CAPITULO V

V. EVALUACIÓN DEL PROCESO DE DATOS Y DE LOS EQUIPOS DE CÓMPUTO

Introducción

Los datos son uno de los recursos mas valiosos de las organizaciones y, aunque son intangibles, necesitan ser controlados y auditados con el mismo cuidado que los demás inventarios de la organización, por lo cual se debe tener presente:

a) La responsabilidad de los datos es compartida conjuntamente por alguna función determinada de la organización y la dirección de informática.
b) Un problema que se debe considerar es el que se origina por la duplicidad de los datos y consiste en poder determinar los propietarios o usuarios posibles (principalmente en el caso de redes y banco de datos) y la responsabilidad de su actualización y consistencia.
c) Los datos deberán tener una clasificación estándar y un mecanismo de identificación que permita detectar duplicidad y redundancia dentro de una aplicación y de todas las aplicaciones en general.
d) Se deben relacionar los elementos de los datos con las bases de datos donde están
e) almacenados, así como los reportes y grupos de procesos donde son generados.

La mayoría de los delitos por computadora son cometidos por modificaciones de datos fuente al:

- Suprimir u omitir datos
- Adicionar datos
- Alterar datos
- Duplicar procesos

Esto es de suma importancia en caso de equipos de cómputo que cuentan con sistemas en línea, en los que los usuarios son los responsables de la captura y modificación de la información al tener un adecuado control con señalamiento de responsables de los datos (uno de los usuarios debe ser el único responsable de determinado dato), con claves de acceso de acuerdo a niveles.

El primer nivel es el que puede hacer únicamente consultas. El segundo nivel es aquel que puede hacer captura, modificaciones y consultas y el tercer nivel es el que sólo puede hacer todo 10 anterior y además puede realizar bajas.

Por lo expuesto anteriormente las lecturas seleccionadas abordan los tópicos más relevantes acerca del proceso de datos y los equipos de cómputo que expone Oscar toro.

V.1 Controles

Fuente: http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml

Revisión de Controles de la Gestión Informática:

Una vez conseguida la Operatividad de los Sistemas, el segundo objetivo de la auditoría es la verificación de la observancia de las normas teóricamente existentes en el departamento de Informática y su coherencia con las del resto de la empresa. Para ello, habrán de revisarse sucesivamente y en este orden:

1. Las Normas Generales de la Instalación Informática. Se realizará una revisión inicial sin estudiar a fondo las contradicciones que pudieran existir, pero registrando las áreas que carezcan de normativa, y sobre todo verificando que esta Normativa General Informática no está en contradicción con alguna Norma General no informática de la empresa.

2. Los Procedimientos Generales Informáticos. Se verificará su existencia, al menos en los sectores más importantes. Por ejemplo, la recepción definitiva de las máquinas debería estar firmada por los responsables de Explotación. Tampoco el alta de una nueva Aplicación podría producirse si no existieran los Procedimientos de Backup y Recuperación correspondientes.

3. Los Procedimientos Específicos Informáticos. Igualmente, se revisara su existencia en las áreas fundamentales. Así, Explotación no debería explotar una Aplicación sin haber exigido a Desarrollo la pertinente documentación. Del mismo modo, deberá comprobarse que los Procedimientos Específicos no se opongan a los Procedimientos Generales. En todos los casos anteriores, a su vez, deberá verificarse que no existe contradicción alguna con la Normativa y los Procedimientos Generales de la propia empresa, a los que la Informática debe estar sometida.

Auditoría informática de explotación:

La Explotación Informática se ocupa de producir resultados informáticos de todo tipo: listados impresos, ficheros soportados magnéticamente para otros informáticos, ordenes automatizadas para lanzar o modificar procesos industriales, etc. La explotación informática se puede considerar como una fabrica con ciertas peculiaridades que la distinguen de las reales. Para realizar la Explotación Informática se dispone de una materia prima, los Datos, que es necesario transformar, y que se someten previamente a controles de integridad y calidad. La transformación se realiza por medio del Proceso informático, el cual está gobernado por programas. Obtenido el producto final, los resultados son sometidos a varios controles de calidad y, finalmente, son distribuidos al cliente, al usuario.

