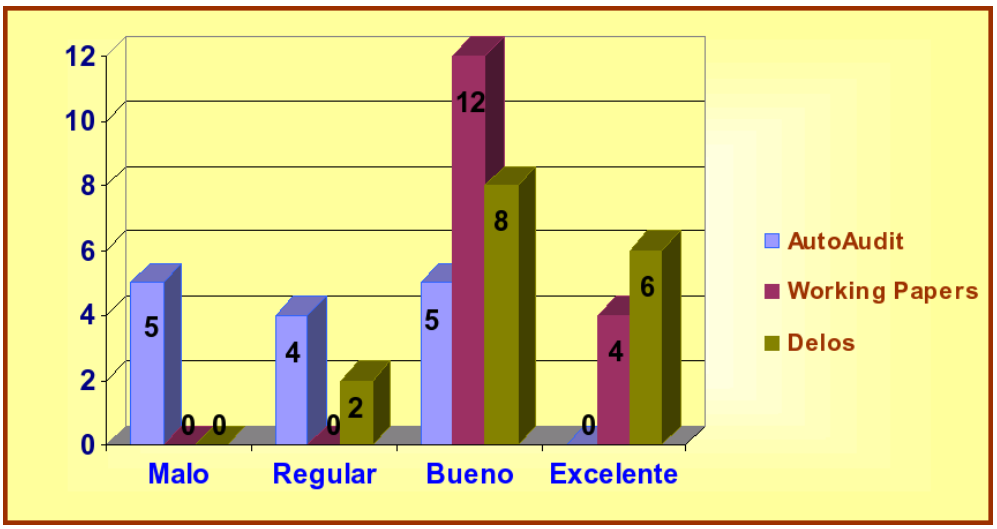
   - Sí: Ninguno
   - No: 15

   Observaciones principales: Solo es necesario tomar capacitación en la paquetería principal y la que el proveedor brinde de acuerdo al software especifico.

6. De los demos a los que asististe, ¿Qué producto crees que sería mejor adaptar a la Subcontraloría de Auditoría?



7. De acuerdo a su funcionalidad y facilidad de uso de los demos a los que asististe, ¿Qué calificación le darías a cada uno de ellos? (malo/regular/bueno/excelente)



8. ¿Qué comentarios tienes acerca de estos productos?

Principales Comentarios:

Auto Audit	Auto Audit Su manejo es más complicado, necesita ser complementado, la presentación no fue adecuada, no puede ser ajustado a las necesidades específicas de cámara por ello es inadecuado.
Working Papers	Working Papers Se puede adaptar específicamente a los procesos que se realizan aquí, es bueno solo que necesita una base de datos, más práctico en cuanto a los tiempos de respuesta, además cuenta con soporte técnico de calidad, el manejo de word y excel facilita su uso, conviene mucho para revisiones financieras, sería necesario un caso práctico para ver su funcionalidad.
Delos	Delos

Faltó más explicación; sin embargo puede ser aplicable con una buena capacitación lo podemos aplicar, puede funcionar en cuestión de control de los programas establecidos para las revisiones y tiempos de atención de los auditores, es el más adecuado para adaptarse a las necesidades específicas de la Cámara, debe considerarse un curso de este software, es el más adecuado

Capítulo 5. Propuesta de implantación de un área de auditoría en informática en un órgano legislativo

En este capítulo, una vez que ya se conoce la conformación de la H. Cámara de Diputados, mostramos la formación general de su Órgano de Control Interno y cómo encaja la Subcontraloría de Auditoría dentro de este Órgano Legislativo, se detallan las posibilidades en cuanto a mejores prácticas, certificaciones, técnicas de auditoría y herramientas automatizadas y del análisis a cada uno de ellos, de acuerdo a lo anterior se dan a conocer los resultados a los que se llega en el desarrollo de este informe de seminario de titulación.

Derivado del estudio de costo beneficio y de factibilidad, así como del análisis de las consecuencias y riesgos a los que se enfrentará el área al implantar esta área, así como de cuáles serían las consecuencias de seguir con la estructura y funciones, misma que se realiza para darle a los Mandos Medios y Superiores de la Contraloría Interna una visión a futuro de las mejoras que traería consigo la adaptación de esta propuesta, benéficas para este Órgano de Control Interno así como de estar a la vanguardia en las nuevas tendencias de auditoría en informática actuales, y con ello brindarle a la ciudadanía una mejor rendición de cuentas.

Así, en este capítulo, brindamos las bases y una guía completamente práctica del cómo y porqué es recomendable contar con un área o las funciones encaminadas a realizar auditorías en informática dentro de este Órgano, desde la óptica de las nuevas tendencias mundiales de auditoría y tratando de dar cumplimiento a las recientes Leyes de Transparencia y Acceso a la Información Pública Gubernamental.

Propuesta de creación del área de auditoría informática

Nuestro informe de seminario concretamente propone la implantación de un área de auditoría en informática dentro de la Subcontraloría de Auditoría de la H. Cámara de Diputados. Lo anterior, lo fundamos a lo largo de este informe, los principales motivos son:

1. Implantar esta área dentro del Órgano de Control Interno traerá consigo la innovación de la Subcontraloría de Auditoría para cubrir las funciones de una parte de la Cámara de Diputados que actualmente no es auditada, la Dirección General de Tecnologías de Información;

2. La eficiencia, eficacia y calidad de las auditorías que se realizan en el órgano se verán beneficiadas por la capacitación adecuada del personal y la consecuente automatización de procedimientos, que dejarán de ser tradicionales para estar a la vanguardia.

3. El crecimiento constante de la Dirección General de Tecnologías de Información eventualmente obligará a la Subcontraloría de Auditoría a implantar procedimientos para auditarla, es por ello que será benéfico aplicar estos procedimientos antes de ser rebasados en un futuro por esta problemática, es decir tomas medidas preventivas antes de afrontar una contingencia seria en la Cámara de Diputados.

