

MANUAL DE AUDITORIA DE SISTEMAS

Indice de Temas

AUDITORIA DE SISTEMAS	4
PLANEACIÓN DE LA AUDITORÍA EN INFORMÁTICA	4
INVESTIGACIÓN PRELIMINAR.....	5
ADMINISTRACIÓN	5
SISTEMAS.....	6
PERSONAL PARTICIPANTE	8
EVALUACIÓN DE SISTEMAS.....	9
EVALUACIÓN DEL ANÁLISIS.....	12
EVALUACIÓN DEL DISEÑO LÓGICO DEL SISTEMA	14
EVALUACIÓN DEL DESARROLLO DEL SISTEMA.....	17
CONTROL DE PROYECTOS.....	18
CUESTIONARIO.....	19
CONTROL DE DISEÑO DE SISTEMAS Y PROGRAMACIÓN.....	20
INSTRUCTIVOS DE OPERACIÓN	24
FORMA DE IMPLEMENTACIÓN	24
ENTREVISTA A USUARIOS	25
CONTROLES.....	29
CONTROL DE LOS DATOS FUENTE Y MANEJO CIFRAS DE CONTROL	30

CONTROL DE OPERACIÓN.....	34
CONTROLES DE SALIDA	40
CONTROL DE MEDIOS DE ALMACENAMIENTO MASIVO.....	40
CONTROL DE ALMACENAMIENTO MASIVO	
.....	41
OBJETIVOS.....	41
CONTROL DE MANTENIMIENTO	46
ORDEN EN EL CENTRO DE CÓMPUTO	48
EVALUACIÓN DE LA CONFIGURACIÓN DEL SISTEMA DE CÓMPUTO	49
SEGURIDAD LÓGICA Y CONFIDENCIAL	51
SEGURIDAD FÍSICA	55
SEGURIDAD EN LA UTILIZACIÓN DEL EQUIPO.....	65
SEGURIDAD AL RESTAURAR EL EQUIPO	67
PROCEDIMIENTOS DE RESPALDO EN CASO DE DESASTRE	70
ANEXO 1.....	74
ANEXO 2.....	75

AUDITORIA DE SISTEMAS

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

La auditoría en informática deberá comprender no sólo la evaluación de los equipos de cómputo, de un sistema o procedimiento específico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.

La auditoría en informática es de vital importancia para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad. Además debe evaluar todo (informática, organización de centros de información, hardware y software).

PLANEACIÓN DE LA AUDITORÍA EN INFORMÁTICA

Para hacer una adecuada planeación de la auditoría en informática, hay que seguir una serie de pasos previos que permitirán dimensionar el tamaño y características de área dentro del organismo a auditar, sus sistemas, organización y equipo.

En el caso de la auditoría en informática, la planeación es fundamental, pues habrá que hacerla desde el punto de vista de los dos objetivos:

Evaluación de los sistemas y procedimientos.

Evaluación de los equipos de cómputo.

Para hacer una planeación eficaz, lo primero que se requiere es obtener información general sobre la organización y sobre la función de informática a evaluar. Para ello es preciso hacer una investigación preliminar y algunas entrevistas previas, con base en esto planear el programa de trabajo, el cual deberá incluir tiempo, costo, personal necesario y documentos auxiliares a solicitar o formular durante el desarrollo de la misma.

INVESTIGACIÓN PRELIMINAR

Se deberá observar el estado general del área, su situación dentro de la organización, si existe la información solicitada, si es o no necesaria y la fecha de su última actualización.

Se debe hacer la investigación preliminar solicitando y revisando la información de cada una de las áreas basándose en los siguientes puntos:

ADMINISTRACIÓN

Se recopila la información para obtener una visión general del departamento por medio de observaciones, entrevistas preliminares y solicitud de documentos para poder definir el objetivo y alcances del departamento.

PARA ANALIZAR Y DIMENSIONAR LA ESTRUCTURA POR AUDITAR SE DEBE SOLICITAR:

A NIVEL DEL ÁREA DE INFORMÁTICA

Objetivos a corto y largo plazo.

RECURSOS MATERIALES Y TECNICOS

Solicitar documentos sobre los equipos, número de ellos, localización y características.

Estudios de viabilidad.

Número de equipos, localización y las características (de los equipos instalados y por instalar y programados)

Fechas de instalación de los equipos y planes de instalación.

Contratos vigentes de compra, renta y servicio de mantenimiento.

Contratos de seguros.

Convenios que se tienen con otras instalaciones.

Configuración de los equipos y capacidades actuales y máximas.

Planes de expansión.

Ubicación general de los equipos.

Políticas de operación.

Políticas de uso de los equipos.

SISTEMAS

Descripción general de los sistemas instalados y de los que estén por instalarse que contengan volúmenes de información.

Manual de formas.

Manual de procedimientos de los sistemas.

Descripción genérica.

Diagramas de entrada, archivos, salida.

Salidas.

Fecha de instalación de los sistemas.

Proyecto de instalación de nuevos sistemas.

En el momento de hacer la planeación de la auditoría o bien su realización, debemos evaluar que pueden presentarse las siguientes situaciones.

Se solicita la información y se ve que:

No tiene y se necesita.

No se tiene y no se necesita.

Se tiene la información pero:

No se usa.

Es incompleta.

No esta actualizada.

No es la adecuada.

Se usa, está actualizada, es la adecuada y está completa.

En el caso de No se tiene y no se necesita, se debe evaluar la causa por la que no es necesaria. En el caso de No se tiene pero es necesaria, se debe recomendar que se elabore de acuerdo con las necesidades y con el uso que se le va a dar. En el caso de que se tenga la información pero no se utilice, se debe analizar por que no se usa. En caso de que se tenga la información, se debe analizar si se usa, si está actualizada, si es la adecuada y si está completa.

El éxito del análisis crítico depende de las consideraciones siguientes:

Estudiar hechos y no opiniones (no se toman en cuenta los rumores ni la información sin fundamento)

Investigar las causas, no los efectos.

Atender razones, no excusas.

No confiar en la memoria, preguntar constantemente.

Criticar objetivamente y a fondo todos los informes y los datos recabados.

PERSONAL PARTICIPANTE

Una de las partes más importantes dentro de la planeación de la auditoría en informática es el personal que deberá participar y sus características.

Uno de los esquemas generalmente aceptados para tener un adecuado control es que el personal que intervengan esté debidamente capacitado, con alto sentido de moralidad, al cual se le exija la optimización de recursos (eficiencia) y se le retribuya o compense justamente por su trabajo.

Con estas bases se debe considerar las características de conocimientos, práctica profesional y capacitación que debe tener el personal que intervendrá en la auditoría. En primer lugar se debe pensar que hay personal asignado por la organización, con el suficiente nivel para poder coordinar el desarrollo de la auditoría, proporcionar toda la información que se solicite y programar las reuniones y entrevistas requeridas.

Éste es un punto muy importante ya que, de no tener el apoyo de la alta dirección, ni contar con un grupo multidisciplinario en el cual estén presentes una o varias personas del área a auditar, sería casi imposible obtener información en el momento y con las características deseadas.

También se debe contar con personas asignadas por los usuarios para que en el momento que se solicite información o bien se efectúe alguna entrevista de comprobación de hipótesis, nos proporcionen aquello que se está solicitando, y complementen el grupo multidisciplinario, ya que se debe analizar no sólo el punto de vista de la dirección de informática, sino también el del usuario del sistema.

Para completar el grupo, como colaboradores directos en la realización de la auditoría se deben tener personas con las siguientes características:

Técnico en informática.

Experiencia en el área de informática.

Experiencia en operación y análisis de sistemas.

Conocimientos de los sistemas más importantes.

En caso de sistemas complejos se deberá contar con personal con conocimientos y experiencia en áreas específicas como base de datos, redes, etc. Lo anterior no significa que una sola persona tenga los conocimientos y experiencias señaladas, pero si deben intervenir una o varias personas con las características apuntadas.

Una vez que se ha hecho la planeación, se puede utilizar el formato señalado en el anexo 1, el figura el organismo, las fases y subfases que comprenden la descripción de la actividad, el número de personas participantes, las fechas estimadas de inicio y terminación, el número de días hábiles y el número de días/hombre estimado. El control del avance de la auditoría lo podemos llevar mediante el anexo 2, el cual nos permite cumplir con los procedimientos de control y asegurarnos que el trabajo se está llevando a cabo de acuerdo con el programa de auditoría, con los recursos estimados y en el tiempo señalado en la planeación.

El hecho de contar con la información del avance nos permite revisar el trabajo elaborado por cualquiera de los asistentes. Como ejemplo de propuesta de auditoría en informática véase el anexo 3.

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 deberá 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 serán utilizarán y cuando?

¿Qué lenguajes se utilizarán y en que software?

¿Qué tecnología será utilizada y cuando se implementará?

¿Cuántos 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 de que 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, cuál es 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.

EVALUACIÓN DEL ANÁLISIS

En esta etapa se evaluarán las políticas, procedimientos y normas que se tienen para llevar a cabo el análisis.

