NORMAS GENERALES DE AUDITORIA Y ESTRUCTURAS DE ORGANIZACIÓN DE LAS EMPRESAS Y ÁREAS DEDICADAS A LA AUDITORIA

Edwin Delgado Huaynalaya
Universidad Nacional Jorge Basadre Grohmann
Tacna, Perú
E-mail edychrist@gmail.com

ABSTRACT

The article presents related information of general norms of audit and norms of internal control applied to the public sector to the field of computer science which is interpreted for their greater understanding. Also It's shown basic information about the structure of organization of companies dedicated to the audit.

Key words: Audit, Norms of Internal Control, Public Sector.

RESUMEN

El artículo presenta información de normas generales de auditoría y normas de control interno aplicadas al sector público relacionadas al campo de la informática las cuales se interpretan para su mayor entendimiento. También se muestra información básica sobre la estructura de organización de empresas dedicadas a la auditoría.

Palabras Claves: Auditoría, Normas de Control Interno, Sector Público.

NORMAS GENERALES DE AUDITORIA

La profesión de auditoría se rige, al menos en el aspecto contable y financiero, por normas y criterios aceptados generalmente, los cuales son emitidos por asociaciones de profesionales quienes aportan experiencias, conocimientos y actualizaciones en esta materia, a fin de que los practicantes de esta profesión y similares conozcan estas normas y las cumplan en el desarrollo de algún tipo de auditoría, según la profesión que practiquen.

En la actualidad existen muchas asociaciones de profesionales dedicados a la contabilidad y la ingeniería financiera. Debido a esto, en casi todos los países existe alguna asociación o colegio de contadores, los cuales tienen entre sus principales funciones regular la actuación profesional de sus agremiados. Entre estas regulaciones se encuentran las normas aplicables a la auditoría financiera y contable.

A continuación citamos las normas generales de auditoría que son emitidas por asociaciones de contadores, mismas que consideran las actividades que debe cumplir el auditor. El propósito de señalar estas normas es que nos sirvan de referencia para tomas en cuenta los aspectos fundamentales del estudio de la auditoria como disciplina y deducir como seria su aplicación en las normas de auditoria de sistemas computaciones.

Normas Generales de auditoría emitidas por el AICPA (American Institute Certified Public Accounting)

- Normas Generales
  - La auditoría debe ser realizada por personal que cuenta con la capacitación técnica adecuada y la competencia para ejercer como auditor.
  - El auditor debe conservar una actitud mental independiente en todos los aspectos.
  - El auditor debe ser diligente en la presentación de los resultados de su auditoría.
- Normas para el trabajo
  - Para que una auditoría sea eficiente y eficaz, se debe plantear y supervisar cabalmente.

- El control interno se debe entender en estructura y contenido a fin de aplicarlo en la planeación y determinación de la naturaleza, duración, extensión y profundidad de la realización de una auditoría.
- La evidencia que soporta el informe del auditor debe ser suficiente, competente y oportuna, esto se logra mediante las técnicas, métodos y procedimientos de auditoría.

- Normas de la Información
  - El informe de la auditoría debe presentarse en estricto apego a las normas de auditoría y contabilidad generalmente aceptadas.
  - En el informe de la auditoría se deben señalar las observaciones que se hayan detectado durante el periodo de evaluación, destacando aquellas desviaciones de los procedimientos normales de la operación de la empresa y de los principios generalmente aceptados.
  - Los informes de auditoría financieras deberán contener la opinión razonada del auditor. [1]

NORMAS DE CONTROL INTERNO PARA EL SECTOR PÚBLICO

Según RESOLUCION DE CONTRALORIA Nº 072-98-CG, en la Sección 500 NORMAS DE CONTROL INTERNO PARA SISTEMAS COMPUTARIZADOS, podemos ver que se dirigen a promover la eficiencia en la organización, mantenimiento y seguridad de los sistemas computarizados que procesan la información, que requieren las entidades para el desarrollo de sus actividades.

Está sección posee los siguientes contenidos:

- 500-01 Organización del área informática
  La dirección debe establecer políticas para la organización adecuada del área de Informática que permita cumplir sus actividades con eficiencia, contribuyendo al desarrollo de las operaciones de la entidad.
  La estructura básica del Área de Informática debe estar constituida por 3 áreas: **producción, desarrollo y soporte técnico**.
- 500-02 Plan de sistemas de información.
  Toda entidad que disponga de un área de informática debe implementar un plan de sistemas de información con el objeto que prever que el desarrollo de sus actividades contribuya al logro de sus objetivos institucionales.
  Debe contener por ejemplo un Diagnóstico de la Situación informática, Elaboración de objetivos y estrategias, Modelamiento de datos, Ordenamiento y priorización de datos, Programación de tiempos requeridos.
- 500-03 Controles de datos fuente, de operación y de salida.
  Deben diseñarse controles con el propósito de salvaguardar los datos fuente de origen, operaciones de proceso y salida de información, con la finalidad de preservar la integridad de la información procesada por la entidad.
  Para implementar los controles sobre datos fuente, es necesario que la entidad designe a los usuarios encargados de salvaguardar los datos. Para ello, deben establecerse políticas que definan las claves de acceso para los tres niveles: a) primer nivel: únicamente tiene opción de consulta de datos, b) segundo nivel: captura, modifica y consulta datos, c) tercer nivel: captura, modifica, consulta y además puede realizar bajas de los datos (borrar).
- 500-04 Mantenimiento de equipos de computación.
  La dirección de cada entidad debe establecer políticas respecto al mantenimiento de los equipos de computación que permitan optimizar su rendimiento.
  Existen dos clases de mantenimiento que deben considerarse: el mantenimiento correctivo y el mantenimiento preventivo.
- 500-05 Seguridad de programas, de datos y equipos de cómputo.
  Deben establecerse mecanismos de seguridad en los programas y datos del sistema para proteger la información procesada por la entidad, garantizando su integridad y exactitud, así como respecto de los equipos de computación.
  Para la seguridad lógica, los requisitos de control más importante son: a) restricciones de acceso a los archivos y programas para los programadores, analistas u operadores; b) claves acceso (password) por usuario para no violar la confidencialidad de la información; c) elaborar copias de respaldo de los datos procesados en forma diaria, semanal o mensual (backups), y descentralizada para evitar pérdida de la información; d) desarrollar un sistemas de seguridad como software de control de todas las actividades; y, e) mantener programas antivirus actualizados para evitar el deterioro de la información, según la vulnerabilidad del sistema.
  Para la seguridad física de equipos, que tiene como propósito evitar las interrupciones prolongadas del servicio de procesamiento de datos, debido a desperfectos en los equipos, accidentes, incendios y toda serie de circunstancias que haga peligrar el funcionamiento del sistema. Esta puede establecerse mediante la asignación de personal de vigilancia, disposición de alarmas, extinguidores y demás dispositivos que eviten cualquier contingencia y, la adquisición de equipos que protejan al computador principal de la ausencia de energía eléctrica.
- 500-06 Plan de contingencias.

El Área de Informática debe elaborar el Plan de Contingencias de la entidad que establezca los procedimientos a utilizarse para evitar interrupciones en la operación del sistema de cómputo.
La aplicación del plan permite operar en un nivel aceptable cuando las facilidades de procesamiento de información no están disponibles.

- 500-07 Aplicación de técnicas de Intranet.
  La implementación de las técnicas de INTRANET dentro de las entidades debe efectuarse con el objeto de fortalecer el control interno e incrementar la eficiencia de las comunicaciones internas, previa evaluación del costo-beneficio que reportaría su aplicación.
  Dentro de las pautas más importantes para iniciar un Intranet puede referirse: a) instalación del protocolo de comunicaciones TCP/IP; b) escoger un servidor comercial que ofrezca funcionalidades de empaquetado, seguridad y enlaces a la base de datos corporativa; c) organización de la información mediante reuniones con los ejecutivos de más alto rango, determinando que información estará en Intranet; d) familiarizarse con el software de manipulación de la información que es utilizada en Internet; y e) conectarse a una base de datos, con la finalidad de organizar mejor la documentación existente en el Servidor Web.
- 500-08 Gestión óptima de software adquirido a medida por entidades públicas.
  Debe establecerse políticas sobre el software a medida adquirido por las entidades, a fin de que los derechos de propiedad se registren a nombre del Estado. [2]

NORMAS DE CONTROL INTERNO PARA EL SECTOR PÚBLICO Y PRIVADO

El Control Interno al Servicio de Informática debe contemplar:

- LA ORGANIZACIÓN.
  Se deber verificar que por un concepto de integralidad, existan funciones claramente definidas que obligatoriamente deben efectuarse y que existan grupos de trabajo diferenciados, que permita delimitar responsabilidades y dinamizar la gestión de informática. Las funciones que deben existir son:
  - Desarrollo de Sistemas.
  - Operación de Sistemas.
  - Mantenimiento de Sistemas.
  - Soporte Técnico.
  - Soporte a equipos.
  - Control de Sistemas.