Por lo anterior, en los siguientes puntos detallamos la propuesta específica que contempla cuales serían las actualizaciones más adecuadas para lograr este objetivo, comenzando por proponer los cambios pertinentes en la normatividad actual, cuál sería su nueva estructura orgánica, proponemos las nuevas funciones del área de auditoría en informática de acuerdo a las nuevas tendencias de la auditoría en Tecnologías de Información mundiales; asimismo, de entre las diferentes herramientas y técnicas de auditoría en informática, seleccionamos aquellas que resultarían más convenientes de acuerdo a las

características específicas de la Subcontraloría de Auditoría así como de la Dirección General de Tecnologías de Información, tomando en cuanta su tamaño, su capacidad y tecnología actual.

Objetivo

Evaluar el desempeño de los sistemas informáticos y las redes de comunicaciones para proporcionar los controles necesarios que permitan la confiabilidad de la Información así como un elevado nivel de seguridad.

Realizar auditorías operacionales, integrales, especiales y de cumplimiento al área de sistemas, ayudando en la gestión de control de la Auditoría Interna y buscando las áreas de oportunidad.

1. Evaluar los controles establecidos para proteger los bienes institucionales, referente al manejo hardware, software y valores.

2. Proporcionar al Órgano Legislativo, un conocimiento de la situación informática real del área de Sistemas.

3. Realizar auditorías operacionales, integrales, especiales y de cumplimiento a aquellas áreas administrativas y Grupos Parlamentarios que así lo requieran.

El Área de Auditoría Informática, como parte de la SubContraloría de la H. Cámara de Diputados tendrá como misión y visión, los que a continuación se describe:

Justificación de la creación del área

Es bien sabido que actualmente existe la necesidad de crear un ámbito de seguridad en cualquier organización, debido al aumento de casos internacionales de fraudes tanto contables como informáticos, como ya se mencionó anteriormente el activo más valioso de casi cualquier organización actualmente es precisamente la información, este es el caso de la Cámara de Diputados.

En base a los análisis realizados, se propone la creación de un área de Auditoría Informática que proporcione seguridad y control en el ámbito tecnológico, misma que deberá promover elevar la cultura informática tanto dentro de la Subcontraloría de Auditoría, como en el resto de la Cámara de Diputados. Esta área deberá estar encargada de constatar que se sigan procedimientos que aseguren la confidencialidad, confiabilidad y disponibilidad de los datos, garanticen la seguridad de la información y prevean las posibles contingencias en cuanto a la seguridad de la información que se maneja en este órgano, misma que por definición es muy delicada, asimismo que regule la gestión de la infraestructura y que en general se dedique a guiar el desarrollo y correcto funcionamiento del área de sistemas de esta Institución mediante las auditorías correspondientes.

Adicionalmente, esta área deberá contar con las actualizaciones sobre las regulaciones de la seguridad informática, mejores prácticas para aplicarlas a esta Institución, así como de las nuevas técnicas de auditoría en informática ya sean manuales o asistidas por computadora, apoyados en profesionales capacitados para mantener sistemas informáticos seguros, confiables y confidenciales, que eviten y prevengan la ocurrencia de situaciones de riesgo derivadas de las actuales debilidades en los sistemas de control.

Modificación a la normatividad existente

La normatividad que propone ser modificada comienza a nivel del Manual de Organización General de la Cámara de Diputados que en Capítulo 1, *Descripción del órgano legislativo y de su organo interno de control* se menciona textualmente, dentro del objetivo que ahí se plasma, deberá cambiar de la siguiente forma:

Importante

Vigilar que las operaciones de la Cámara de Diputados se realicen con apego a los programas y procedimientos establecidos de conformidad a la normatividad aplicable, verificando que el manejo y aplicación de los recursos financieros, humanos, materiales y tecnológicos se lleven a cabo de acuerdo con las disposiciones presupuestales en el Presupuesto de Egresos de la Federación.

Adicionalmente, en el Manual de Organización de la Contraloría General el texto propuesto es el siguiente:

Importante

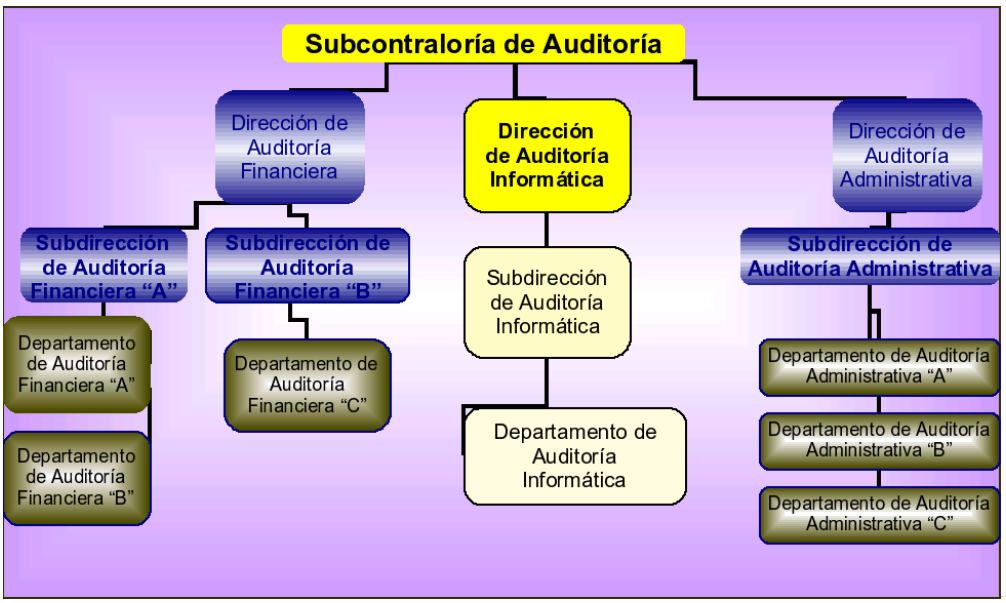
Establecer los mecanismos de fiscalización, control, auditoría y evaluación para supervisar el funcionamiento de las unidades administrativas dentro de su campo de acción, así como realizar las recomendaciones necesarias orientadas a mejorar los procedimientos administrativos que emplean las áreas, con el propósito de que éstas cumplan con los ordenamientos legales aplicables y así lograr el óptimo aprovechamiento de los recursos financieros, humanos, materiales y tecnológicos de los que dispone la Cámara.