Se deberá evaluar la planeación de las aplicaciones que pueden provenir de tres fuentes principales:

La planeación estratégica: agrupadas las aplicaciones en conjuntos relacionados entre sí y no como programas aislados. Las aplicaciones deben comprender todos los sistemas que puedan ser desarrollados en la

dependencia, independientemente de los recursos que impliquen su desarrollo y justificación en el momento de la planeación.

Los requerimientos de los usuarios.

El inventario de sistemas en proceso al recopilar la información de los cambios que han sido solicitados, sin importar si se efectuaron o se registraron.

La situación de una aplicación en dicho inventario puede ser alguna de las siguientes:

Planeada para ser desarrollada en el futuro.

En desarrollo.

En proceso, pero con modificaciones en desarrollo.

En proceso con problemas detectados.

En proceso sin problemas.

En proceso esporádicamente.

Nota: Se deberá documentar detalladamente la fuente que generó la necesidad de la aplicación. La primera parte será evaluar la forma en que se encuentran especificadas las políticas, los procedimientos y los estándares de análisis, si es que se cumplen y si son los adecuados para la dependencia.

Es importante revisar la situación en que se encuentran los manuales de análisis y si están acordes con las necesidades de la dependencia. En algunas ocasiones se tiene una microcomputadora, con sistemas sumamente sencillos y se solicita que se lleve a cabo una serie de análisis que después hay que plasmar en documentos señalados en los estándares, lo cual hace que esta fase sea muy compleja y costosa. Los sistemas y su documentación deben estar acordes con las características y necesidades de una dependencia específica.

Se debe evaluar la obtención de datos sobre la operación, flujo, nivel, jerarquía de la información que se tendrá a través del sistema. Se han de comparar los objetivos de los sistemas desarrollados con las operaciones actuales, para ver si el estudio de la ejecución deseada corresponde al actual.

La auditoría en sistemas debe evaluar los documentos y registros usados en la elaboración del sistema, así como todas las salidas y reportes, la descripción de las actividades de flujo de la información y de procedimientos, los archivos almacenados, su uso y su relación con otros archivos y sistemas, su frecuencia de acceso, su conservación, su seguridad y control, la documentación propuesta, las entradas y salidas del sistema y los documentos fuentes a usarse.

Con la información obtenida podemos contestar a las siguientes preguntas:

¿Se está ejecutando en forma correcta y eficiente el proceso de información?

¿Puede ser simplificado para mejorar su aprovechamiento?

¿Se debe tener una mayor interacción con otros sistemas?

¿Se tiene propuesto un adecuado control y seguridad sobre el sistema?

¿Está en el análisis la documentación adecuada?

EVALUACIÓN DEL DISEÑO LÓGICO DEL SISTEMA

En esta etapa se deberán analizar las especificaciones del sistema.

¿Qué deberá hacer?, ¿Cómo lo deberá hacer?, ¿Secuencia y ocurrencia de los datos, el proceso y salida de reportes?

Una vez que hemos analizado estas partes, se deberá estudiar la participación que tuvo el usuario en la identificación del nuevo sistema, la participación de auditoría interna en el diseño de los controles y la determinación de los procedimientos de operación y decisión.

Al tener el análisis del diseño lógico del sistema debemos compararlo con lo que realmente se está obteniendo en la cual debemos evaluar lo planeado, cómo fue planeado y lo que realmente se está obteniendo.

Los puntos a evaluar son:

Entradas.

Salidas.

Procesos.

Especificaciones de datos.

Especificaciones de proceso.

Métodos de acceso.

Operaciones.

Manipulación de datos (antes y después del proceso electrónico de datos).

Proceso lógico necesario para producir informes.

Identificación de archivos, tamaño de los campos y registros.

Proceso en línea o lote y su justificación.

Frecuencia y volúmenes de operación.

Sistemas de seguridad.

Sistemas de control.

Responsables.

Número de usuarios.

Dentro del estudio de los sistemas en uso se deberá solicitar:

Manual del usuario.

Descripción de flujo de información y/o procesos.

Descripción y distribución de información.

Manual de formas.

Manual de reportes.

Lista de archivos y especificaciones.

Lo que se debe determinar en el sistema:

En el procedimiento:

¿Quién hace, cuando y como?

¿Qué formas se utilizan en el sistema?

¿Son necesarias, se usan, están duplicadas?

¿El número de copias es el adecuado?

¿Existen puntos de control o faltan?

En la gráfica de flujo de información:

¿Es fácil de usar?

¿Es lógica?

¿Se encontraron lagunas?

¿Hay faltas de control?

En el diseño:

¿Cómo se usará la herramienta de diseño si existe?

¿Qué también se ajusta la herramienta al procedimiento?

EVALUACIÓN DEL DESARROLLO DEL SISTEMA

En esta etapa del sistema se deberán auditar los programas, su diseño, el lenguaje utilizado, interconexión entre los programas y características del hardware empleado (total o parcial) para el desarrollo del sistema. Al evaluar un sistema de información se tendrá presente que todo sistema debe proporcionar información para planear, organizar y controlar de manera eficaz y oportuna, para reducir la duplicidad de datos y de reportes y obtener una mayor seguridad en la forma más económica posible. De ese modo contará con los mejores elementos para una adecuada toma de decisiones. Al tener un proceso distribuido, es preciso considerar la seguridad del movimiento de la información entre nodos. El proceso de planeación de sistemas debe definir la red óptima de comunicaciones, los tipos de mensajes requeridos, el tráfico esperado en las líneas de comunicación y otros factores que afectan el diseño. Es importante considerar las variables que afectan a un sistema: ubicación en los niveles de la organización, el tamaño y los recursos que utiliza. Las características que deben evaluarse en los sistemas son:

Dinámicos (susceptibles de modificarse).

Estructurados (las interacciones de sus componentes o subsistemas deben actuar como un todo)

Integrados (un solo objetivo). En él habrá sistemas que puedan ser interrelacionados y no programas aislados.

Accesibles (que estén disponibles).

Necesarios (que se pruebe su utilización).

Comprensibles (que contengan todos los atributos).

Oportunos (que esté la información en el momento que se requiere).

Funcionales (que proporcionen la información adecuada a cada nivel).

Estándar (que la información tenga la misma interpretación en los distintos niveles).

Modulares (facilidad para ser expandidos o reducidos).

Jerárquicos (por niveles funcionales).

Seguros (que sólo las personas autorizadas tengan acceso).

Únicos (que no duplique información).

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 programador y su jefe inmediato elaboren un plan de trabajo en el cual se especifiquen actividades, metas, personal participante y tiempos. Este plan debe 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 estar el calendario de reuniones de revisión, las cuales tendrán diferentes niveles de detalle.

CUESTIONARIO

1. ¿Existe una lista de proyectos de sistema de procedimiento de información y fechas programadas de implantación que puedan ser considerados como plan maestro?
2. ¿Está relacionado el plan maestro con un plan general de desarrollo de la dependencia?
3. ¿Ofrece el plan maestro la atención de solicitudes urgentes de los usuarios?
4. ¿Asigna el plan maestro un porcentaje del tiempo total de producción al reproceso o fallas de equipo?
5. Escribir la lista de proyectos a corto plazo y largo plazo.
6. Escribir una lista de sistemas en proceso periodicidad y usuarios.
7. ¿Quién autoriza los proyectos?
8. ¿Cómo se asignan los recursos?
9. ¿Cómo se estiman los tiempos de duración?
10. ¿Quién interviene en la planeación de los proyectos?
11. ¿Cómo se calcula el presupuesto del proyecto?
12. ¿Qué técnicas se usan en el control de los proyectos?
13. ¿Quién asigna las prioridades?
14. ¿Cómo se asignan las prioridades?
15. ¿Cómo se controla el avance del proyecto?
16. ¿Con qué periodicidad se revisa el reporte de avance del proyecto?

17. ¿Cómo se estima el rendimiento del personal?
18. ¿Con que frecuencia se estiman los costos del proyecto para compararlo con lo presupuestado?
19. ¿Qué acciones correctivas se toman en caso de desviaciones?
20. ¿Qué pasos y técnicas siguen en la planeación y control de los proyectos?

Enumérelos secuencialmente.

- () Determinación de los objetivos.
- () Señalamiento de las políticas.
- () Designación del funcionario responsable del proyecto.
- () Integración del grupo de trabajo.
- () Integración de un comité de decisiones.
- () Desarrollo de la investigación.
- () Documentación de la investigación.
- () Factibilidad de los sistemas.
- () Análisis y valuación de propuestas.
- () Selección de equipos.

21. ¿Se llevan a cabo revisiones periódicas de los sistemas para determinar si aún cumplen con los objetivos para los cuales fueron diseñados?

De análisis SÍ () NO ()

De programación SÍ () NO ()

Observaciones

22. Incluir el plazo estimado de acuerdo con los proyectos que se tienen en que el departamento de informática podría satisfacer las necesidades de la dependencia, según la situación actual.

CONTROL DE DISEÑO DE SISTEMAS Y PROGRAMACIÓN

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.