- EVALUACION FUNCIONAL.
  Desarrollo de Sistemas
  Operación de Sistemas
  . El proceso normal.
  . Mensajes de advertencia y error.
  . Recomendaciones para la solución a los mensajes presentados.
  . Puntos de reinicio.
  . Comunicación de Problemas.
  Mantenimiento de Sistemas
  Soporte Técnico
  Soporte a Equipos de Cómputo
  Debe existir Registros de:
  Equipos existentes, Softwares instalados en cada equipo, Mantenimientos realizados a cada equipo firmados por el proveedor, soporte técnico y usuario.
  Control de Sistemas

- LOS PROCEDIMIENTOS GENERALES.
  Las normas que deberían disponer son :
  . Norma de Análisis de Sistemas.
  . Norma de Diseño de Sistemas.
  . Norma de Programación de Sistemas.
  . Norma de Implantación de Sistemas.
  . Norma de Operación de Sistemas.
  . Norma de Mantenimiento de Sistemas.
  . Norma de Control de Sistemas.

Los procedimientos que debieran estar disponibles son:
. Procedimientos de Operación de todos los Sistemas.
. Procedimiento General de Seguridad.
. Procedimiento General de Respaldo de la Información.
. Procedimientos ante Contingencias.
. Procedimientos de Administración de Bibliotecas de Software.

- Metodologías Utilizadas (Una podría ser).
  Planeamiento de Sistema
  Análisis de Sistemas:
  - Entrevistas.
  - Diagrama de Flujo de Datos (D.F.D.).
  - Modelización de Datos.
  - Diagrama de Estructura de Datos (D.E.D.).
  - Historia de Vida de la Entidad (H.E.V.).
  - Análisis de Costo-Beneficio (A.C.B.).
  - Prototipeo.

  Diseño de Sistemas:
  - Diseño Estructurado.
  - Diagrama de Estructura de Cuadros.
  - Optimización del Diseño Físico.
  - Diseño de Pruebas.
  - Prototipeo.

  Programación:
  - Programación Estructurada.
  - Pruebas Unitarias.
  - Pruebas de Integración.
  - Prueba del Sistema.

  Implantación de Sistemas:
  - Capacitación.
  - Creación de archivos iniciales.
  - Proceso en paralelo.

- Recursos Humanos.
  Debe evaluarse que la formación y experiencia de los recursos humanos, asignados a cada área para el desempeño de sus funciones, sean las adecuadas.
  Se debe analizar también el balance de la cantidad de recursos humanos por área, de tal forma que no existan desequilibrios que afecten el desempeño del Servicio Informático en su conjunto.
  Debe analizarse si los tiempos utilizados para la obtención de resultados en cada uno de los tipos de actividades son los adecuados y se efectúan dentro de los plazos razonables.

- Seguridad.
  Debe comprobarse que el área de Servicios Informáticos cuente con los siguientes tipos de seguridad:
  - Seguridad en el acceso a la información.
  - Seguridad de los Sistemas.
  - Seguridades Físicas. [3]

ESTRUCTURAS DE ORGANIZACIÓN DE LAS EMPRESAS Y ÁREAS DEDICADAS A LA AUDITORIA

1) Estructura de organización de las empresas dedicadas a la auditoría externa

- Grandes empresas dedicadas a la auditoría
  - Director o gerente general
  - Funcionarios de cuenta
  - Gerentes o jefes de departamento o de área de atención
  - Supervisores de auditoría
  - Jefes de grupo o responsables de auditoría
  - Auditores asignados
  - Apoyo administrativo y secretarial
- Despachos o empresas medianas dedicadas a la auditoría
  - Gerente de auditoría
  - Encargado de auditoría
  - Auditores Junior
  - Apoyo Secretarial
- Pequeños despachos o auditores independientes
  - Auditor Senior
  - Auditor Junior
  - Apoyo secretarial

2) Estructura de organización de las áreas de auditoría interna

- Para auditorías internas de macroempresas y empresas grandes
  - Director o gerente al nivel de área funcional
  - Gerentes o jefes de departamento, de área o de función a auditar.
  - Jefes de grupo o encargados
  - Auditores internos
  - Apoyo administrativo y secretarial
- Para auditorías internas de empresas medianas
  - Gerente de auditoría
  - Auditor Senior
  - Auditores Junior
  - Apoyo Secretarial
- Para auditorías internas de empresas pequeñas y microempresas
  - Auditor Senior
  - Auditor Junior
  - Apoyo secretarial [1]

BIBLIOGRAFÍA

[1] Auditoría en Sistemas Computacionales. pp 43 – 44, 48 - 50
[2] Oficina Nacional de Gobierno Electrónico e Informática. RESOLUCION DE CONTRALORIA Nº 072-98-CG. Disponible: http://www.pcm.gob.pe/portal_ongei/Banco_Normas/normasNAGU.pdf
[3] Instituto Nacional de Estadística e Informática. Auditoría de Sistemas. Control Interno del Servicio Informática. Disponible: http://www.inei.gob.pe/biblioineipub/bancopub/Inf/Lib5002/DOC5.htm