Estructura orgánica de la Subcontraloría de Auditoría

La reestructuración de la Subcontraloría de Auditoría no estará completa si no contempla una modificación a su estructura orgánica que incluya un área que se dedique a realizar las funciones propias de la auditoría en informática, como se puede apreciar en la Figura 1.3, “Estructura orgánica de la Contraloría Interna de la Cámara de Diputados”, los puestos de la Subdirección hacia abajo son genéricos, lo que redunda en confusiones en los tramos de control y funciones, por ello y para acabar con esta problemática, además de incluir esta nueva área se propone que el Organigráma de la Subcontraloría detalle los nombres específicos de los puestos.

La nueva estructura orgánica de la Subcontraloría de Auditoría deberá establecerse como se indica en la Figura 5.1, “Nueva estructura orgánica para la Subcontraloría de Auditoría”.

Figura 5.1. Nueva estructura orgánica para la Subcontraloría de Auditoría



Misión, visión y funciones del área de Auditoría Informática.

En esta parte del capitulo, serán presentadas las funciones que deberá realizar el Área de Auditoría Informática, como parte de la Subcontraloría de la H. Cámara de Diputados; mismas que han sido definidas para la realización de auditorias internas dentro de éste Órgano Legislativo.

Misión. Brindar a través de las auditorías, la información suficiente y competente, que permita la implementación de controles para una mejora continua que ayude a la prevención de delitos informáticos.

Visión. Consolidar el Área de Auditor í a Informática, como un área que pueda prever apoyo y asesoría a la H. Cámara de Diputados, para el cumplimiento de sus metas institucionales.

Funciones. El área de Auditoría Informática deberá realizar las actividades correspondientes a la verificación de los controles internos establecidos en el área de Sistemas así como estudios de seguridad física y lógica; análisis de los riesgos a que está expuesta la información y los equipos y la elaboración de documentación que en las auditorías sea requerida. Además deberá promover elevar la cultura informática tanto dentro de la Subcontraloría de Auditoría, como en el resto de la Cámara de Diputados, constatar que se sigan procedimientos que aseguren la confidencialidad, confiabilidad y disponibilidad de los datos, garanticen la seguridad de la información y prevean las posibles contingencias en cuanto a la seguridad de la información que se maneja en este órgano, misma que por definición es muy delicada, asimismo que regule la gestión de la infraestructura y que en general se dedique a guiar el desarrollo y correcto funcionamiento del área de sistemas de esta Institución mediante las auditorías correspondientes.

A continuación se listan las funciones principales que esta área, deberá llevar a cabo.

1. Elaboración de planes de trabajo para llevar a cabo auditorías en informática y el desarrollo de actividades apropiadas que permitan maximizar la eficacia del área de sistemas.

2. Elaboración de cuestionarios, encuestas, matrices y herramientas que ayuden al levantamiento de la información para el debido desarrollo de las auditorías.

3. Implementación de los planes de trabajo llevando un control de las actividades a realizar en tiempos estimados reales.

4. Evaluación de sistemas, procedimientos y equipos de cómputo.

5. Verificar que los activos, estén debidamente controlados y salvaguardados contra pérdida y mal uso.

6. Evaluar los resultados de los programas operativos que realice el área de Sistemas para conocer eficiencia y efectividad con que se han utilizado los recursos.

7. Comprobar el cumplimiento de mandatos constitucionales, legales y reglamentarios, políticas, planes y acuerdos normativos que rigen a la Institución.

8. Realizar auditorías y estudios especiales de acuerdo con programas y especiales debidamente respaldados por las Normas para el ejercicio profesional de la Auditoría Interna.

9. Evaluar la problemática del área de Sistemas a través de un pre-análisis de la situación del área, para la determinación de las principales necesidades de ésta.

10. Comunicar los resultados y recomendaciones que resulten de sus evaluaciones, mediante los informes de auditoría.

11. Comprobar que el área de Sistemas ha tomado las medidas correctivas de los informes de la Auditoría Interna así como de las omisiones que al respecto se verifiquen en el seguimiento de informes.

12. Evaluación de los controles de seguridades lógicas y físicas que garanticen la integridad, confidencialidad y disponibilidad de los datos de esta institución.

13. Constatar que el área de sistemas se riga por los procedimientos más adecuados para garantizar el adecuado funcionamiento de la red de trabajo.

14. Evaluación de los riegos y controles establecidos para la búsqueda e identificación de debilidades, así como de las áreas de oportunidad

15. Evaluar la existencia de políticas[1], objetivos[2], normas[3], metodologías[4], así como la asignación de tareas y adecuada administración[5] de los recursos, humanos e informáticos.

16. Generar el Archivo de Papeles de Trabajo con la documentación las auditorías realizadas.

Tipos de auditoría que realizará el área de Auditoría Informática.

1. Auditoría a Sistemas de Información,

2. Auditoría a las Comunicaciones,

3. Auditoría a la Red Física, y

4. Auditoría a la Red Lógica.

Metodología para la realización de auditorías informáticas

Para la realización especifica de auditorías en informática se propone también se propone una metodología especifica, misma que se menciona a continuación:

- Conocimiento general del área de sistemas
    - Organigrama
    - Estructura del área o departamento
    - Relaciones funcionales y jerárquicas
    - Recursos (equipos con los que se cuenta)
    - Aplicaciones en desarrollo
    - Aplicaciones en producción
    - Sistemas de explotación
- Planificación
    - Concentración de objetivos

[1] http://www.monografias.com/trabajos10/poli/poli.shtml
[2] http://www.monografias.com/trabajos16/objetivos-educacion/objetivos-educacion.shtml" [http://www.monografias.com/trabajos16/objetivos-educacion/objetivos-educacion.shtml]
[3] http://www.monografias.com/trabajos4/leyes/leyes.shtml
[4] http://www.monografias.com/trabajos11/metods/metods.shtml
[5] http://www.monografias.com/Administracion_y_Finanzas/index.shtml