El siguiente cuestionario se presenta como ejemplo para la evaluación del diseño y prueba de los sistemas:

1. ¿Quiénes intervienen al diseñar un sistema?

Usuario.

Analista.

Programadores.

Operadores.

Gerente de departamento.

Audidores internos.

Asesores.

Otros.

2. ¿Los analistas son también programadores?

SÍ () NO ()

3. ¿Qué lenguaje o lenguajes conocen los analistas?

4. ¿Cuántos analistas hay y qué experiencia tienen?

5. ¿Qué lenguaje conocen los programadores?

6. ¿Cómo se controla el trabajo de los analistas?

7. ¿Cómo se controla el trabajo de los programadores?

8. Indique qué pasos siguen los programadores en el desarrollo de un programa:

Estudio de la definición ()

Discusión con el analista ()

Diagrama de bloques ()

Tabla de decisiones ()

Prueba de escritorio ()

Codificación ()

¿Es enviado a captura o los programadores capturan? ()

¿Quién los captura? _____

- | | |
|------------------------------|-----|
| Compilación | () |
| Elaborar datos de prueba | () |
| Solicitar datos al analista | () |
| Correr programas con datos | () |
| Revisión de resultados | () |
| Corrección del programa | () |
| Documentar el programa | () |
| Someter resultados de prueba | () |
| Entrega del programa | () |

9. ¿Qué documentación acompaña al programa cuando se entrega?

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)_____

ENTREVISTA 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.

Con esta información se puede comenzar a realizar la entrevista para determinar si los servicios proporcionados y planeados por la dirección de Informática cubren las necesidades de información de las dependencias.

A continuación se presenta una guía de cuestionario para aplicarse durante la entrevista con el usuario.

1. ¿Considera que el Departamento de Sistemas de Información de los resultados esperados?.

Si () No ()

¿Por que?

2. ¿Cómo considera usted, en general, el servicio proporcionado por el Departamento de Sistemas de Información?

Deficiente ()

Aceptable ()

Satisfactorio ()

Excelente ()

¿Por que?

3. ¿Cubre sus necesidades el sistema que utiliza el departamento de cómputo?

No las cubre ()

Parcialmente ()

La mayor parte ()

Todas ()

¿Por que?

4. ¿Hay disponibilidad del departamento de cómputo para sus requerimientos?

Generalmente no existe ()

Hay ocasionalmente ()

Regularmente ()

Siempre ()

¿Por que?

5. ¿Son entregados con puntualidad los trabajos?

Nunca ()

Rara vez ()

Ocasionalmente ()

Generalmente ()

Siempre ()

¿Por que?

6. ¿Que piensa de la presentación de los trabajadores solicitados al departamento de cómputo?

Deficiente ()

Aceptable ()

Satisfactorio ()

Excelente ()

¿Por que?

7. ¿Que piensa de la asesoría que se imparte sobre informática?

No se proporciona ()

Es insuficiente ()

Satisfactoria ()

Excelente ()

¿Por que?

8. ¿Que piensa de la seguridad en el manejo de la información proporcionada por el sistema que utiliza?

Nula ()

Riesgosa ()

Satisfactoria ()

Excelente ()

Lo desconoce ()

¿Por que?

9. ¿Existen fallas de exactitud en los procesos de información?

¿Cuáles?

10. ¿Cómo utiliza los reportes que se le proporcionan?

11. ¿Cuáles no Utiliza?

12. De aquellos que no utiliza ¿por que razón los recibe?

13. ¿Que sugerencias presenta en cuanto a la eliminación de reportes modificación, fusión, división de reporte?

14. ¿Se cuenta con un manual de usuario por Sistema?

SI () NO ()

15. ¿Es claro y objetivo el manual del usuario?

SI () NO ()

16. ¿Que opinión tiene el manual?

NOTA: Pida el manual del usuario para evaluarlo.

17. ¿Quién interviene de su departamento en el diseño de sistemas?

18. ¿Que sistemas desearía que se incluyeran?

19. Observaciones.

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.

CONTROL DE LOS DATOS FUENTE Y MANEJO 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.

NOTA: Debido a que se denomina de diferentes formas la actividad de transcribir la información del dato fuente a la computadora, en el presente trabajo se le denominará captura o captación considerándola como sinónimo de digitalizar (capturista, digitalizadora).

Lo primero que se debe evaluar es la entrada de la información y que se tengan las cifras de control necesarias para determinar la veracidad de la información, para lo cual se puede utilizar el siguiente cuestionario:

1. Indique el porcentaje de datos que se reciben en el área de captación
2. Indique el contenido de la orden de trabajo que se recibe en el área de captación de datos:

Número de folio () Número(s) de formato(s) ()

Fecha y hora de Nombre, Depto. ()

Recepción () Usuario ()

Nombre del documento () Nombre responsable ()

Volumen aproximado Clave de cargo

de registro () (Número de cuenta) ()

Número de registros () Fecha y hora de entrega de

Clave del capturista () documentos y registros captados ()

Fecha estimada de entrega ()

3. Indique cuál(es) control(es) interno(s) existe(n) en el área de captación de datos:

Firmas de autorización ()

Recepción de trabajos () Control de trabajos atrasados ()

Revisión del documento () Avance de trabajos ()

fuentes (legibilidad,

verificación de datos

completos, etc.) ()

Prioridades de captación () Errores por trabajo ()

Producción de trabajo () Corrección de errores ()

Producción de cada operador () Entrega de trabajos ()

Verificación de cifras Costo Mensual por trabajo ()

de control de entrada con

las de salida. ()

4. ¿Existe un programa de trabajo de captación de datos?

a) ¿Se elabora ese programa para cada turno?

Diariamente ()

Semanalmente ()

Mensualmente ()

b) La elaboración del programa de trabajos se hace:

Internamente ()

Se les señalan a los usuarios las prioridades ()

c) ¿Que acción(es) se toma(n) si el trabajo programado no se recibe a tiempo?

5. ¿Quién controla las entradas de documentos fuente?

6. ¿En que forma las controla?

7. ¿Que cifras de control se obtienen?

Sistema Cifras que se Observaciones

Obtienen

8. ¿Que documento de entrada se tienen?
Sistemas Documentos Depto. que periodicidad Observaciones
proporciona
el documento

9. ¿Se anota que persona recibe la información y su volumen?
SI () NO ()

10. ¿Se anota a que capturista se entrega la información, el volumen y la hora?
SI () NO ()

11. ¿Se verifica la cantidad de la información recibida para su captura?
SI () NO ()

12. ¿Se revisan las cifras de control antes de enviarlas a captura?
SI () NO ()

13. ¿Para aquellos procesos que no traigan cifras de control se ha establecido criterios a fin de asegurar que la información es completa y valida?
SI () NO ()

14. ¿Existe un procedimiento escrito que indique como tratar la información inválida (sin firma ilegible, no corresponden las cifras de control)?

15. En caso de resguardo de información de entrada en sistemas, ¿Se custodian en un lugar seguro?

16. Si se queda en el departamento de sistemas, ¿Por cuanto tiempo se guarda?

17. ¿Existe un registro de anomalías en la información debido a mala codificación?

18. ¿Existe una relación completa de distribución de listados, en la cual se indiquen personas, secuencia y sistemas a los que pertenecen?

19. ¿Se verifica que las cifras de las validaciones concuerden con los documentos de entrada?

20. ¿Se hace una relación de cuando y a quién fueron distribuidos los listados?

21. ¿Se controlan separadamente los documentos confidenciales?

22. ¿Se aprovecha adecuadamente el papel de los listados inservibles?

23. ¿Existe un registro de los documentos que entran a capturar?

24. ¿Se hace un reporte diario, semanal o mensual de captura?

25. ¿Se hace un reporte diario, semanal o mensual de anomalías en la información de entrada?

26. ¿Se lleva un control de la producción por persona?

27. ¿Quién revisa este control?

28. ¿Existen instrucciones escritas para capturar cada aplicación o, en su defecto existe una relación de programas?

CONTROL DE OPERACIÓN

La eficiencia y el costo de la operación de un sistema de cómputo se ven fuertemente afectados por la calidad e integridad de la documentación requerida para el proceso en la computadora.

El objetivo del presente ejemplo de cuestionario es señalar los procedimientos e instructivos formales de operación, analizar su estandarización y evaluar el cumplimiento de los mismos.

1. ¿Existen procedimientos formales para la operación del sistema de computo?

SI () NO ()

2. ¿Están actualizados los procedimientos?

SI () NO ()

3. Indique la periodicidad de la actualización de los procedimientos:

Semestral ()

Anual ()

Cada vez que haya cambio de equipo ()

4. Indique el contenido de los instructivos de operación para cada aplicación:

Identificación del sistema ()

Identificación del programa ()

Periodicidad y duración de la corrida ()

Especificación de formas especiales ()

Especificación de cintas de impresoras ()

- Etiquetas de archivos de salida, nombre, ()
 archivo lógico, y fechas de creación y expiración
- Instructivo sobre materiales de entrada y salida ()
- Altos programados y la acciones requeridas ()
- Instructivos específicos
 a los operadores en caso de falla del equipo ()
- Instructivos de reinicio ()
- Procedimientos de recuperación para proceso de
 gran duración o criterios ()
- Identificación de todos los
 dispositivos de la máquina a ser usados ()
- Especificaciones de resultados
 (cifras de control, registros de salida por archivo, etc)()

5. ¿Existen órdenes de proceso para cada corrida en la computadora (incluyendo pruebas, compilaciones y producción)?