Auditar Explotación consiste en auditar las secciones que la componen y sus interrelaciones. La Explotación Informática se divide en tres grandes áreas: Planificación, Producción y Soporte Técnico, en la que cada cual tiene varios grupos.

<u>Control de Entrada de Datos:</u>

Se analizará la captura de la información en soporte compatible con los Sistemas, el cumplimiento de plazos y calendarios de tratamientos y entrega de datos; la correcta transmisión de datos entre entornos diferentes. Se verificará que los controles de integridad y calidad de datos se realizan de acuerdo a Norma.

Planificación y Recepción de Aplicaciones:

Se auditarán las normas de entrega de Aplicaciones por parte de Desarrollo, verificando su cumplimiento y su calidad de interlocutor único. Deberán realizarse muestreos selectivos de la Documentación de las Aplicaciones explotadas. Se inquirirá sobre la anticipación de contactos con Desarrollo para la planificación a medio y largo plazo.

Centro de Control y Seguimiento de Trabajos:

Se analizará cómo se prepara, se lanza y se sigue la producción diaria. Básicamente, la explotación Informática ejecuta procesos por cadenas o lotes sucesivos (Batch*), o en tiempo real (Tiempo Real*). Mientras que las Aplicaciones de Teleproceso están permanentemente activas y la función de Explotación se limita a vigilar y recuperar incidencias, el trabajo Batch absorbe una buena parte de los efectivos de Explotación. En muchos Centros de Proceso de Datos, éste órgano recibe el nombre de Centro de Control de Batch. Este grupo determina el éxito de la explotación, en cuanto que es uno de los factores más importantes en el mantenimiento de la producción.

*Batch y Tiempo Real:

Las Aplicaciones que son Batch son Aplicaciones que cargan mucha información durante el día y durante la noche se corre un proceso enorme que lo que hace es relacionar toda la información, calcular cosas y obtener como salida, por ejemplo, reportes. O sea, recolecta información durante el día, pero todavía no procesa nada. Es solamente un tema de "Data Entry" que recolecta información, corre el proceso Batch (por lotes), y calcula todo lo necesario para arrancar al día siguiente.

Las Aplicaciones que son Tiempo Real u Online, son las que, luego de haber ingresado la información correspondiente, inmediatamente procesan y devuelven un resultado. Son Sistemas que tienen que responder en Tiempo Real.

Operación. Salas de Ordenadores:

Se intentarán analizar las relaciones personales y la coherencia de cargos y salarios, así como la equidad en la asignación de turnos de trabajo. Se verificará la existencia de un responsable de Sala en cada turno de trabajo. Se analizará el grado de automatización de comandos, se verificara la existencia y grado de uso de los Manuales de Operación. Se analizará no solo la existencia de planes de formación, sino el cumplimiento de los mismos y el tiempo transcurrido para cada Operador desde el último Curso recibido. Se estudiarán los montajes diarios y por horas de cintas o cartuchos, así como los tiempos transcurridos entre la petición de montaje por parte del Sistema hasta el montaje real. Se verificarán las líneas de papel impresas diarias y por horas, así como la manipulación de papel que comportan.

Centro de Control de Red y Centro de Diagnosis:

El Centro de Control de Red suele ubicarse en el área de producción de Explotación. Sus funciones se refieren exclusivamente al ámbito de las Comunicaciones, estando muy relacionado con la organización de Software de Comunicaciones de Técnicas de Sistemas. Debe analizarse la fluidez de esa relación y el grado de coordinación entre ambos. Se verificará la existencia de un punto focal único, desde el cual sean perceptibles todas las líneas asociadas al Sistema. El Centro de Diagnosis es el ente en donde se atienden las llamadas de los usuarios-clientes que han sufrido averías o incidencias, tanto de Software como de Hardware. El Centro de Diagnosis está

especialmente indicado para informáticos grandes y con usuarios dispersos en un amplio territorio. Es uno de los elementos que más contribuyen a configurar la imagen de la Informática de la empresa. Debe ser auditada desde esta perspectiva, desde la sensibilidad del usuario sobre el servicio que se le dispone. No basta con comprobar la eficiencia técnica del Centro, es necesario analizarlo simultáneamente en el ámbito de Usuario.

