Capítulo 3
Control en la operación de sistemas de información

En este capítulo se incluye los controles en la planeación y administración de los recursos informáticos, la operación y mantenimiento del hardware y software como función sustantiva del centro de cómputo así como aspectos relacionados con la seguridad.

Introducción

Actualmente se reconoce el valor de la información y se busca el desarrollarla y administrarla como un recurso. Hoy día vivimos en una sociedad basada en la tecnología de la información, las organizaciones dependen de esa tecnología para desarrollar sus actividades, los procesos de la organización se transforman para incrementar su productividad y el éxito se determina por la efectividad con la cual la tecnología de información es utilizada.

Por lo anterior administrar los sistemas de información y demás recursos informáticos resulta esencial, ya que integra a la gran variedad de elementos y habilidades utilizadas en la creación, almacenamiento y distribución de información, cumpliendo con su propósito de resolver problemas, liberar la creatividad e incrementar la productividad en el personal.

La tecnología de la información ofrece productos a tal velocidad que no permite su fácil y rápida asimilación por parte de la organización, lo que evita que dicha tecnología se aproveche apropiadamente, el administrador de los servicios informáticos manejará como elementos clave de su actividad profesional la integración y alineación de estrategias, cultura organizacional, habilidades, tecnologías, sistemas, procesos, tareas y resultados.

Por lo anterior es importante proveer los fundamentos para la administración integral de los recursos informáticos, que incluyan los controles en la operación y mantenimiento del hardware y software, relación con el personal informático como función sustantiva del centro de cómputo así como aspectos relacionados con la seguridad.

II.3.1. Planeación y administración de recursos.

Fuente: David H. Li, "Auditoría en centros de cómputo: Objetivos, lineamientos y procedimientos", 1ª Ed. Trillas, México, 1992

- Presupuesto anual de operación para sistemas de información.
- Plan de adquisición de equipo.
- Evaluación del rendimiento del equipo.

Consideraciones para la Normatividad

Fuente: Aguilar Castillo Gildardo, "Apuntes para la materia Administración de Recursos Informáticos", Facultad de Estadística e Informática, Universidad Veracruzana. México, 1998

Presupuesto anual de operación para sistemas de información.

Deben planearse y administrarse los recursos adecuados para apoyar los objetivos del procesamiento de información. Debe elaborarse el presupuesto anual de operación para estar en condiciones de desarrollar y después operar los sistemas de información bajo las siguientes consideraciones:

- Se debe preparar y aprobar un presupuesto de operación para los centros de procesamiento de información separando las diferentes partidas presupuestales de los recursos de cómputo.
- Deben participar las áreas que componen la estructura orgánica, tales como, sistemas, programación, operación y control de la información. [33]
- Debe ser aprobado por el jefe de Área de Informática y por la gerencia de alto nivel que corresponda.
- Se deben definir partidas presupuestales tales como:
  - Adquisición, mantenimiento y arrendamiento de equipo de cómputo.
  - Adquisición y mantenimiento de software.
  - Outsourcing.
  - Gastos de servicios de personal.
  - Capacitación y desarrollo.
  - Gastos de telecomunicaciones e Internet.
  - Gastos de servicios de conservación de inmuebles.
  - Adecuación de áreas e instalaciones.
  - Controles de seguridad.
  - Adquisición, mantenimiento y arrendamiento del equipo auxiliar.
  - Adquisición y conservación del equipo de oficina.
  - Material de oficina.
  - Impresos y papelería.
  - .....

[33] Se citan algunos nombres de las diferentes áreas que podrían conformar un centro de computo, sin embargo estas pueden variar dependiendo de la estructura orgánica y del modo de procesamiento.

Plan de adquisición de equipo.

- Este plan deberá reflejar los requerimientos a corto plazo y las necesidades a largo plazo del centro de cómputo tomando en consideración las perspectivas de obsolescencia tecnológica y nuevas instalaciones.
- Considerar las especificaciones de software y hardware, tiempo de entrega, instalación y soporte técnico, así como compromisos con el usuario.

Evaluación del rendimiento del equipo

- Desarrollar un plan de rendimiento del equipo para obtener datos históricos de los registros de fallas, reporte de los mantenimientos preventivos y correctivos en otras instalaciones.
- Calcular la oferta y la demanda de cada una de las configuraciones a fin de determinar el correcto uso del recurso informático.

II.3.2 Administración de la operación de sistemas de cómputo en producción.