SI () NO ()

6. ¿Son suficientemente claras para los operadores estas órdenes?

SI () NO ()

7. ¿Existe una estandarización de las ordenes de proceso?

SI () NO ()

8. ¿Existe un control que asegure la justificación de los procesos en el computador? (Que los procesos que se están autorizados y tengan una razón de ser procesados.

SI () NO ()

9. ¿Cómo programan los operadores los trabajos dentro del departamento de cómputo?

Primero que entra, primero que sale ()

se respetan las prioridades, ()

Otra (especifique) ()

10. ¿Los retrasos o incumplimiento con el programa de operación diaria, se revisa y analiza?

SI () NO ()

11. ¿Quién revisa este reporte en su caso?

12. Analice la eficiencia con que se ejecutan los trabajos dentro del departamento de cómputo, tomando en cuenta equipo y operador, a través de inspección visual, y describa sus observaciones.

13. ¿Existen procedimientos escritos para la recuperación del sistema en caso de falla?

14. ¿Cómo se actúa en caso de errores?

15. ¿Existen instrucciones específicas para cada proceso, con las indicaciones pertinentes?

16. ¿Se tienen procedimientos específicos que indiquen al operador que hacer cuando un programa interrumpe su ejecución u otras dificultades en proceso?

17. ¿Puede el operador modificar los datos de entrada?

18. ¿Se prohíbe a analistas y programadores la operación del sistema que programo o analizo?

19. ¿Se prohíbe al operador modificar información de archivos o bibliotecas de programas?

20. ¿El operador realiza funciones de mantenimiento diario en dispositivos que así lo requieran?

21. ¿Las intervenciones de los operadores:

Son muy numerosas? SI () NO ()

Se limitan los mensajes esenciales? SI () NO ()

Otras

(especifique) _____

22. ¿Se tiene un control adecuado sobre los sistemas y programas que están en operación?

SI () NO ()

23. ¿Cómo controlan los trabajos dentro del departamento de cómputo?

24. ¿Se rota al personal de control de información con los operadores procurando un entrenamiento cruzado y evitando la manipulación fraudulenta de datos?

SI () NO ()

25. ¿Cuentan los operadores con una bitácora para mantener registros de cualquier evento y acción tomada por ellos?

Si ()

por máquina ()

escrita manualmente ()

NO ()

26. Verificar que exista un registro de funcionamiento que muestre el tiempo de paros y mantenimiento o instalaciones de software.

27. ¿Existen procedimientos para evitar las corridas de programas no autorizados?

SI () NO ()

28. ¿Existe un plan definido para el cambio de turno de operaciones que evite el descontrol y discontinuidad de la operación.

29. Verificar que sea razonable el plan para coordinar el cambio de turno.

30. ¿Se hacen inspecciones periódicas de muestreo?

SI () NO ()

31. Enuncie los procedimientos mencionados en el inciso anterior:

32. ¿Se permite a los operadores el acceso a los diagramas de flujo, programas fuente, etc. fuera del departamento de cómputo?
SI () NO ()

33. ¿Se controla estrictamente el acceso a la documentación de programas o de aplicaciones rutinarias?

SI () NO ()

¿Cómo?_____

34. Verifique que los privilegios del operador se restrinjan a aquellos que le son asignados a la clasificación de seguridad de operador.

35. ¿Existen procedimientos formales que se deban observar antes de que sean aceptados en operación, sistemas nuevos o modificaciones a los mismos?

SI () NO ()

36. ¿Estos procedimientos incluyen corridas en paralelo de los sistemas modificados con las versiones anteriores?

SI () NO ()

37. ¿Durante cuanto tiempo?

38. ¿Que precauciones se toman durante el periodo de implantación?

39. ¿Quién da la aprobación formal cuando las corridas de prueba de un sistema modificado o nuevo están acordes con los instructivos de operación.

40. ¿Se catalogan los programas liberados para producción rutinaria?

SI () NO ()

41. Mencione que instructivos se proporcionan a las personas que intervienen en la operación rutinaria de un sistema.

42. Indique que tipo de controles tiene sobre los archivos magnéticos de los archivos de datos, que aseguren la utilización de los datos precisos en los procesos correspondientes.

43. ¿Existe un lugar para archivar las bitácoras del sistema del equipo de cómputo?

SI () NO ()

44. Indique como está organizado este archivo de bitácora.

Por fecha ()

Por fecha y hora ()

Por turno de operación ()

Otros ()

45. ¿Cuál es la utilización sistemática de las bitácoras?

46. ¿Además de las mencionadas anteriormente, que otras funciones o áreas se encuentran en el departamento de cómputo actualmente?

47. Verifique que se lleve un registro de utilización del equipo diario, sistemas en línea y batch, de tal manera que se pueda medir la eficiencia del uso de equipo.

48. ¿Se tiene inventario actualizado de los equipos y terminales con su localización?

SI () NO ()

49. ¿Cómo se controlan los procesos en línea?

50. ¿Se tienen seguros sobre todos los equipos?

SI () NO ()

51. ¿Con que compañía?

Solicitar pólizas de seguros y verificar tipo de seguro y montos.

52. ¿Cómo se controlan las llaves de acceso (Password)?.

CONTROLES DE SALIDA

1. ¿Se tienen copias de los archivos en otros locales?
 2. ¿Dónde se encuentran esos locales?
 3. ¿Que seguridad física se tiene en esos locales?
 4. ¿Que confidencialidad se tiene en esos locales?
 5. ¿Quién entrega los documentos de salida?
 6. ¿En que forma se entregan?
 7. ¿Que documentos?
 8. ¿Que controles se tienen?
 9. ¿Se tiene un responsable (usuario) de la información de cada sistema?
¿Cómo se atienden solicitudes de información a otros usuarios del mismo sistema?
 10. ¿Se destruye la información utilizada, o bien que se hace con ella?
- Destruye () Vende () Tira () Otro _____

CONTROL DE MEDIOS DE ALMACENAMIENTO MASIVO

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.

CONTROL DE ALMACENAMIENTO MASIVO

OBJETIVOS

El objetivo de este cuestionario es evaluar la forma como se administran los dispositivos de almacenamiento básico de la dirección.

1. Los locales asignados a la cinta teca y discoteca tienen:

Aire acondicionado ()

Protección contra el fuego ()

(Señalar que tipo de protección)_____

Cerradura especial ()

Otra

2. ¿Tienen la cinta teca y discoteca protección automática contra el fuego?

SI () NO ()

(señalar de que tipo)_____

3. ¿Que información mínima contiene el inventario de la cinta teca y la discoteca?

Número de serie o carrete

Número o clave del usuario

Número del archivo lógico

Nombre del sistema que lo genera

Fecha de expiración del archivo

Fecha de expiración del archivo

Número de volumen

Otros

4. ¿Se verifican con frecuencia la validez de los inventarios de los archivos magnéticos?

SI NO

5. En caso de existir discrepancia entre las cintas o discos y su contenido, se resuelven y explican satisfactoriamente las discrepancias?

SI NO

6. ¿Que tan frecuentes son estas discrepancias?

7. ¿Se tienen procedimientos que permitan la reconstrucción de un archivo en cinta a disco, el cual fue inadvertidamente destruido?

SI NO

8. ¿Se tienen identificados los archivos con información confidencial y se cuenta con claves de acceso?

SI NO

¿Cómo? _____

9. ¿Existe un control estricto de las copias de estos archivos?

SI NO

10. ¿Que medio se utiliza para almacenarlos?

Mueble con cerradura ()

Bóveda ()

Otro(especifique)_____

11. Este almacén esta situado:

En el mismo edificio del departamento ()

En otro lugar ()

¿Cual?_____

12. ¿Se borran los archivos de los dispositivos de almacenamiento, cuando se desechan estos?

SI () NO ()

13. ¿Se certifica la destrucción o baja de los archivos defectuosos?

SI () NO ()

14. ¿Se registran como parte del inventario las nuevas cintas que recibe la biblioteca?

SI () NO ()

15 ¿Se tiene un responsable, por turno, de la cinto teca y discoteca?

SI () NO ()

16. ¿Se realizan auditorias periódicas a los medios de almacenamiento?

SI () NO ()

17. ¿Que medidas se toman en el caso de extravío de algún dispositivo de almacenamiento?

18. ¿Se restringe el acceso a los lugares asignados para guardar los dispositivos de almacenamiento, al personal autorizado?

SI () NO ()

19. ¿Se tiene relación del personal autorizado para firmar la salida de archivos confidenciales?