V.2 Control de diseño de sistemas y programación

Fuente: (http://www.itapizaco.edu.mx/paginas/maudisist.html) Toro Oscar.

El objetivo es asegurarse de que el sistema funcione conforme a las especificaciones funcionales, a fin de que el usuario tenga la suficiente información para su manejo, operación y aceptación. Las revisiones se efectúan en forma paralela desde el análisis hasta la programación y sus objetivos son los siguientes:

ETAPA DE ANÁLISIS: Identificar inexactitudes, ambigüedades y omisiones en las especificaciones.

ETAPA DE DISEÑO: Descubrir errores, debilidades, omisiones antes de iniciar la codificación.

ETAPA DE PROGRAMACIÓN: Buscar la claridad, modularidad y verificar con base en las especificaciones.

Esta actividad es muy importante ya que el costo de corregir errores es directamente proporcional al momento que se detectan: si se, descubren en el, momento de programación será más alto que si se detecta en la etapa de análisis. Esta función tiene una gran importancia en el ciclo de evaluación de aplicaciones de los sistemas de información y busca comprobar que la aplicación cumple las especificaciones del usuario, que se haya desarrollado dentro de lo presupuestado, que tenga los controles necesarios y que efectivamente cumpla con los objetivos y beneficios esperados.

Difícilmente se controla realmente el flujo de la información de un sistema que desde su inicio ha sido mal analizado, mal diseñado, mal programado e incluso mal documentado. El excesivo mantenimiento de los sistemas generalmente ocasionado por un mal desarrollo, se inicia desde que el usuario establece sus requerimientos (en ocasiones sin saber qué desea) hasta la instalación del mismo, sin que se haya establecido un plan de prueba del sistema para medir su grado de confiabilidad en la operación que efectuará. Para verificar si existe esta situación, se debe pedir a los analistas y a los programadores las actividades que están desarrollando en el momento de la auditoría y evaluar si están efectuando actividades de mantenimiento o de realización de nuevos proyectos. En ambos casos se deberá evaluar el tiempo que llevan dentro del mismo sistema, la prioridad que se le asignó y cómo está en el tiempo real en relación al tiempo estimado en el plan maestro.

Instructivos de operación

Se debe evaluar los instructivos de operación de los sistemas para evitar que los programadores tengan acceso a los sistemas en operación, y el contenido mínimo de los instructivos de operación se puedan verificar mediante el siguiente cuestionario.

El instructivo de operación deberá comprender:
- Diagrama de flujo por cada programa. ( )
- Diagrama particular de entrada/salida ( )
- Mensaje y su explicación ( )
- Parámetros y su explicación ( )
- Diseño de impresión de resultados ( )
- Cifras de control ( )
- Fórmulas de verificación ( )
- Observaciones ( )
- Instrucciones en caso de error ( )
- Calendario de proceso y resultados ( )

Forma de implementación

La finalidad de evaluar los trabajos que se realizan para iniciar la operación de un sistema, esto es, la prueba integral del sistema, adecuación, aceptación por parte del usuario, entrenamiento de los responsables del sistema etc.

Indicar cuáles puntos se toman en cuenta para la prueba de un sistema:
Prueba particular de cada programa ( )
Prueba por fase validación, actualización ( )
Prueba integral del paralelo ( )
Prueba en paralelo sistema ( )
Otros (especificar)_____

V.3 Entrevistas a usuarios

La entrevista se deberá llevar a cabo para comprobar datos proporcionados y la situación de la dependencia en el departamento de Sistemas de Información.

Su objeto es conocer la opinión que tienen los usuarios sobre los servicios proporcionados, así como la difusión de las aplicaciones de la computadora y de los sistemas en operación.