- Definición de objetivos y alcances
- Personas de la organización que se involucrarán en el proceso de auditoría
- Plan de trabajo
  - Tareas
  - Calendario
  - Resultados parciales
  - Presupuesto
- Desarrollo de la auditoría
  - Entrevistas
  - Cuestionarios
  - Observación de las situaciones deficientes
  - Observación de los procedimientos
- Fase de diagnóstico
  - Definición de los puntos débiles y fuertes, los riesgos eventuales y posibles tipos de solución y mejora
- Presentación de conclusiones
  - Integración de soporte documental
  - Formulación de cédulas de observaciones y papeles de trabajo
  - Informe final
- Formación del plan de mejoras
  - Resumen de las deficiencias encontradas
  - Recogerá las recomendaciones encaminadas a paliar las deficiencias detectadas
  - Medidas a corto plazo: mejoras en plazo, calidad, planificación o formación
  - Medidas a medio plazo: mayor necesidad de recursos, optimización de programas o documentación y aspectos de diseño
  - Medidas a largo plazo: cambios en políticas, medios y estructuras del servicio
  - Seguimiento de cumplimiento de recomendaciones

Guía de auditoría

Existirán tantas guías de auditoría como procedimientos se realicen, sin embargo, a manera de ejemplo, se presenta la siguiente guía como propuesta de las subsecuentes:

Unidad administrativa	**Objetivos**
Punto de revisión	Aspectos a revisar

Unidad administrativa	**Objetivos**
Objetivo general:	Verificar que la seguridad física y lógica en la red de la H. Cámara de Diputados que maneja la Dirección General de Tecnologías de Información.
	Actividades:
Dirección General de Tecnologías de Información	1.- Conocimiento general de la Dirección General de Tecnologías de Información a fin de conocer sus instalaciones, tamaño, condiciones de trabajo, software, hardware, estructura, etc.
	2.- Definición de objetivos y alcances de auditoría claros y bien delimitados de acuerdo a la magnitud del área a revisar.
	3.- Realización de Gráfica de GANTT para planeación de actividades y tiempos estimados de inicio y término de auditoría.
	4.- Preparación del formato de oficio de presentación.
	5.- Preparación del cuestionario de control interno y demás material de apoyo.
	6.- Conocimiento previo de los manuales de procedimientos, manuales de organización, planes de contingencia, recuperación, lineamientos, políticas, normas, reglamentos, procedimientos, etc., existentes en el área.
	7.- Preparación de pruebas de cumplimiento, para la realización de pruebas generales y específicas a fin de cubrir el alcance de la revisión.
	8.- Preparación del material de apoyo, formato de cédulas de marcas, guía de auditoría, cuestionario, check list, formato de papeles de trabajo, cédulas de observaciones, etc.
	9.- Aplicación del oficio de presentación.
	10.- Plática con el equipo, para determinar el desarrollo de la auditoría y actividades a realizar.
	11.- Levantamiento de la información. Aplicación de técnicas de auditoría y material de apoyo previamente diseñado para la obtención de información.
	12.- Análisis de la información.- Detección de debilidades de control, identificación de observaciones por medio del análisis de la información recabada. Así como determinación de causas e impactos.
	13.- Integración de Papeles de trabajo.- Apoyados en las pruebas necesarias, como son los cuestionarios, fotografías o cualquier tipo de constancia de hechos.
	14.- Confirmación de observaciones.- Verificar que las observaciones están fundamentadas y que se cuenta con la evidencia suficiente para presentar las observaciones levantadas.
	15.- Identificación de niveles de riesgo.- Por medio del análisis de la información de cada una de las observaciones, se le asocia un nivel de riesgo; inminente, potencial o controlable.
	16.- Consolidación de niveles de riesgo.- Agrupación de observaciones comunes, con objeto de determinar las debilidades y sugerencias de forma general.
	17.- Elaboración del informe final.
	18.- Actividades finales de papeles de trabajo.

Requerimientos para creación del área de Auditoria Informática

Dados los antecedentes con los que contamos sobre la estructura de la Subcontraloría Auditoría de la H. Cámara de Diputados, su conformación y los activos informáticos con los que cuenta, a continuación

realizamos la propuesta de los requerimientos que serán necesarios para el funcionamiento de la nueva área.

Requerimientos de hardware y software

En este apartado proponemos la herramienta y el equipo que será necesario para la implantación de esta nueva área. Los factores relevantes para la determinación de la adquisición de estos activos son los siguientes:

- Proveedor CYNTHUS
- Herramienta DELOS
- Mejor Practica COBIT
- Precio $26000 dls (herramienta y mejor práctica)
- Cantidad de equipos existentes 18 PC
- Cantidad de equipos necesarios 6 laptop adicionales
- Características de equipos modelo Pentium 4
- Equipos auxiliares SQL Server

Requerimientos de personal

Puestos	**Plazas**	**Experiencia en el puesto**	**Capacitación requerida**	**Horas de capacitación**
Dirección General	1	5	B	24
Subdirección	1	3	B	24
Jefe de Departamento	1	2	C	24
Auditores	1	5	C	24

Claves

Tipo de capacitación Requerida

A. Principiante

B. Intermedio

C. Avanzado

Pasos a realizar para la implantación del área

Derivado de este informe, se determina que los pasos más recomendables para la implantación del área de auditoría en informática son los siguientes:

1. Presentar la propuesta al Comité de Administración para la implantación del área de auditoría en informática.
2. Revisión de la propuesta para la implantación del área.
3. Aprobación de la propuesta.
4. Modificaciones a la estructura orgánica y normatividad pertinente.

5. Solicitud de recursos para infraestructura, personal, software y/o capacitación.
6. Remodelación de áreas.
7. Contratación y/o capacitación de personal.
8. Adquisición de equipo de hardware.
9. Adquisición de software especializado.
10. Inclusión de la(s) auditoría(s) en el PACA.
11. Aplicación de la metodología para las revisiones al área de sistemas.