SI () NO ()

20. ¿Existe un procedimiento para registrar los archivos que se prestan y la fecha en que se devolverán?

SI () NO ()

21. ¿Se lleva control sobre los archivos prestados por la instalación?

SI () NO ()

22. En caso de préstamo ¿Conque información se documentan?
Nombre de la institución a quién se hace el préstamo.

Fecha de recepción ()

Fecha en que se debe devolver ()

Archivos que contiene ()

Formatos ()

Cifras de control ()

Código de grabación ()

Nombre del responsable que los presto ()

Otros

23. Indique qué procedimiento se sigue en el reemplazo de las cintas que contienen los archivos maestros:

24. ¿Se conserva la cinta maestra anterior hasta después de la nueva cinta?

SI () NO ()

25. ¿El cintotecario controla la cinta maestra anterior previendo su uso incorrecto o su eliminación prematura

SI () NO ()

26. ¿La operación de reemplazo es controlada por el cintotecario?
SI () NO ()

27. ¿Se utiliza la política de conservación de archivos hijo-padre-abuelo?
SI () NO ()

28. En los procesos que manejan archivos en línea, ¿Existen procedimientos para recuperar los archivos?

SI () NO ()

29. ¿Estos procedimientos los conocen los operadores?
SI () NO ()

30. ¿Con que periodicidad se revisan estos procedimientos?

MENSUAL () ANUAL ()

SEMESTRAL () OTRA ()

31. ¿Existe un responsable en caso de falla?
SI () NO ()

32. ¿Explique que políticas se siguen para la obtención de archivos de respaldo?

33. ¿Existe un procedimiento para el manejo de la información de la cintoteca?
SI () NO ()

34. ¿Lo conoce y lo sigue el cintotecario?
SI () NO ()

35. ¿Se distribuyen en forma periódica entre los jefes de sistemas y programación informes de archivos para que liberen los dispositivos de almacenamiento?

SI () NO ()

¿Con qué frecuencia?

CONTROL DE MANTENIMIENTO

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 mas 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.

Para evaluar el control que se tiene sobre el mantenimiento y las fallas se pueden utilizar los siguientes cuestionarios:

1. Especifique el tipo de contrato de mantenimiento que se tiene (solicitar copia del contrato).

2. ¿Existe un programa de mantenimiento preventivo para cada dispositivo del sistema de computo?

SI () NO ()

3. ¿Se lleva a cabo tal programa?

SI () NO ()

4. ¿Existen tiempos de respuesta y de compostura estipulados en los contratos?

SI () NO ()

5. Si los tiempos de reparación son superiores a los estipulados en el contrato, ¿Qué acciones correctivas se toman para ajustarlos a lo convenido?

SI () NO ()

6. Solicite el plan de mantenimiento preventivo que debe ser proporcionado por el proveedor.-

SI () NO ()

¿Cual?

8. ¿Cómo se notifican las fallas?

9. ¿Cómo se les da seguimiento?

ORDEN EN EL CENTRO DE CÓMPUTO

Una dirección de Sistemas de Información bien administrada debe tener y observar reglas relativas al orden y cuidado del departamento de cómputo. Los dispositivos del sistema de cómputo, los archivos magnéticos, pueden ser dañados si se manejan en forma inadecuada y eso puede traducirse en pérdidas irreparables de información o en costos muy elevados en la reconstrucción de archivos. Se deben revisar las disposiciones y reglamentos que coadyuven al mantenimiento del orden dentro del departamento de cómputo.

1. Indique la periodicidad con que se hace la limpieza del departamento de cómputo y de la cámara de aire que se encuentra abajo del piso falso si existe y los ductos de aire:

Semanalmente () Quincenalmente ()

Mensualmente () Bimestralmente ()

No hay programa () Otra (especifique) ()

2. Existe un lugar asignado a las cintas y discos magnéticos?

SI () NO ()

3. ¿Se tiene asignado un lugar específico para papelería y utensilios de trabajo?

SI () NO ()

4. ¿Son funcionales los muebles asignados para la cinta teca y discoteca?

SI () NO ()

5. ¿Se tienen disposiciones para que se acomoden en su lugar correspondiente, después de su uso, las cintas, los discos magnéticos, la papelería, etc.?

SI () NO ()

6. Indique la periodicidad con que se limpian las unidades de cinta:

Al cambio de turno () cada semana ()
cada día () otra (especificar) ()

7. ¿Existen prohibiciones para fumar, tomar alimentos y refrescos en el departamento de cómputo?
SI () NO ()

8. ¿Se cuenta con carteles en lugares visibles que recuerdan dicha prohibición?
SI () NO ()

9. ¿Se tiene restringida la operación del sistema de cómputo al personal especializado de la Dirección de Informática?
SI () NO ()

10. Mencione los casos en que personal ajeno al departamento de operación opera el sistema de cómputo.

EVALUACIÓN DE LA CONFIGURACIÓN DEL SISTEMA DE CÓMPUTO

Los objetivos son evaluar la configuración actual tomando en consideración las aplicaciones y el nivel de uso del sistema, evaluar el grado de eficiencia con el cual el sistema operativo satisface las necesidades de la instalación y revisar las políticas seguidas por la unidad de informática en la conservación de su programa teca.

Esta sección esta orientada a:

a) Evaluar posibles cambios en el hardware a fin de nivelar el sistema de cómputo con la carga de trabajo actual o de comparar la capacidad instalada con los planes de desarrollo a mediano y largo plazo.

b) Evaluar las posibilidades de modificar el equipo para reducir el costo o bien el tiempo de proceso.

c) Evaluar la utilización de los diferentes dispositivos periféricos.

1. De acuerdo con los tiempos de utilización de cada dispositivo del sistema de cómputo, ¿existe equipo?

¿Con poco uso? SI () NO ()

¿Ocioso? SI () NO ()

¿Con capacidad superior a la necesaria? SI () NO ()

Describa cual es

2. ¿El equipo mencionado en el inciso anterior puede reemplazarse por otro mas lento y de menor costo?

SI () NO ()

3. Si la respuesta al inciso anterior es negativa, ¿el equipo puede ser cancelado?

SI () NO ()

4. De ser negativa la respuesta al inciso anterior, explique las causas por las que no puede ser cancelado o cambiado.

—

5. ¿El sistema de cómputo tiene capacidad de teleproceso?

SI () NO ()

6. ¿Se utiliza la capacidad de teleproceso?

SI () NO ()

7. ¿En caso negativo, exponga los motivos por los cuales no utiliza el teleproceso?

SI () NO ()

8. ¿Cuántas terminales se tienen conectadas al sistema de cómputo?

9. ¿Se ha investigado si ese tiempo de respuesta satisface a los usuarios?

SI () NO ()

10. ¿La capacidad de memoria y de almacenamiento máximo del sistema de cómputo es suficiente

para atender el proceso por lotes y el proceso remoto?

SI () NO ()

SEGURIDAD LÓGICA Y CONFIDENCIAL

La computadora es un instrumento que estructura gran cantidad de información, la cual puede ser confidencial para individuos, empresas o instituciones, y puede ser mal utilizada o divulgada a personas que hagan mal uso de esta. También puede ocurrir robos, fraudes o sabotajes que provoquen la destrucción total o parcial de la actividad computacional.

Esta información puede ser de suma importancia, y el no tenerla en el momento preciso puede provocar retrasos sumamente costosos. Antes esta situación, en el transcurso del siglo XX, el mundo ha sido testigo de la transformación de algunos aspectos de seguridad y de derecho.

En la actualidad y principalmente en las computadoras personales, se ha dado otro factor que hay que considerar el llamado "virus" de las computadoras, el cual aunque tiene diferentes intenciones se encuentra principalmente para paquetes que son copiados sin autorización ("piratas") y borra toda la información que se tiene en un disco.

Al auditar los sistemas se debe tener cuidado que no se tengan copias "piratas" o bien que, al conectarnos en red con otras computadoras, no exista la posibilidad de transmisión del virus.

El uso inadecuado de la computadora comienza desde la utilización de tiempo de máquina para usos ajenos de la organización, la copia de programas para fines de comercialización sin reportar los derechos de autor hasta el acceso por vía telefónica a bases de datos a fin de modificar la información con propósitos fraudulentos.

Un método eficaz para proteger sistemas de computación es el software de control de acceso. Dicho simplemente, los paquetes de control de acceso protegen contra el acceso no autorizado, pues piden del usuario una contraseña antes de permitirle el acceso a información confidencial. Dichos paquetes han sido populares desde hace muchos años en el mundo de las computadoras grandes, y los principales proveedores ponen a disposición de clientes algunos de estos paquetes.

El sistema integral de seguridad debe comprender:

Elementos administrativos

Definición de una política de seguridad

Organización y división de responsabilidades

Seguridad física y contra catástrofes (incendio, terremotos, etc.)

Prácticas de seguridad del personal

Elementos técnicos y procedimientos

Sistemas de seguridad (de equipos y de sistemas, incluyendo todos los elementos, tanto redes como terminales.

Aplicación de los sistemas de seguridad, incluyendo datos y archivos

El papel de los auditores, tanto internos como externos

Planeación de programas de desastre y su prueba.