Las entrevistas se deberán hacer, en caso de ser posible, a todos los usuarios o bien en forma aleatoria a algunos de los usuarios, tanto de los más importantes como de los de menor importancia, en cuanto al uso del equipo.

Desde el punto de vista del usuario los sistemas deben:

Cumplir con los requerimientos totales del usuario.
Cubrir todos los controles necesarios.
No exceder las estimaciones del presupuesto inicial.
Serán fácilmente modificables.

Para que un sistema cumpla con los requerimientos del usuario, se necesita una comunicación completa entre usuarios y responsable del desarrollo del sistema.

En esta misma etapa debió haberse definido la calidad de la información que será procesada por la computadora, estableciéndose los riesgos de la misma y la forma de

minimizarlos. Para ello se debieron definir los controles adecuados, estableciéndose además los niveles de acceso a la información, es decir, quién tiene privilegios de consulta, modificar o incluso borrar información.

Esta etapa habrá de ser cuidadosamente verificada por el auditor interno especialista en sistemas y por el auditor en informática, para comprobar que se logro una adecuada comprensión de los requerimientos del usuario y un control satisfactorio de información.

Para verificar si los servicios que se proporcionan a los usuarios son los requeridos y se están proporcionando en forma adecuada, cuando menos será preciso considerar la siguiente información.

- Descripción de los servicios prestados.
- Criterios de evaluación que utilizan los usuarios para evaluar el nivel del servicio prestado.
- Reporte periódico del uso y concepto del usuario sobre el servicio.
- Registro de los requerimientos planteados por el usuario.

Controles

Los datos son uno de los recursos más valiosos de las organizaciones y, aunque son intangibles, necesitan ser controlados y auditados con el mismo cuidado que los demás inventarios de la organización, por lo cual se debe tener presente:

a) La responsabilidad de los datos es compartida conjuntamente por alguna función determinada y el departamento de cómputo.

b) Un problema de dependencia que se debe considerar es el que se origina por la duplicidad de los datos y consiste en poder determinar los propietarios o usuarios posibles(principalmente en el caso de redes y banco de datos) y la responsabilidad de su actualización y consistencia.

c) Los datos deberán tener una clasificación estándar y un mecanismo de identificación que permita detectar duplicidad y redundancia dentro de una aplicación y de todas las aplicaciones en general.

d) Se deben relacionar los elementos de los datos con las bases de datos donde están almacenados, así como los reportes y grupos de procesos donde son generados.

V.4 Control de los datos fuente y manejo de cifras de control

La mayoría de los Delitos por computadora son cometidos por modificaciones de datos fuente al:

- Suprimir u omitir datos.
- Adicionar Datos.
- Alterar datos.
- Duplicar procesos.

Esto es de suma importancia en caso de equipos de cómputo que cuentan con sistemas en línea, en los que los usuarios son los responsables de la captura y modificación de la información al tener un adecuado control con señalamiento de responsables de los datos (uno de los usuarios debe ser el único responsable de determinado dato), con claves de acceso de acuerdo a niveles.

El primer nivel es el que puede hacer únicamente consultas. El segundo nivel es aquel que puede hacer captura, modificaciones y consultas y el tercer nivel es el que solo puede hacer todos lo anterior y además puede realizar bajas.

Los dispositivos de almacenamiento representan, para cualquier centro de cómputo, archivos extremadamente importantes cuya pérdida parcial o total podría tener repercusiones muy serias, no sólo en la unidad de informática, sino en la dependencia de la cual se presta servicio. Una dirección de informática bien administrada debe tener perfectamente protegidos estos dispositivos de almacenamiento, además de mantener registros sistemáticos de la utilización de estos archivos, de modo que servirán de base a registros sistemáticos de la utilización de estos archivos, de modo que sirvan de base a los programas de limpieza (borrado de información), principalmente en el caso de las cintas.

Además se deben tener perfectamente identificados los carretes para reducir la posibilidad de utilización errónea o destrucción de la información.