Fuente: David H. Li, "<u>Auditoría en centros de cómputo: Objetivos, lineamientos y procedimientos</u>", 1ª Ed. Trillas, México, 1992

- Programas de cargas de trabajo.
- Administración del personal.[34]
- Calendario de mantenimiento.
- Evaluación de la efectividad de la calendarización.
- Programación con cambios de recursos.
- Contabilidad de los procesos.
- Procedimientos de facturación para el usuario.
- Asignación de las responsabilidades del almacenamiento de datos.
- Sistema de administración de archivos.
- Revisión de operaciones.
- Documentación de los procedimientos de operaciones.

[34] Este temas se trata mas ampliamente en la sección; I.1.4 Responsabilidades organizacionales y administración de personal, Pág. 9 de esta antología.

Consideraciones para la Normatividad

Fuente: Aguilar Castillo Gildardo, "Apuntes para la materia Administración de Recursos Informáticos", Facultad de Estadística e Informática, Universidad Veracruzana. México, 1998

Los recursos de cómputo para operar sistemas de información deben utilizarse en forma efectiva, manteniendo un programa de producción, proporcionando los controles de entrada y salida adecuados, resguardando los archivos de datos en almacenamientos seguros.

Programas de cargas de trabajo.

- Las tareas deben ser programadas para promover el uso eficiente de las instalaciones y el cumplimiento de los requerimientos del usuario.
- Las aplicaciones deberán ser calendarizadas en función de las fechas límites de: entrada de datos, los tiempos de preparación, tiempos estimados de proceso y las fechas límites de salida de datos y entrega.
- Se deben identificar las aplicaciones de alta prioridad y riesgo con el fin de adecuar su procesamiento a la calendarización normal.
- Evaluar el calendario de proceso para mantener una distribución de carga de trabajo constante.
- Considerar los calendarios de mantenimiento preventivo a fin de mantener la disponibilidad del equipo para cumplir con los compromisos de procesamiento.
- Implantar por turno un registro de incidencias y problemas en cada área funcional y revisar las observaciones a fin de determinar el efecto que puedan tener en la programación de recursos.
- Los usuarios deben participar en la preparación de calendarios.

Administración del personal.

- Es importante mantener actualizado el organigrama del centro de cómputo, identificando cada área en la estructura, definir sus funciones y tramo de control.
- La responsabilidad de cada área funcional debe estar asignada al personal con mayor capacidad y que reúna el perfil definido en la evaluación de puestos.
- La plantilla de personal debe mantenerse el equilibrio de plazas autorizadas y ocupadas para proporcionar un adecuado apoyo a cada función del centro de procesamiento de datos.
- Debe cumplirse fielmente con el procedimiento de selección de personal a fin de encontrar el personal adecuado para el puesto asignado.
- Deben establecerse estrategias de capacitación y desarrollo a fin de mantener un nivel alto de capacidad y motivación.
- Implementar un sistema de valoración de méritos que permita reconocer el nivel de actuación de cada empleado y reconocerle su productividad.

Calendario de mantenimiento.

- Debe diseñarse un calendario para la realización de los mantenimientos preventivos en coordinación con el proveedor y/o soporte técnico.
- Debe incluirse en el plan de trabajo general del centro de cómputo el calendario de mantenimiento preventivo de los equipos.

- Se deben implementar procedimiento de control de fallas, que permita conocer la frecuencia con que se presentan estas incidencias y en que dispositivo en particular ocurren.
- Se deben definir los diferentes niveles de mantenimiento preventivo para cada equipo y la frecuencia de su aplicación.
- Considerar en los mantenimientos a los equipos de cómputo, equipos auxiliares, instrumentos de medición e instalaciones.

Evaluación de la efectividad de la calendarización.

- Entrevistas periódicas con el encargado del área de operación y/o usuario a fin de determinar si se mantienen los registros y bitácoras que permita determinar el desempeño actual de cada sistema en relación con el cumplimiento de calendarios.
- Analizar en coordinación con los usuarios las fallas recurrentes y que puedan afectar el cumplimiento de calendarios.
- Investigar las causas de los atrasos en cuanto a procesos, captura e identificar las causas.
- Revisar las estadísticas de tiempos de respuesta de los sistemas en línea y determinar posibles causas de fluctuaciones significativas.

Programación con cambios de recursos.