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

Clasificar la instalación en términos de riesgo (alto, mediano, pequeño).

Identificar aquellas aplicaciones que tengan un alto riesgo.

Cuantificar el impacto en el caso de suspensión del servicio en aquellas aplicaciones con un alto riesgo.

Formular las medidas de seguridad necesarias dependiendo del nivel de seguridad que se requiera.

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

Que sucedería si no se puede usar el sistema?

Si la contestación es que no se podría seguir trabajando, esto nos sitúa en un sistema de alto riesgo.

La siguiente pregunta es:

¿Que implicaciones tiene el que no se obtenga el sistema y cuanto tiempo podríamos estar sin utilizarlo?

¿Existe un procedimiento alternativo y que problemas nos ocasionaría?

¿Que se ha hecho para un caso de emergencia?

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

Hay que tener mucho cuidado con la información que sale de la oficina, su utilización y que sea borrada al momento de dejar la instalación que está dando respaldo.

Para clasificar la instalación en términos de riesgo se debe:

Clasificar los datos, información y programas que contienen información confidencial que tenga un alto valor dentro del mercado de competencia de una organización, e información que sea de difícil recuperación.

Identificar aquella información que tenga un gran costo financiero en caso de pérdida o bien puede provocar un gran impacto en la toma de decisiones.

Determinar la información que tenga una gran pérdida en la organización y, consecuentemente, puedan provocar hasta la posibilidad de que no pueda sobrevivir sin esa información.

Para cuantificar el riesgo es necesario que se efectúen entrevistas con los altos niveles administrativos que sean directamente afectados por la suspensión en el procesamiento y que cuantifiquen el impacto que les puede causar este tipo de situaciones.

Para evaluar las medidas de seguridad se debe:

Especificar la aplicación, los programas y archivos.

Las medidas en caso de desastre, pérdida total, abuso y los planes necesarios.

Las prioridades que se deben tomar en cuanto a las acciones a corto y largo plazo.

En cuanto a la división del trabajo se debe evaluar que se tomen las siguientes precauciones, las cuales dependerán del riesgo que tenga la información y del tipo y tamaño de la organización.

El personal que prepara la información no debe tener acceso a la operación.

Los análisis y programadores no deben tener acceso al área de operaciones y viceversa.

Los operadores no debe tener acceso irrestringido a las librerías ni a los lugares donde se tengan los archivos almacenados; es importante separar las funciones de librería y de operación.

Los operadores no deben ser los únicos que tengan el control sobre los trabajos procesados y no deben hacer las correcciones a los errores detectados.

Al implantar sistemas de seguridad puede, reducirse la flexibilidad en el trabajo, pero no debe reducir la eficiencia.

SEGURIDAD FÍSICA

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

Entre las precauciones que se deben revisar están:

Los ductos del aire acondicionado deben estar limpios, ya que son una de las principales causas del polvo y se habrá de contar con detectores de humo que indiquen la posible presencia de fuego.

En las instalaciones de alto riesgo se debe tener equipo de fuente no interrumpible, tanto en la computadora como en la red y los equipos de teleproceso.

En cuanto a los extintores, se debe revisar en número de estos, su capacidad, fácil acceso, peso y tipo de producto que utilizan. Es muy frecuente que se tengan los extintores, pero puede suceder que no se encuentren recargados o bien que sean de difícil acceso de un peso tal que sea difícil utilizarlos.

Esto es común en lugares donde se encuentran trabajando hombres y mujeres y los extintores están a tal altura o con un peso tan grande que una mujer no puede utilizarlos.

Otro de los problemas es la utilización de extintores inadecuados que pueden provocar mayor perjuicio a las máquinas (extintores líquidos) o que producen gases tóxicos.

También se debe ver si el personal sabe usar los equipos contra incendio y si ha habido prácticas en cuanto a su uso.

Se debe verificar que existan suficientes salidas de emergencia y que estén debidamente controladas para evitar robos por medio de estas salidas.

Los materiales mas peligrosos son las cintas magnéticas que al quemarse, producen gases tóxicos y el papel carbón que es altamente inflamable.

Tomando en cuenta lo anterior se elaboro el siguiente cuestionario:

1. ¿Se han adoptado medidas de seguridad en el departamento de sistemas de información?

SI () NO ()

2. ¿Existen una persona responsable de la seguridad?

SI () NO ()

3. ¿Se ha dividido la responsabilidad para tener un mejor control de la seguridad?

SI () NO ()

4. ¿Existe personal de vigilancia en la institución?

SI () NO ()

5. ¿La vigilancia se contrata?

a) Directamente ()

b) Por medio de empresas que venden ese servicio ()

6. ¿Existe una clara definición de funciones entre los puestos clave?

SI () NO ()

7. ¿Se investiga a los vigilantes cuando son contratados directamente?

SI () NO ()

8. ¿Se controla el trabajo fuera de horario?

SI () NO ()

9. ¿Se registran las acciones de los operadores para evitar que realicen algunas pruebas que puedan dañar los sistemas?.

SI () NO ()

10. ¿Existe vigilancia en el departamento de cómputo las 24 horas?

SI () NO ()

11. ¿Existe vigilancia a la entrada del departamento de cómputo las 24 horas?

a) Vigilante? ()

b) Recepcionista? ()

c) Tarjeta de control de acceso? ()

d) Nadie? ()

12. ¿Se permite el acceso a los archivos y programas a los programadores, analistas y operadores?

SI () NO ()

13. Se ha instruido a estas personas sobre que medidas tomar en caso de que alguien pretenda entrar sin autorización?

SI () NO ()

14. El edificio donde se encuentra la computadora esta situado a salvo de:

a) Inundación? ()

b) Terremoto? ()

c) Fuego? ()

d) Sabotaje? ()

15. El centro de cómputo tiene salida al exterior al exterior?
SI () NO ()

16. Describa brevemente la construcción del centro de cómputo, de preferencia proporcionando planos y material con que construido y equipo (muebles, sillas etc.) dentro del centro.

17. ¿Existe control en el acceso a este cuarto?

a) Por identificación personal? ()

b) Por tarjeta magnética? ()

c) Por claves verbales? ()

d) Otras? ()

18. ¿Son controladas las visitas y demostraciones en el centro de cómputo?
SI () NO ()

19. ¿Se registra el acceso al departamento de cómputo de personas ajenas a la dirección de informática?

SI () NO ()

20. ¿Se vigilan la moral y comportamiento del personal de la dirección de informática con el fin de mantener una buena imagen y evitar un posible fraude?
SI () NO ()

21. ¿Existe alarma para

a) Detectar fuego (calor o humo) en forma automática? ()

b) Avisar en forma manual la presencia del fuego? ()

c) Detectar una fuga de agua? ()

- d) Detectar magnéticos?
- e) No existe

22. ¿Estas alarmas están...

- a) En el departamento de cómputo?
- b) En la cinto teca y discoteca?

23. ¿Existe alarma para detectar condiciones anormales del ambiente?

- a) En el departamento de cómputo?
- b) En la cinto teca y discoteca?
- c) En otros lados

24. ¿La alarma es perfectamente audible?

SI NO

25. ¿Esta alarma también está conectada

- a) Al puesto de guardias?
- b) A la estación de Bomberos?
- c) A ningún otro lado?

Otro _____

26. Existen extintores de fuego

- a) Manuales?
- b) Automáticos?
- c) No existen

27. ¿Se ha adiestrado el personal en el manejo de los extintores?

SI NO

28. ¿Los extintores, manuales o automáticos a base de

TIPO SI NO

- a) Agua, SI NO
- b) Gas? SI NO
- c) Otros SI NO

29. ¿Se revisa de acuerdo con el proveedor el funcionamiento de los extintores?

SI () NO ()

30. ¿Si es que existen extintores automáticos son activador por detectores automáticos de fuego?

SI () NO ()

31. ¿Si los extintores automáticos son a base de agua ¿Se han tomado medidas para evitar que el agua cause mas daño que el fuego?

SI () NO ()

32. ¿Si los extintores automáticos son a base de gas, ¿Se ha tomado medidas para evitar que el gas cause mas daño que el fuego?

SI () NO ()

33. ¿Existe un lapso de tiempo suficiente, antes de que funcionen los extintores automáticos para que el personal

a) Corte la acción de los extintores por tratarse de falsas alarmas? SI () NO ()

b) Pueda cortar la energía Eléctrica SI () NO ()

c) Pueda abandonar el local sin peligro de intoxicación SI () NO ()

d) Es inmediata su acción? SI () NO ()

34. ¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos?

SI () NO ()

35. ¿Saben que hacer los operadores del departamento de cómputo, en caso de que ocurra una emergencia ocasionado por fuego?

SI () NO ()

36. ¿El personal ajeno a operación sabe que hacer en el caso de una emergencia (incendio)?

SI () NO ()

37. ¿Existe salida de emergencia?