Un manejo adecuado de estos dispositivos permitirá una operación más eficiente y segura, mejorando además los tiempos de procesos.

V.5 Control de mantenimiento

Fuente: (http://html.rincondelvago.com/auditoria-computacional.html)

Como se sabe existen básicamente tres tipos de contrato de mantenimiento: El contrato de mantenimiento total que incluye el mantenimiento correctivo y preventivo, el cual a su vez puede dividirse en aquel que incluye las partes dentro del contrato y el que no incluye partes. El contrato que incluye refacciones es propiamente como un seguro, ya que en caso de descompostura el proveedor debe proporcionar las partes sin costo alguno. Este tipo de contrato es normalmente más caro, pero se deja al proveedor la responsabilidad total del mantenimiento a excepción de daños por negligencia en la utilización del equipo. (Este tipo de mantenimiento normalmente se emplea en equipos grandes).

El segundo tipo de mantenimiento es "por llamada", en el cual en caso de descompostura se le llama al proveedor y éste cobra de acuerdo a una tarifa y al tiempo que se requiera para componerlo (casi todos los proveedores incluyen, en la cotización de compostura, el tiempo de traslado de su oficina a donde se encuentre el equipo y viceversa). Este tipo de mantenimiento no incluye refacciones.

El tercer tipo de mantenimiento es el que se conoce como "en banco", y es aquel en el cual el cliente lleva a las oficinas del proveedor el equipo, y este hace una cotización de acuerdo con el tiempo necesario para su compostura mas las refacciones (este tipo de mantenimiento puede ser el adecuado para computadoras personales).

Al evaluar el mantenimiento se debe primero analizar cual de los tres tipos es el que más nos conviene y en segundo lugar pedir los contratos y revisar con detalles que las cláusulas estén perfectamente definidas en las cuales se elimine toda la subjetividad y con penalización en caso de incumplimiento, para evitar contratos que sean parciales.

Para poder exigirle el cumplimiento del contrato de debe tener un estricto control sobre las fallas, frecuencia, y el tiempo de reparación.

V.6 Control de proyectos

Debido a las características propias del análisis y la programación, es muy frecuente que la implantación de los sistemas se retrase y se llegue a suceder que una persona lleva trabajando varios años dentro de un sistema o bien que se presenten irregularidades en las que los programadores se ponen a realizar actividades ajenas a la dirección de informática. Para poder controlar el avance de los sistemas, ya que ésta es una actividad de difícil evaluación, se recomienda que se utilice la técnica de administración por proyectos para su adecuado control.

Para tener una buena administración por proyectos se requiere que el analista o el programado y su jefe inmediato elaboren un plan de trabajo en el cual se especifiquen actividades, metas, personal participante y tiempos. Este plan debe de ser revisado periódicamente (semanal, mensual, etc.) para evaluar el avance respecto a lo programado. La estructura estándar de la planeación de proyectos deberá incluir la facilidad de asignar fechas predefinidas de terminación de cada tarea. Dentro de estas fechas debe de estar el calendario de reuniones de revisión, las cuales tendrán diferentes niveles de detalles

V.7 Evaluación y configuración del sistema de cómputo

Fuente: http//www.ilustrados.com/publicaciones/EpuppFZZkpIJTHHuCg.php.

Evaluación de sistemas

La elaboración de sistemas debe ser evaluada con mucho detalle, para lo cual se debe revisar si existen realmente sistemas entrelazados como un todo o bien si existen programas aislados. Otro de los factores a evaluar es si existe un plan estratégico para la elaboración de los sistemas o si se están elaborados sin el adecuado señalamiento de prioridades y de objetivos.

El plan estratégico deberá establecer los servicios que se presentarán en un futuro contestando preguntas como las siguientes:

- ¿Cuáles servicios se implementarán?
- ¿Cuándo se pondrán a disposición de los usuarios?
- ¿Qué características tendrán?
- ¿Cuántos recursos se requerirán?