- El impacto de un cambio en el equipo o en el software debe reflejarse en los calendarios de proceso.
- Se debe considerar el tiempo requerido para la instalación adecuada y la prueba del nuevo equipo o software.

Contabilidad de los procesos.

- Debe existir un registro del desempeño exacto de todos y cada uno de los procesos del centro de cómputo, a través de implementar bitácoras de control que muestren el consumo de recursos así como las incidencias que se presenten proceso a proceso.
- En las bitácoras, se debe considerar el número de función y proceso, nombre, hora de inicio, hora de término, duración, dispositivos de entrada, dispositivos de salida y cifras de control y deben implementarse en todas las instalaciones y para todos los sistemas aplicativos por separado.

Procedimientos de facturación para el usuario.

- Deben ser diseñados para incrementar el uso adecuado de los recursos de cómputo y para que los departamentos usuarios tengan un trato justo y equitativo de acuerdo a sus necesidades.
- Revisar junto con el usuario el procedimiento de cobro por los servicios de sistemas y si esta satisfecho con éste.

Asignación de las responsabilidades del almacenamiento de datos.

Los dispositivos de almacenamientos representan, para cualquier centro de cómputo archivos extremadamente importantes cuya pérdida parcial o total podría tener repercusiones muy serias, no solo en la unidad de informática, sino en la dependencia de la cual se presta servicio.

El Área de informática -bien administrada- debe tener perfectamente protegidos los dispositivos de almacenamiento de datos, además debe mantener registros sistemáticos de la utilización de estos archivos, de modo que sirvan de base a los programas de limpieza, principalmente en el caso de las cintas. Un manejo adecuado de estos dispositivos permitirá una operación más eficiente y segura, mejorando además los tiempos de procesos.

- Debe asignarse la responsabilidad del almacenamiento de datos y deben establecerse los procedimientos necesarios de registro que garanticen la protección del contenido de las bibliotecas. [35]
- La custodia de los archivos deberá ser ubicada en un lugar y bajo responsabilidad de personal independiente a los operadores del centro de cómputo y de los programadores.
- Deberá administrarse la información en bibliotecas de programas, archivos, de producción así como de prueba.
- Se deben crear procedimientos de seguridad para controlar el acceso y uso de la información en las diferentes bibliotecas.
- El área de almacenamiento deberá estar protegida contra situaciones de desastre o de sabotajes.
- Deberán existir instalaciones de almacenamiento fuera del centro de cómputo, para dar apoyo en situaciones críticas, conteniendo en éstas los respaldos de archivos y bibliotecas del centro de cómputo.

Sistema de administración de archivos.

- Los archivos de cómputo deben ser inventariados y controlados a través de registros específicos, que contengan; nombre del archivo, fecha de creación, programa que lo genera, vigencia de su información, total de registros, tipo de organización, método de acceso, etc.

[35] También suele reconocérseles con el nombre de ficheros, carpetas, directorios.

Revisión de operaciones.

- Implementar procedimientos de trabajo para las operaciones del centro de cómputo a fin de asegurar que éstas se realicen eficientemente.
- Todos los procedimientos deberán estar debidamente documentados en los manuales de procedimientos.
- El manual de procedimientos es el que señala el orden preciso que se debe seguir para ejecutar actividades de trabajo, este tipo de manual describe en secuencia lógica, los distintos pasos que componen un proceso, señalando generalmente quién, cómo, dónde, cuándo y para qué han de realizarse.
- Todo manual de procedimientos debe estar elaborado de acuerdo a los estándares establecidos por la organización y es recomendable que contemplen reglas de ejecución, diagramas de operación y formatos.

Documentación de los procedimientos de operaciones.

- Un manual de procedimientos generalmente contiene la descripción de las operaciones que deben seguirse en la realización de las funciones de un centro de cómputo, tanto en sus diferentes áreas como en el enlace con los usuarios.
- Los procedimientos deben incluir los puestos o unidades administrativas que intervienen, detallando su responsabilidad y participación.
- Un manual de procedimientos, persigue los siguientes objetivos:
  1. Uniformar y controlar el cumplimiento de las rutinas de trabajo y evitar su alteración arbitraria.
  2. Simplifica la determinación de responsabilidades por fallas o errores.
  3. Facilita las labores de evaluación y control.
  4. Enseña el trabajo a nuevos usuarios.
  5. Aumenta la eficiencia de los empleados.
  6. Ayuda a la coordinación de trabajo entre puestos y áreas.
  7. Es la base para el mejoramiento de métodos y procedimientos.