SI () NO ()

38. ¿Esta puerta solo es posible abrirla:

- a) Desde el interior? ()
- b) Desde el exterior? ()
- c) Ambos Lados ()

39. ¿Se revisa frecuentemente que no esté abierta o descompuesta la cerradura de esta puerta y de las ventanas, si es que existen?

SI () NO ()

40. ¿Se ha adiestrado a todo el personal en la forma en que se deben desalojar las instalaciones en caso de emergencia?

SI () NO ()

41. ¿Se ha tomado medidas para minimizar la posibilidad de fuego:

- a) Evitando artículos inflamables en el departamento de cómputo? ()
- b) Prohibiendo fumar a los operadores en el interior? ()
- c) Vigilando y manteniendo el sistema eléctrico? ()
- d) No se ha previsto ()

42. ¿Se ha prohibido a los operadores el consumo de alimentos y bebidas en el interior del departamento de cómputo para evitar daños al equipo?

SI () NO ()

43. ¿Se limpia con frecuencia el polvo acumulado debajo del piso falso si existe?

SI () NO ()

44. ¿Se controla el acceso y préstamo en la

a) Discoteca?

b) Cinto teca?

c) Programo teca?

45. Explique la forma como se ha clasificado la información vital, esencial, no esencial etc.

46. ¿Se cuenta con copias de los archivos en lugar distinto al de la computadora?

SI NO

47. Explique la forma en que están protegidas físicamente estas copias (bóveda, cajas de seguridad etc.) que garantice su integridad en caso de incendio, inundación, terremotos, etc.

48. ¿Se tienen establecidos procedimientos de actualización a estas copias?

SI NO

49. Indique el número de copias que se mantienen, de acuerdo con la forma en que se clasifique la información:

0 1 2 3

50. ¿Existe departamento de auditoria interna en la institución?

SI NO

51. ¿Este departamento de auditoria interna conoce todos los aspectos de los sistemas?

SI NO

52. ¿Que tipos de controles ha propuesto?

53. ¿Se cumplen?

SI NO

54. ¿Se auditan los sistemas en operación?

SI () NO ()

55.¿Con que frecuencia?

- a) Cada seis meses ()
- b) Cada año ()
- c) Otra (especifique) ()

56.¿Cuándo se efectúan modificaciones a los programas, a iniciativa de quiénes?

- a) Usuario ()
 - b) Director de informática ()
 - c) Jefe de análisis y programación ()
 - d) Programador ()
 - e) Otras (especifique)
-

57.¿La solicitud de modificaciones a los programas se hacen en forma?

- a) Oral? ()
- b) Escrita? ()

En caso de ser escrita solicite formatos,

58.Una vez efectuadas las modificaciones, ¿se presentan las pruebas a los interesados?

SI () NO ()

59.¿Existe control estricto en las modificaciones?

SI () NO ()

60.¿Se revisa que tengan la fecha de las modificaciones cuando se hayan efectuado?

SI () NO ()

61.¿Si se tienen terminales conectadas, ¿se ha establecido procedimientos de operación?

SI () NO ()

62. Se verifica identificación:

- a) De la terminal
- b) Del Usuario
- c) No se pide identificación

63. ¿Se ha establecido que información puede ser accedida y por qué persona?
SI NO

64. ¿Se ha establecido un número máximo de violaciones en sucesión para que la computadora cierre esa terminal y se de aviso al responsable de ella?
SI NO

65. ¿Se registra cada violación a los procedimientos con el fin de llevar estadísticas y frenar las tendencias mayores?
SI NO

66. ¿Existen controles y medidas de seguridad sobre las siguientes operaciones?

¿Cuales son?

Recepción de documentos _____

Información Confidencial _____

Captación de documentos _____

Cómputo Electrónico _____

Programas _____

Discotecas y Cintas _____

Documentos de Salida _____

Archivos Magnéticos _____

Operación del equipo de computación _____

En cuanto al acceso de personal_____

Identificación del personal_____

Policía_____

Seguros contra robo e incendio_____

Cajas de seguridad_____

Otras (especifique)_____

SEGURIDAD EN LA UTILIZACIÓN DEL EQUIPO

En la actualidad los programas y los equipos son altamente sofisticados y sólo algunas personas dentro del centro de cómputo conocen al detalle el diseño, lo que puede provocar que puedan producir algún deterioro a los sistemas si no se toman las siguientes medidas:

- 1) Se debe restringir el acceso a los programas y a los archivos.
- 2) Los operadores deben trabajar con poca supervisión y sin la participación de los programadores, y no deben modificar los programas ni los archivos.
- 3) Se debe asegurar en todo momento que los datos y archivos usados sean los adecuados, procurando no usar respaldos inadecuados.
- 4) No debe permitirse la entrada a la red a personas no autorizadas, ni a usar las terminales.
- 5) Se deben realizar periódicamente una verificación física del uso de terminales y de los reportes obtenidos.

6) Se deben monitorear periódicamente el uso que se le está dando a las terminales.

7) Se deben hacer auditorias periódicas sobre el área de operación y la utilización de las terminales.

8) El usuario es el responsable de los datos, por lo que debe asegurarse que los datos recolectados sean procesados completamente. Esto sólo se logrará por medio de los controles adecuados, los cuales deben ser definidos desde el momento del diseño general del sistema

9) Deben existir registros que reflejen la transformación entre las diferentes funciones de un sistema.

10) Debe controlarse la distribución de las salidas (reportes, cintas, etc.).

11) Se debe guardar copias de los archivos y programas en lugares ajenos al centro de cómputo y en las instalaciones de alta seguridad; por ejemplo: los bancos.

12) Se debe tener un estricto control sobre el acceso físico a los archivos.

13) En el caso de programas, se debe asignar a cada uno de ellos, una clave que identifique el sistema, subsistema, programa y versión.

También evitará que el programador ponga nombres que nos signifiquen nada y que sean difíciles de identificar, lo que evitará que el programador utilice la computadora para trabajos personales. Otro de los puntos en los que hay que tener seguridad es en el manejo de información. Para controlar este tipo de información se debe:

1) Cuidar que no se obtengan fotocopias de información confidencial sin la debida autorización.

2) Sólo el personal autorizado debe tener acceso a la información confidencial.

3) Controlar los listados tanto de los procesos correctos como aquellos procesos con terminación incorrecta.

4) Controlar el número de copias y la destrucción de la información y del papel carbón de los reportes muy confidenciales.

El factor más importante de la eliminación de riesgos en la programación es que todos los programas y archivos estén debidamente documentados.

El siguiente factor en importancia es contar con los respaldos, y duplicados de los sistemas, programas, archivos y documentación necesarios para que pueda funcionar el plan de emergencia.

Equipo, programas y archivos

Control de aplicaciones por terminal

Definir una estrategia de seguridad de la red y de respaldos

Requerimientos físicos.

Estándar de archivos.

Auditoria interna en el momento del diseño del sistema, su implantación y puntos de verificación y control.

SEGURIDAD AL RESTAURAR EL EQUIPO

En un mundo que depende cada día mas de los servicios proporcionados por las computadoras, es vital definir procedimientos en caso de una posible falta o siniestro. Cuando ocurra una contingencia, es esencial que se conozca al detalle el motivo que la originó y el daño causado, lo que permitirá recuperar en el menor tiempo posible el proceso perdido. También se debe analizar el impacto futuro en el funcionamiento de la organización y prevenir cualquier implicación negativa.

En todas las actividades relacionadas con las ciencias de la computación, existe un riesgo aceptable, y es necesario analizar y entender estos factores para establecer los procedimientos que permitan analizarlos al máximo y en caso que ocurran, poder reparar el daño y reanudar la operación lo más rápidamente posible.

En una situación ideal, se deberían elaborar planes para manejar cualquier contingencia que se presente.

Analizando cada aplicación se deben definir planes de recuperación y reanudación, para asegurarse que los usuarios se vean afectados lo menos posible en caso de falla o siniestro. Las acciones de recuperación disponibles a nivel operativo pueden ser algunas de las siguientes:

En algunos casos es conveniente no realizar ninguna acción y reanudar el proceso.

Mediante copias periódicas de los archivos se puede reanudar un proceso a partir de una fecha determinada.

El procesamiento anterior complementado con un registro de las transacciones que afectaron a los archivos permitirá retroceder en los movimientos realizados a un archivo al punto de tener la seguridad del contenido del mismo a partir de él reanudar el proceso.

Analizar el flujo de datos y procedimientos y cambiar el proceso normal por un proceso alterno de emergencia.

Reconfigurar los recursos disponibles, tanto de equipo y sistemas como de comunicaciones.

Cualquier procedimiento que se determine que es el adecuado para un caso de emergencia deberá ser planeado y probado previamente.

Este grupo de emergencia deberá tener un conocimiento de los posibles procedimientos que puede utilizar, además de un conocimiento de las características de las aplicaciones, tanto desde el punto técnico como de su

prioridad, el nivel de servicio planeado y su influjo en la operación de la organización.