Propuesta de mejor práctica

El objetivo que se persigue al establecer que el área de auditoría en informática haga uso de una mejor práctica es promover una cultura informática que ayude al cumplimiento de las metas organizacionales de seguridad y calidad de la información respaldadas por una organización mundial que aporte la experiencia en este campo, mediante el establecimiento de controles.

Justificación

La misión y objetivo principal de COBIT es investigar, desarrollar, publicar y promocionar objetivos de control de TI internacionales, actualizados a la realidad actual para ser usados por los gerentes de negocios y auditores.

COBIT ha sido desarrollado como estándares generalmente aplicables y aceptados para mejorar las prácticas de control y seguridad de las TI, que provean un marco de referencia para la administración, los usuarios y los auditores de cualquier tipo.

Hemos considerado que COBIT es la mejor práctica que podría ser de mayor utilidad a la Subcontraloría de Auditoría, debido a que provee a la administración un entendimiento de los principios y conceptos claves sobre los requerimientos del negocio para la información e impactos preliminares de recursos de TI a detalle en sus 34 Objetivos de Control de TI.

COBIT preverá al negocio de guías de auditoría, las cuales contienen pasos de auditoría sugeridos, correspondientes a cada uno de los 34 Objetivos de Control, estas guías serán un macro para asistir a los auditores de sistemas de información en cuanto a las en revisiones de los procesos de TI y la seguridad de la administración.

Objetivo

Importante

Preparar a los funcionarios en temas como auditoría, seguridad y control de TI. Así como en impulsar la investigación y el desarrollo de temas sobre seguridad y riesgos en cuanto al uso de TI.

Propuesta de herramienta CAAT

Del análisis realizado en Capítulo 4, *Análisis de información*, determinamos que es importante la implantación de una herramienta CAAT dados los beneficios que estas proveen a la organización.

Esencialmente el uso de una herramienta CAAT mejoraría favorablemente la realización de las actividades de la Subcontraloría de Auditoría principalmente en lo que se refiere a los tiempos de realización de las actividades que actualmente se desempeñan así, como en las que se han propuesto para la nueva área de auditoría en informática.

De las 3 herramientas que fueron comparadas, hemos determinado que Delos By Cynthus es la que proporciona mayores beneficios y mayor funcionalidad, además de ser la que se adapta al 100% a las necesidades específicas del área.

Adicionalmente Delos como propuesta de herramienta CAAT incorpora todos los componentes de COBIT y es un complemento ideal para el software de extracción y análisis de datos (IDEA), ya que permite identificar las causas (deficiencias en el control interno de TI) de posibles inconsistencias en los archivos de datos.

Capítulo 6. Conclusión

Durante el desarrollo de este informe de seminario de tesis, podemos observar que en la Cámara de Diputados las tecnologías de información no han sido controladas por su Órgano de Control Interno, siendo este la Subcontraloría de Auditoría, y debido a la creciente dependencia de toda organización en su activo informático más importante “la información”, ésta debe ser correctamente gestionada, controlada y asegurada por medio de controles que prevengan la ocurrencia de situaciones de riesgo para la organización y que a su vez asegure su integridad, disponibilidad y confidencialidad tanto de los datos como de los procesos, asimismo, contar con mecanismos de recuperación.

La propuesta de la creación de un área de auditoría en informática, deberán estar apoyada en las nuevas técnicas y procedimientos de auditoría como son análisis de datos de prueba, simulación paralela, paquetes de auditoría, software de auditoría, juegos de prueba, entre otros.

De manera importante, se concluye que los productos de software especiales para la auditoría informática son de particular importancia para el apoyo de la labor de auditoría, no solo en informática, sino de cualquier área debido a la facilidad con que el auditor podrá manipular la Información con algunas de las antes mencionadas técnicas y procedimientos de auditoría informática.

Para lo cual, y en base a los análisis efectuados se recomienda el uso de las técnicas de auditoría asistidas por computadora, ya que son de gran utilidad para un área de auditoría informática, debido a que con su uso se obtiene considerables beneficios tanto para la Subcontraloría de Auditoría como para la Cámara de Diputados, como son: reducción de los tiempos hombre por concepto de realización de papeles de trabajo e informes de auditoría y mayor dedicación al trabajo sustantivo y pruebas de cumplimiento, mejora de la calidad en la presentación y contenido de cada auditoría, aumento de programación y cumplimiento, estandarización del trabajo de auditoría y reducción de costos para la realización de las mismas por insumos.

Como último factor de decisión para la selección de esta herramienta fue su costo y los beneficios que conlleva la propuesta, ya que es más bajo que el las demás comparando los beneficios que esta provee y sus funcionalidades extras.

Es muy importante mencionar que dentro del análisis de costo beneficio pudimos percatarnos que la organización no cuentan con los suficientes elementos para el buen funcionamiento de un área de auditoría dentro de la Subcontraloría de Auditoría.

Concluimos, por tanto que esta propuesta aportará considerables beneficios a la Contraloría Interna, los principales son mayor eficiencia en el trabajo, contar con una base de conocimiento que pueda retroalimentar a los auditores y apoyar sus funciones, flexibilidad de procesos, estandarización y control, adaptabilidad a los diferentes procesos, mayor comunicación, reducción de costos y aprovechamiento de recursos materiales y humanos, garantizar la seguridad, confiabilidad y disponibilidad de los datos, facilidad en el manejo de la información y mayor integración en los equipos de trabajo.

Capítulo 7. Bibliografía

Libros

[bib-solis-2002] *Reingeniería de la Auditoría Informática*. Gustavo Adolfo. Solís Montes. 2002. Trillas. México.

Metodología de la Investigación. Roberto. Hernández Sapieri. Segunda Edición. 1997. McGraw-Hill. México.

Constitución Política de los Estados Unidos Mexicanos. http://constitucion.presidencia.gob.mx/index.php?idseccion=211 .

Normas y Procedimientos de Auditoría. Comisión de Normas y Procedimientos de Auditoría, Instituto Mexicano de Contadores Públicos. 2ª Edición. Agosto de 2000. ANFECA.