El manual de procedimientos generalmente contiene:

a) Identificación y autorizaciones
b) Índice
c) Introducción
d) Objetivo
e) Políticas
f) Procedimientos
g) Formatos
h) Instructivos de llenado

a) Identificación y autorizaciones. En este apartado se incluyen los datos de : Nombre oficial del organismo, título del manual, nombre completo del procedimiento al que se refiere, área que lo elaboró, y a quién va dirigido, lugar y fecha de elaboración y nombre y firma de los jefes que lo autorizan.

b) Índice. Es una relación de los capítulos que constituyen la estructura del documento.

c) Introducción. Se explica al lector a quién va dirigido el manual el porque se realiza, como se usará, cómo y cuando se harán las revisiones y actualizaciones, además de una breve descripción de cada uno de los capítulos y su finalidad.

d) Objetivo. Se describe cual es la finalidad que se persigue al documentar los procedimientos, así como los beneficios que esto puede aportar.

e) Políticas. Son las guías de acción y de pensamiento que garanticen la correcta aplicación del procedimiento, las políticas se pueden separar en generales para el organismo y específicas para cada una de las áreas que participan en el procedimiento.

f) Procedimientos. Se presenta por escrito en el formato de libreto, en forma narrativa y secuencial, cada una de las actividades que hay que realizar, explicando detalladamente en qué consisten, cuándo, cómo, con qué y dónde, señalando a los responsables de su ejecución.

Cuando la descripción del procedimiento sea general y comprenda diferentes áreas, debe indicarse para cada actividad, la unidad administrativa encargada de su ejecución, si se trata de una descripción detallada dentro de una unidad administrativa, debe indicarse el puesto del responsable de la ejecución de cada operación. Es conveniente relacionar las diferentes operaciones de manera que faciliten su comprensión e identificación aún en los casos de varias alternativas en una misma operación.

g) Formatos. Las formas impresas que se utilizan dentro de un procedimiento deben también formar parte del manual, incluyéndolas como un apéndice del mismo. En la descripción de la actividad que impliquen el uso de un formato, debe hacerse referencia a éste, utilizando para ello números indicadores.

h) Instructivos de llenado. Todos los formatos que se utilicen en el procedimiento, deben ir acompañados de un instructivo de llenado que garantice el correcto requisitado de éstos.

El instructivo debe contener los datos generales de la forma, como su nombre, su objetivo, su clave, quién la elabora, en cuantos tantos, cual es su distribución, alguna política de control y la vigencia de su información, también debe contener las instrucciones de llenado, es decir, relacionar campo por campo detallando las características de la información que deben contener.

Metodología para la elaboración de un Manual de Procedimientos

La elaboración de un manual de procedimientos permite el logro de los siguientes objetivos :

1. La reglamentación de los procedimientos, para que los mismos se realicen conforme a la descripción del manual.
2. El establecimiento de políticas de trabajo, que mediante la aplicación de los procedimientos se asegure la correcta ejecución de las operaciones.
3. El mejoramiento de los métodos y procedimientos de trabajo.

Antes de iniciar la elaboración de un manual de procedimientos, es indispensable caracterizar en forma precisa la necesidad del mismo, ya que el análisis para su elaboración es muy detallado debido a que cada una de las actividades que conforman un procedimiento deben ser considerada. La necesidad de elaborar un manual de este tipo se justifica cuando :

1. Existen trámites de cierto grado de complejidad, por lo que es necesario la descripción precisa de cada uno de sus pasos, de tal manera que sea fácil su consulta y aclaración de posibles dudas.
2. Se requiere asegurar la uniformidad en el desarrollo de los trámites y procedimientos para un evento repetitivo, para lo cual se hace indispensable contar con descripciones escritas del mismo.
3. Se requiere emprender tareas de simplificación del trabajo, tales como estudios de tiempos y movimientos, delegación de autoridad, facultad para la toma de decisiones, etc.
4. Es necesario apoyar la capacitación del personal para el desarrollo de determinadas actividades, tramites o procedimientos.
5. Cuando se desee establecer un nuevo sistema de información o bien modificar el ya existente y se necesite conocer el flujo que actualmente sigue la información.