Además de los procedimientos de recuperación y reinicio de la información, se deben contemplar los procedimientos operativos de los recursos físicos como hardware y comunicaciones, planeando la utilización de equipos que permitan seguir operando en caso de falta de la corriente eléctrica, caminos alternos de comunicación y utilización de instalaciones de cómputo similares. Estas y otras medidas de recuperación y reinicio deberán ser planeadas y probadas previamente como en el caso de la información.

El objetivo del siguiente cuestionario es evaluar los procedimientos de restauración y repetición de procesos en el sistema de cómputo.

1) ¿Existen procedimientos relativos a la restauración y repetición de procesos en el sistema de cómputo?

SI () NO ()

2) ¿Enuncie los procedimientos mencionados en el inciso anterior?

3) ¿Cuentan los operadores con alguna documentación en donde se guarden las instrucciones actualizadas para el manejo de restauraciones?

SI () NO ()

En el momento que se hacen cambios o correcciones a los programas y/o archivos se deben tener las siguientes precauciones:

1) Las correcciones de programas deben ser debidamente autorizadas y probadas. Con esto se busca evitar que se cambien por nueva versión que antes no ha sido perfectamente probada y actualizada.

2) Los nuevos sistemas deben estar adecuadamente documentados y probados.

3) Los errores corregidos deben estar adecuadamente documentados y las correcciones autorizadas y verificadas.

Los archivos de nuevos registros o correcciones ya existentes deben estar documentados y verificados antes de obtener reportes.

PROCEDIMIENTOS DE RESPALDO EN CASO DE DESASTRE

Se debe establecer en cada dirección de informática un plan de emergencia el cual ha de ser aprobado por la dirección de informática y contener tanto procedimiento como información para ayudar a la recuperación de interrupciones en la operación del sistema de cómputo.

El sistema debe ser probado y utilizado en condiciones anormales, para que en caso de usarse en situaciones de emergencia, se tenga la seguridad que funcionará.

La prueba del plan de emergencia debe hacerse sobre la base de que la emergencia existe y se ha de utilizar respaldos.

Se deben evitar suposiciones que, en un momento de emergencia, hagan inoperante el respaldo, en efecto, aunque el equipo de cómputo sea aparentemente el mismo, puede haber diferencias en la configuración, el sistema operativo, en disco etc.

El plan de emergencia una vez aprobado, se distribuye entre personal responsable de su operación, por precaución es conveniente tener una copia fuera de la dirección de informática.

En virtud de la información que contiene el plan de emergencia, se considerará como confidencial o de acceso restringido.

La elaboración del plan y de los componentes puede hacerse en forma independiente de acuerdo con los requerimientos de emergencia, La estructura del plan debe ser tal que facilite su actualización.

Para la preparación del plan se seleccionará el personal que realice las actividades claves del plan. El grupo de recuperación en caso de emergencia debe estar integrado por personal de administración de la dirección de informática, debe tener tareas específicas como la operación del equipo de respaldo, la interfaz administrativa.

Los desastres que pueden suceder podemos clasificar así:

- a) Completa destrucción del centro de cómputo,
- b) Destrucción parcial del centro de cómputo,
- c) Destrucción o mal funcionamiento de los equipos auxiliares del centro de cómputo (electricidad, aire, acondicionado, etc.)
- d) Destrucción parcial o total de los equipos descentralizados
- e) Pérdida total o parcial de información, manuales o documentación
- f) Pérdida del personal clave
- g) Huelga o problemas laborales.

El plan en caso de desastre debe incluir:

La documentación de programación y de operación.

Los equipos:

El equipo completo

El ambiente de los equipos

Datos y archivos

Papelería y equipo accesorio

Sistemas (sistemas operativos, bases de datos, programas).

El plan en caso de desastre debe considerar todos los puntos por separado y en forma integral como sistema. La documentación estará en todo momento tan actualizada como sea posible, ya que en muchas ocasiones no se tienen

actualizadas las últimas modificaciones y eso provoca que el plan de emergencia no pueda ser utilizado.

Cuando el plan sea requerido debido a una emergencia, el grupo deberá:

Asegurarse de que todos los miembros sean notificados,

Informar al director de informática,

Cuantificar el daño o pérdida del equipo, archivos y documentos para definir que parte del plan debe ser activada.

Determinar el estado de todos los sistemas en proceso,

Notificar a los proveedores del equipo cual fue el daño,

Establecer la estrategia para llevar a cabo las operaciones de emergencias tomando en cuenta:

Elaboración de una lista con los métodos disponibles para realizar la recuperación

Señalamiento de la posibilidad de alternar los procedimientos de operación (por ejemplo, cambios en los dispositivos, sustituciones de procesos en línea por procesos en lote).

Señalamiento de las necesidades para armar y transportar al lugar de respaldo todos los archivos, programas, etc., que se requieren.

Estimación de las necesidades de tiempo de las computadoras para un periodo largo.

Cuando ocurra la emergencia, se deberá reducir la carga de procesos, analizando alternativas como:

Posponer las aplicaciones de prioridad más baja,

Cambiar la frecuencia del proceso de trabajos.

Suspender las aplicaciones en desarrollo.

Por otro lado, se debe establecer una coordinación estrecha con el personal de seguridad a fin de proteger la información.

Respecto a la configuración del equipo hay que tener toda la información correspondiente al hardware y software del equipo propio y del respaldo.

Deberán tenerse todas las especificaciones de los servicios auxiliares tales como energía eléctrica, aire acondicionado, etc. a fin de contar con servicios de respaldo adecuados y reducir al mínimo las restricciones de procesos, se deberán tomar en cuenta las siguientes consideraciones:

Mínimo de memoria principal requerida y el equipo periférico que permita procesar las aplicaciones esenciales.

Se debe tener documentados los cambios de software.

En caso de respaldo en otras instituciones, previamente se deberá conocer el tiempo de computadora disponible.

Es conveniente incluir en el acuerdo de soporte recíproco los siguientes puntos:

Configuración de equipos.

Configuración de equipos de captación de datos.

Sistemas operativos.

Configuración de equipos periféricos.

ANEXO 3

Ejemplo de Propuesta de Servicios de Auditoria en Informática

ANTECEDENTES

(Anotar los antecedentes específicos del proyecto de Auditoria)

OBJETIVOS

(Anotar el objetivo de la Auditoria)

ALCANCES DEL PROYECTO

El alcance del proyecto comprende:

Evaluación de la Dirección de Informática en lo que corresponde a:

Capacitación

Planes de trabajo

Controles

Estándares

Evaluación de los Sistemas

Evaluación de los diferentes sistemas en operación (flujo de información, procedimientos, documentación, redundancia, organización de archivos, estándares de programación, controles, utilización de los sistemas)

Evaluación del avance de los sistemas en desarrollo y congruencia con el diseño general

Evaluación de prioridades y recursos asignados (humanos y equipos de cómputo)

Seguridad física y lógica de los sistemas, su confidencialidad y respaldos

Evaluación de los equipos

Capacidades

Utilización

Nuevos Proyectos

Seguridad física y lógica

Evaluación física y lógica

METODOLOGIA

La metodología de investigación a utilizar en el proyecto se presenta a continuación:

Para la evaluación de la Dirección de Informática se llevarán a cabo las siguientes actividades:

Solicitud de los estándares utilizados y programa de trabajo

Aplicación del cuestionario al personal

Análisis y evaluación de la información

Elaboración del informe

Para la evaluación de los sistemas tanto en operación como en desarrollo se llevarán a cabo las siguientes actividades:

Solicitud del análisis y diseño de los sistemas en desarrollo y en operación

Solicitud de la documentación de los sistemas en operación (manuales técnicos, de operación del usuario, diseño de archivos y programas)

Recopilación y análisis de los procedimientos administrativos de cada sistema (flujo de información, formatos, reportes y consultas)

Análisis de llaves, redundancia, control, seguridad, confidencial y respaldos

Análisis del avance de los proyectos en desarrollo, prioridades y personal asignado

Entrevista con los usuarios de los sistemas

Evaluación directa de la información obtenida contra las necesidades y requerimientos del usuario

Análisis objetivo de la estructuración y flujo de los programas

Análisis y evaluación de la información recopilada

Elaboración del informe

Para la evaluación de los equipos se llevarán a cabo las siguientes actividades:

Solicitud de los estudios de viabilidad y características de los equipos actuales, proyectos sobre ampliación de equipo, su actualización

Solicitud de contratos de compra y mantenimientos de equipo y sistemas

Solicitud de contratos y convenios de respaldo

Solicitud de contratos de Seguros

Elaboración de un cuestionario sobre la utilización de equipos, memoria, archivos, unidades de entrada/salida, equipos periféricos y su seguridad

Visita técnica de comprobación de seguridad física y lógica de la instalaciones de la Dirección de Informática

Evaluación técnica del sistema electrónico y ambiental de los equipos y del local utilizado

Evaluación de la información recopilada, obtención de gráficas, porcentaje de utilización de los equipos y su justificación

Elaboración y presentación del informe final (conclusiones y recomendaciones)

TIEMPO Y COSTO

(Poner el tiempo en que se llevará a cabo el proyecto, de preferencia indicando el tiempo de cada una de las etapas, costo del proyecto)