Estatuto de la Organización Técnica y Administrativa y del Servicio de Carrera de la Cámara de Diputados.

Letras de oro en los muros de honor de la Cámara de Diputados. Comisión de Reglamentos y Prácticas Parlamentarias LIX Legislatura. Primera Edición. Agosto de 2003. Vargas Impresores, S.A.

[bib-ti-complejos] *Formulación de mejores prácticas para entornos TI Complejos*. Eli Egozi, Mike Stephenson, y John Kampman.

Auditoría informática en la empresa. Juan José Archa Itumendi. Ed. Paraninfo.

Auditoría Informática. Mario G. Piattini y Emilio Peso Navarro. Ed. RA-MA.

[bib-guia-17799] *MANAGEMENT SYSTEMS Guía para la implementación del Sistema de Gestión de Seguridad de la Información ISO 17799*. Miguel Díaz S..

Ingeniero de Sistemas. / Socio consultor de AUDISIS / Líder de proyectos de adopción de ITL en Argentina y Venezuela
.

Auditoría informática: un enfoque práctico. 2ª Edición, ampliada y revisada.

[bib-rusbacki-2004] *Sarbanes-Oxley, IT Governance and Enterprise Change Management*. Tim Rusbacki. 2004. MKS White Paper.

[bib-kearns-1994] *Benchmarking*. David T. Kearns. Primera edición. 1994.

Técnicas de la auditoría inforrmática. Yann Derrien. Ed. Marcombo.

[bib-imcp] *Normas y procedimientos de auditoría*. Instituto Mexicano de Contadores Públicos (IMCP).

[bib-zavaro-martinez] *Auditoría informática, las técnicas de auditoría asistidas por computadora (CAAT)*. L. Zavaro y C. Martínez.

Formulación y Evaluación de Proyectos. Francisco Baca Urbina.

Técnicas de los Costos. Sealtiel Alatriste.

Auditoría en Informática. José A. Echenique. McGraw-Hill.

Auditoría en Centros de Cómputo. David H Li. Ed. Trillas.

[bib-manual-camara-diputados] *Manual de Organización General de la Cámara de Diputados* . http://cddhcu.gob.mx/organiza.html .

Instituto de Auditores Internos de España. . V Reunión de Auditores Internos de Banca Central Exposición de Banco de México. 1985. .

[bib-conceptos-itil] *Conceptos Generales sobre ITIL* . Lic. . Patricia Combalia. itSMF Argentina. Buenos Aires. 22 Abril 2005.

[bib-sun-itil] *Soporte de servicios ITIL*. Sun Microsystems. http://www.sun.es/services/itil .

[bib-camara-diputados-web] *Página oficial de la Cámara de Diputados*. http://cddhcu.gob.mx/ .

[bib-isaca-mx] Isaca capítulo Ciudad de México, A.Chttp://www.isaca.com.mx/.

[bib-novell-sarbanes-oxley] *A Flexible Approach for Sarbanes-Oxley and Other Business Drivers [http://www.monografias.com/trabajos16/novell-cuatro-x/novell-cuatro-x.shtml],White Paper*. Novell. 2004. .

Referencias en Internet

- http://www.cibertec.edu.pe/modulos/noticias.asp?ARE=1&PFL=2&NOT=912
- http://www.datasec.com.uy/index.php?option=content&task=view&id=65&Itemid=62
- http://www.emb.cl/gerencia/articulo.mv?sec=14&num=85
- http://www.isaca.org.mx
- http://www.economia.gob.mx
- http://www.tecnologiaempresarial.info/circuito5.asp?id_nota=10568&ids=2
- http://www.info.ccss.sa.cr
- Comité Directivo de CobiT/ISACA [http://www.datasec.com.uy/]
- http://www.datasec.com.uy/ oxely-coso.pdf
- http://www.theiia.org/index.cfm?doc_id=56
- http://www.theiia.org/
- http://www.theiia.org/index.cfm?doc_id=5119
- http://www.facpece.org.ar/boletines/37/60a-confederacion.htm
- http://www.isaca.org
- http://www.theiia.org/index.cfm?doc_id=56
- http://www.inei.gob.pe/web/metodologias/attach/lib604/cap3-6.htm
- http://www.glosarium.com/term/178,12,xhtml
- h t t p : / / w w w . i n e i . g o b . p e / w e b / m e t o d o l o g i a s / a t t a c h / l i b 6 0 4 / h t m [http://www.inei.gob.pe/web/metodologias/attach/lib604/cap3-6.htm]
- http://www.glosarium.com/term/178,12,xhtml
- http://www.itlp.edu.mx/publica/tutoriales/desproyectos/tema%203_1.htm
- http://Ilustrados.com/Publicaciones/Epyfapup.php