<u>Aspectos metodológicos generales:</u>

Debe ser el titular de cada unidad administrativa quién de la aprobación del procedimiento para garantizar el mejor funcionamiento de su área de trabajo y su relación con otras áreas. Es recomendable determinar primeramente:

a) Los tipos de manuales con que cuenta el personal .
b) El grado de utilización de los manuales existentes.
c) Los comentarios respecto a los manuales existentes.
d) Las área de trabajo donde se originen problemas por falta de manuales.

Una vez que se han determinado los manuales requeridos, así como los recursos y el tiempo necesario para su elaboración, es conveniente iniciar la etapa de recolección de la información en la siguiente forma:

a. Elaborar una serie de oficios, dirigidos a las autoridades de la unidades administrativas de las que se requiere apoyo y cooperación para la elaboración del manual.

b. Aplicar las técnicas de recopilación que mas convengan al procedimiento dependiendo de la fuente.

- √ Documentos.- Las técnicas de investigación documental son particularmente útiles inicialmente, ya que permiten obtener la información necesaria para la elaboración de manuales, se deben revisar : Leyes, Reglamentos, Normatividad, Decretos, Acuerdos, Circulares, Manuales, Instructivos, Diagramas, etc.
- √ Personas.- Todas las personas involucradas en los procedimientos tienen algo que decir, y si se considera que éstas son las usuarias del procedimiento es conveniente su opinión, se recomienda la aplicación de las siguientes técnicas : *Entrevista, Cuestionario*, *encuesta, sugerencias, quejas, etc.*
- √ Entorno.- El ambiente en que se implantará el procedimiento, constituye una fuente de información importante, pues de algún modo se recaba información que no se dio en la entrevista o en el cuestionario, además de que, puede comprobarse la información obtenida, la técnica más recomendada es la *Observación*.

c. Una vez que la información ha sido recopilada y registrada, se inicia la etapa del procesamiento de la misma, lo que se considera como la integración propiamente dicha del proyecto de manual.

d. Lo primero que debe hacerse es un análisis y depuración de la misma, con el objeto de facilitar el manejo y ordenamiento de la información que es general, especifica y de apoyo.

e. Es conveniente analizar cuidadosamente el formato con el que debe presentarse cada manual, ya que de ello depende en gran medida la facilidad de lectura, consulta, estudio y conservación, además de permitir hacer referencias rápidas y precisas, considerar la forma de diagrama, de texto, libreto y combinado.

f. Es conveniente diseñar formatos[36] que permitan estandarizar los procedimientos, ya que estos aportan información necesaria para lograr los objetivos, fundamentan la toma de decisiones, controlan y mejoran las operaciones.

[36] Un formato es una hoja de papel en la cual existe información impresa y espacios reservados en blanco para el registro de datos.

g. Cuando los procedimientos que se documentan involucran mas de dos unidades administrativas dentro de la organización, es conveniente elaborar un diagrama de flujo para esquematizar de forma más objetiva el recorrido de la información entre las áreas, esto facilita la comprensión del proceso.

h. Una ves que se cuenta con el proyecto del manual, es necesario someterlo a una revisión final, el propósito será verificar que la información contenida sea la necesaria, esté completa y que corresponda a la realidad, además de comprobar que no tiene contradicciones, ni lagunas o traslapes entre las diferentes áreas o puestos.

i. Después de la revisión, se debe someter a la aprobación de las autoridades correspondientes, preferentemente se debe coordinar una reunión de trabajo para aclarar y tomar nota de todas las observaciones que sobre el documento se puedan realizar, el objeto es contar con las firmas de los funcionarios que le darán la legalidad al documento.

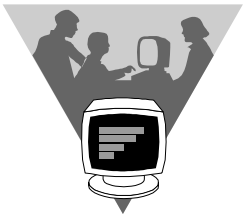
j. Debe ser el departamento de Informática quien coordine la reproducción, difusión, actualización y control de los documentos generados como resultado de la implantación de un sistema de cómputo, en procedimientos como enlace con los usuarios y al uso de los sistemas.

k. Una vez que el manual ha sido elaborado, autorizado e impreso, se debe realizar su difusión y distribución, es recomendable organizar reuniones de trabajo con el personal involucrado en los procedimientos para instruirlos sobre el uso del documento así como las nuevas políticas de trabajo que se implementarán.

l. La utilidad de los manuales radica en la veracidad de su información, por lo que es recomendable, mantenerlos permanentemente actualizados a través de revisiones periódicas y de ser posible diseñar una normatividad para las modificaciones que se puedan sugerir.

m. Se recomienda que cuando alguna área administrativa necesite realizar cambios en algún procedimiento, presente su petición al área de Informática para verificar sus propuestas, en caso de proceder ésta, realizar las adecuaciones pertinentes en todo el documento y difundir su actualización, si no procede explicar la causa por la que se rechaza su petición.