La estrategia de desarrollo deberé establecer las nuevas aplicaciones, recursos y la arquitectura en que estarán fundamentados:

- ¿Qué aplicaciones serán desarrolladas y cuando?
- ¿Qué tipo de archivos se utilizarán y cuando?
- ¿Qué bases de datos se utilizarán y cuando?
- ¿Qué lenguajes se utilizarán y en que software?
- ¿Qué tecnología será utilizada y cuando se implementará?
- ¿Cuantos recursos se requerirán aproximadamente?
- ¿Cuál es aproximadamente el monto de la inversión en hardware y software?

En lo referente a la consulta a los usuarios, el plan estratégico debe definir los requerimientos de información de la dependencia.

- ¿Qué estudios van a ser realizados al respecto?

- ¿Qué metodología se utilizará para dichos estudios?
- ¿Quién administrará y realizará dichos estudios?

En el área de auditoría interna debe evaluarse cuál ha sido la participación del auditor y los controles establecidos.

Por último, el plan estratégico determina la planeación de los recursos.

- ¿Contempla el plan estratégico las ventajas de la nueva tecnología?
- ¿Cuál es la inversión requerida en servicios, desarrollo y consulta a los usuarios?

El proceso de planeación de sistemas deberá asegurarse deque todos los recursos requeridos estén claramente identificados en el plan de desarrollo de aplicaciones y datos. Estos recursos (hardware, software y comunicaciones) deberán ser compatibles con la arquitectura y la tecnología, con que se cuenta actualmente.

Los sistemas deben evaluarse de acuerdo con el ciclo de vida que normalmente siguen: requerimientos del usuario, estudio de factibilidad, diseño general, análisis, diseño lógico, desarrollo físico, pruebas, implementación, evaluación, modificaciones, instalación, mejoras. Y se vuelve nuevamente al ciclo inicial, el cual a su vez debe comenzar con el de factibilidad.

La primera etapa a evaluar del sistema es el estudio de factibilidad, el cual debe analizar si el sistema es factible de realizarse, cuáles su relación costo/beneficio y si es recomendable elaborarlo.

Se deberá solicitar el estudio de factibilidad de los diferentes sistemas que se encuentren en operación, así como los que estén en la fase de análisis para evaluar si se considera la disponibilidad y características del equipo, los sistemas operativos y lenguajes disponibles, la necesidad de los usuarios, las formas de utilización de los sistemas, el costo y los beneficios que reportará el sistema, el efecto que producirá en quienes lo usarán y el efecto que éstos tendrán sobre el sistema y la congruencia de los diferentes sistemas.

En el caso de sistemas que estén funcionando, se deberá comprobar si existe el estudio de factibilidad con los puntos señalados y compararse con la realidad con lo especificado en el estudio de factibilidad.

Por ejemplo en un sistema que el estudio de factibilidad señaló determinado costo y una serie de beneficios de acuerdo con las necesidades del usuario, debemos comparar cual fue su costo real y evaluar si se satisficieron las necesidades indicadas como beneficios del sistema.

Para investigar el costo de un sistema se debe considerar, con una exactitud razonable, el costo de los programas, el uso de los equipos (compilaciones, programas, pruebas, paralelos), tiempo, personal y operación, cosa que en la práctica son costos directos. indirectos y de operación.

Los beneficios que justifiquen el desarrollo de un sistema pueden ser el ahorro en los costos de operación, la reducción del tiempo de proceso de un sistema. Mayor exactitud, mejor servicio, una mejoría en los procedimientos de control, mayor confiabilidad y seguridad.

Bibliografía Capitulo V

05/11/1999. “Auditoría Informática”.
http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml

Toro Oscar. 04/08/2003. “Manual de auditoría de sistemas”.
http://www.itapizaco.edu.mx/paginas/maudisist.html

Inter. Electric Limitada. Ingeniería en ejecución informática de gestión “auditoria computacional”.
http://html.rincondelvago.com/auditoria-computacional.html

http://www.ilustrados.com/publicaciones/EpuppFZZkpIJTHHuCg.php.