Glosario de términos

Algoritmo:	Procedimiento o conjunto de procedimientos que describen una asociación de datos lógicos destinados a la resolución de un problema. Los algoritmos permiten automatizar tareas.
Aplicación:	Aunque se suele utilizar indistintamente como sinónimo genérico de 'programa' es necesario subrayar que se trata de un tipo de programa específicamente dedicado al proceso de una función concreta dentro de la empresa.
Archivo de datos:	Cualquier archivo creado dentro de una aplicación: por ejemplo, un documento creado por un procesador de textos, una hoja de cálculo, una base de datos o un gráfico. También denominado Documento.
Archivo de programa:	Archivo ejecutable que inicia una aplicación o programa. Los archivos de programa tienen las extensiones EXE, PIF, COM o BAT.
Archivo de revisión de auditoría:	Involucra módulos incrustados en una aplicación que monitorea continuamente el sistema de transacciones. Recolecta la información en archivos especiales que puede examinar el auditor
Archivos log:	Archivo de texto que almacena generalmente datos sobre procesos determinados. Para entendernos, es como el "diario" de algunos programas donde se graban todas las operaciones que realizan, para posteriormente abrirlos y ver qué es lo que ha sucedido en cada momento.
Auditor:	Persona que efectúa una auditoría
Auditoría:	Examen de las operaciones de una empresa por especialistas ajenos a ella y con objetivos de evaluar la situación de la misma.
Bases de Datos:	Colección de datos organizada de tal modo que el ordenador pueda acceder rápidamente a ella. Una base de datos relacionar es aquella en la que las conexiones entre los distintos elementos que forman la base de datos están almacenadas explícitamente con el fin de ayudar a la manipulación y el acceso a éstos.
Batch:	En informática, un BATCH es un programa que se ejecuta de forma independiente sin la interacción del usuario. Un ejemplo de archivo Batch puede ser el AUTOEXEC.BAT de los antiguos sistemas basados en DOS.
Benchmarking:	Técnica de auditoría informática en la cual se realiza el proceso continuo de medir productos, servicios y prácticas contra los competidores o aquellas compañías reconocidas como líderes en la industria
Bitácoras:	Es como el "diario" de algunos programas donde se graban todas las operaciones que realizan, para posteriormente abrirlos y ver qué es lo que ha sucedido en cada momento.
CAAT :	Técnicas de Auditoría Asistidas por Computadora, son herramientas (software) que ayudan al auditor a facilitar sus tareas.
C.I.A:	Certified Internal Auditor Certificación de Auditores Internos
C.I.M.S:	Certified Information Security Manager Certificación para la Administración de la Seguridad de la Información
C.I.S.A:	Certified Information Security Auditor Certificación en Auditor en Sistemas de Información

Cliente:	Cliente o 'programa cliente' es aquel programa que permite conectarse a un determinado sistema, servicio o red.
Cliente-Servidor:	Se denomina así al binomio consistente en un programa cliente que consigue datos de otro llamado servidor sin tener que estar obligatoriamente ubicados en el mismo ordenador. Esta técnica de consulta 'remota' se utiliza frecuentemente en redes como 'Internet'.
Confidencialidad:	Se refiere a que la información solo puede ser conocida por individuos autorizados.
Costo:	Desembolso en efectivo o en especie por algún beneficio.
Costo estándar:	Son los que resultan de la suma de precios obtenida sobre las especificaciones de un producto, atendiendo a las unidades básicas anticipadas para el material, trabajo y gastos que entran en su producto.
Costos de inversión (largo plazo):	Esto es equipo de cómputo, hardware, software.
Costos de operaciones:	Estos gastos los origina la administración del Órgano Legislativo, así como inventarios, mano de obra, etc.
Costos de oportunidad:	Son los costos que se derivan de hacer una cosa en lugar de otra.
Costos estimados:	Son los cálculos anticipados de los gastos que predominarán en el futuro (mano de obra, material, etc), dentro de un periodo dado, con la intención de pronosticar un costo total.
Costos fijos:	Son los costos necesarios al inicio de las operaciones de cualquier empresa y
Costos fijos:	Son los costos necesarios al inicio de las operaciones de cualquier empresa y que se mantienen constantes en los diferentes niveles de producción a corto y mediano plazo, como son los salarios de los ejecutivos, los alquileres de locales, los intereses, etc.
Costos indirectos de producción:	Son los formados por aquellos gastos que no pueden ser rápidamente asociados con el producto (técnicos, papelería, renta, herramientas)
Criptografía:	Ciencia dedicada al estudio de técnicas capaces de conferir seguridad a los datos. El cifrado es fundamental a la hora de enviar datos a través de las redes de telecomunicaciones con el fin de conservar su privacidad.
Datos:	Término general para la información procesada por un ordenador.
Dirección IP:	Dirección numérica obligatoria de un dominio 'Internet'. Está compuesta por cuatro cifras (de 0 a 255) decimales separadas por puntos. Por ejemplo: 194.179.52.25 corresponde a la dirección IP de 'ctv.es'
Factibilidad:	Es la disponibilidad de los recursos necesarios para llevar a cabo los objetivos o metas señaladas, sirve para recopilar datos relevantes sobre el desarrollo de un proyecto y en base a ello tomar la mejor decisión.
Gobernabilidad de TI:	
Hardware:	Conjunto de dispositivos de los que consiste un sistema. Comprende componentes tales como el teclado, el Mouse, las unidades de disco y el monitor.
I.I.A:	Institute of Internal Auditors
I.M.A.I.:	Instituto Mexicano de Auditores Internos, A.C.

I.S.A.C.A:	Information Systems Audit and Control Association Asociación de Auditoría y Control de Sistemas de Información
IMCP:	Acrónimo del Instituto Mexicano de Contadores Públicos.
Integridad:	La habilidad de determinar que la información recibida es la misma que la información enviada.
Internet:	Interconexión de redes informáticas que permite a las computadoras conectadas comunicarse directamente.
IP:	Acrónimo de Internet. Es el protocolo que facilita la comunicación entre ordenadores conectados a la red Internet. Cada ordenador en Internet tiene una dirección IP única, que le identifica dentro de la red y permite su localización para posibilitar la comunicación.
ISO:	(Organización Internacional para la Normalización) Organización de carácter voluntario fundada en 1946 que es responsable de la creación de estándares internacionales en muchas arreas, incluyendo la informática y las comunicaciones. Esta formada por las organizaciones de normalización de sus 89 países miembro
Lenguaje:	En informática, conjunto de caracteres e instrucciones utilizadas para escribir programas de ordenador.
Metodología:	Conjunto de métodos utilizados en la investigación científica
Norma:	Principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad.
Papeles de trabajo:	Registra el planeamiento, naturaleza, oportunidad y alcance de los procedimientos de auditoría aplicados por el auditor y los resultados y conclusiones extraídas a la evidencia obtenida. Se utilizan para controlar el progreso del trabajo realizado para respaldar la opinión del auditor. Los papeles de trabajo pueden estar constituidos por datos conservados en papel, película, medios electrónicos u otros medios.
Paquete de auditoría:	Generalizados de computadora diseñados para desempeñar funciones de procesamiento de datos que incluyen leer archivos de computadora, seleccionar información, realizar cálculos, crear archivos de datos e imprimir informes en un formato especificado por el auditor
Parámetro:	Valor especificado para conseguir los resultados deseados. En comunicaciones existe tal cantidad de parámetros que suelen ofuscar a los usuarios noveles: bits por segundo, bits de datos, bits de parada, paridad, etc. Información que se añade al comando que inicia una determinada aplicación. Un parámetro puede ser un nombre de archivo o cualquier tipo de información de hasta 62 caracteres de largo. Vea también Opción.
Password:	Conocida también como 'clave de acceso'. Palabra o clave privada utilizada para confirmar una identidad en un sistema remoto que se utiliza para que una persona no pueda usurpar la identidad de otra.
Procedimiento:	Método o sistema estructurado para la ejecución de actividades
Procedimiento:	En computación, una subrutina o subprograma, como idea general, se presenta como un algoritmo separado del algoritmo principal, el cual permite resolver una tarea específica.

Procesamiento de datos:	Conjunto de diferentes operaciones en secuencia sistemática sobre el dato, las cuales se basan en la elaboración, manipuleo y tratamiento del mismo, mediante máquinas automáticas para producir los resultados esperados.
Procesamiento por lotes:	Archivo de texto que contiene comandos MS-DOS. Cuando se ejecuta un programa de procesamiento por lotes, MS-DOS ejecuta cada uno de los comandos del archivo, tal como si se hubiesen escrito directamente 1 continuación del símbolo de MS-DOS.
Proceso:	Conjunto de operaciones lógicas y aritméticas ordenadas, cuyo fin es la obtención de resultados.
Programa:	Secuencia de instrucciones que obliga al ordenador a realizar una tarea determinada.
Programa cliente:	Programa cliente o simplemente 'cliente' es aquel programa que permite conectarse a un determinado sistema, servicio o red.
Programa emergente:	Programa residente cargado en la memoria, que no es visible hasta que se presione una determinada combinación de teclas o hasta que tenga lugar un determinado hecho, tal como la recepción de un mensaje.
Programas:	Proyecto o planificación ordenada de las distintas partes o actividades que componen algo que se va a realizar.
Programas de administración del sistema:	Herramientas de productividad sofisticadas que son típicamente parte de los sistemas operativos sofisticados, por ejemplo software para recuperación de datos o software para comparación de códigos. Como en el caso anterior estas herramientas no son específicamente diseñadas para usos de auditoría y deben ser utilizadas con cuidado
Programas de utilería:	Son usados por la entidad para desempeñar funciones comunes de procesamiento de datos, como clasificación, creación e impresión de archivos. Estos programas generalmente no están diseñados para propósitos de auditoría y, por lo tanto, pueden no contener características tales como conteo automático de registros o totales de control
Red:	Servicio de comunicación de datos entre ordenadores. Conocido también por su denominación inglesa: 'network'. Se dice que una red está débilmente conectada cuando la red no mantiene conexiones permanentes entre los ordenadores que la forman. Esta estructura es propia de redes no profesionales con el fin de abaratar su mantenimiento.
Repositorio:	Donde se almacenan los elementos definidos o creados por la herramienta, y cuya gestión se realiza mediante el apoyo de un Sistema de Gestión de Base de Datos (SGBD) o de un sistema de gestión de ficheros
Rutinas de auditoría embebidas en Programas de aplicación:	Módulos especiales de recolección de información incluidos en la aplicación y diseñados con fines específicos
Servidor o server:	Ordenador que ejecuta uno o más programas simultáneamente con el fin de distribuir información a los ordenadores que se conecten con él para dicho fin. Vocablo más conocido bajo su denominación inglesa 'server'.
Sintaxis:	Como en las lenguas humanas, la sintaxis es el conjunto de reglas estructurales que gobiernan el uso del lenguaje en el ordenador.
Sistema de información:	Se denomina Sistema de Información al conjunto de procedimientos manuales y/o automatizados que están orientados a proporcionar información para la toma de decisiones.

SnapShots:	Es una fotografía interna al sistema, es decir a la memoria, lo que permite obtener resultados intermedios en diferentes momentos de un proceso o conseguir valores temporales de una variable. Se activa mediante ciertas condiciones preestablecidas. Permite al auditor rastrear los datos y evaluar los algoritmos aplicados a los datos
Software:	Componentes inmateriales del ordenador: programas, sistemas operativos, etc.
Software aplicado:	Programas escritos para la realización de tareas especiales, como el procesado de palabras o listas de correspondencia.
Software de sistemas:	Secciones de códigos que llevan a cabo tareas administrativas dentro del ordenador o ayudan en la escritura de otros programas, pero que no se usan para realizar la tarea que se quiere que ejecute el ordenador.
Software para un propósito específico o diseñado a la medida:	Son programas de computadora diseñados para desempeñar tareas de auditoría en circunstancias específicas. Estos programas pueden ser desarrollados por el auditor, por la entidad, o por un programador externo contratado por el auditor. En algunos casos el auditor puede usar programas existentes en la entidad en su estado original o modificado porque puede ser más eficiente que desarrollar programas independientes
T.I:	Tecnologías de Información
Técnica:	La técnica es el procedimiento o el conjunto de procedimientos que tienen como objetivo obtener un resultado determinado, ya sea en el campo de la ciencia, de la tecnología, de las artesanías o en otra actividad
Técnicas:	Conjunto de procedimientos de una ciencia los cuales nos ayudan a solucionar problemas.
Tunning:	Técnica de observación, de medidas encaminadas a la evaluación del comportamiento del sistema en su conjunto.
UNIX:	Potente y complejo sistema operativo multiproceso/multitarea y multiusuario orientado a comunicaciones y gran devorador de 'RAM'. Fue creado en 1969 por Ken Thompson y Dennis Ritchie (de la empresa norteamericana 'AT&T Laboratories') coincidiendo con el nacimiento de 'Internet'.

Apéndice A. Cotización de proveedores

Apéndice B. Formato de cuestionario

Apéndice C. Cuestionarios respondidos

Apéndice D. Análisis de cuestionarios respondidos