Ejemplo de un ***manual de procedimientos*** de enlace con los usuarios.



INSTITUTO MEXICANO DE INFORMATICA
Subdirección General de Finanzas

Jefatura de Servicios Informáticos

IDENTIFICACIÓN Y AUTORIZACIONES

Nombre del documento: PROCEDIMIENTO DE ENLACE CON LOS USUARIOS

Síntesis del documento: Establece los lineamientos en cuanto a la recepción por parte de las áreas usuarias, de la documentación fuente para captura y/o medios magnéticos para conversión, así como la entrega de productos resultantes del procesamiento de datos.

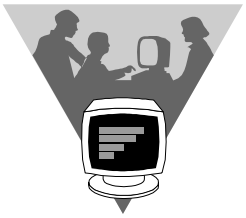
Elaborado por:	Dirigido a :
Departamento de normas y evaluación Departamento de apoyo a la operación	Departamento de Atención a Usuarios Todas las áreas usuarias del servicio

Autorizaciones :

Ing. Gildardo Aguilar Castillo Jefe de los Servicios Informáticos	L.A.E. Doralí Aguilar Sánchez Jefe de los Servicios Administrativos

Clave interna : J.S.I.2202

Fecha de emisión : Nov., 21'2000



INSTITUTO MEXICANO DE INFORMATICA
Subdirección General de Finanzas

Jefatura de Servicios Informáticos

CONTROL DE POSEEDORES

Nombre del documento: PROCEDIMIENTO DE ENLACE CON LOS USUARIOS

Clave interna : J.S.I.2202 Fecha de emisión : Nov., 21'2000

POSEEDOR

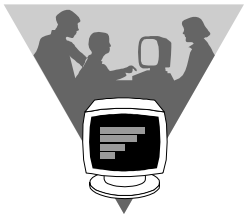
Nombre del poseedor: Ing. Gildardo Aguilar Sánchez

Puesto : Jefe del Departamento de Atención a Usuarios

Dependencia : Jefatura de Servicios Informáticos

Localidad : Xalapa, Veracruz

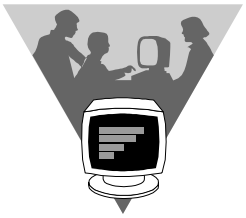
Fecha y firma de recepción :



INSTITUTO MEXICANO DE INFORMATICA
Subdirección General de Finanzas

Jefatura de Servicios Informáticos

INDICE



INSTITUTO MEXICANO DE INFORMATICA
Subdirección General de Finanzas

Jefatura de Servicios Informáticos

INTRODUCCION

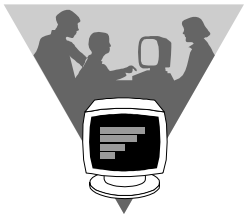
El presente documento se ha desarrollado con el propósito de establecer una adecuada coordinación entre el departamento de Atención a Usuarios y las áreas usuarias que utilizan los servicios de procesamiento de datos para los sistemas implantados.

Primeramente se presentara el objetivo que se pretende al implantar este procedimiento, así como sus políticas de trabajo generales y especificas para cada área participante, posteriormente se describirá el procedimiento en forma detallada y se anexarán los formatos que se deben utilizar con su correspondiente instructivo de llenado.

Esto permitirá homogeneizar los trámites para la recepción de información, captura, proceso y entrega de productos.

OBJETIVO

Contar con una herramienta de trabajo eficaz que permita al Departamento de Atención a Usuarios, establecer la coordinación con las áreas usuarias para otorgar el servicio de procesamiento de datos de una manera eficiente.



INSTITUTO MEXICANO DE INFORMATICA
Subdirección General de Finanzas

Jefatura de Servicios Informáticos

POLITICAS

Generales

- Las áreas involucradas en este procedimiento deberán cumplir con las fechas calendarizadas para la entrega de información, captura, proceso y entrega de productos.

- Etc...

Específicas para el usuario

- Solicitará al Departamento de Atención a Usuarios, los servicios de captura, conversión de dispositivos magnéticos, proceso de acuerdo a los lineamientos establecidos en el presente documento.

- Entregará la información fuente para su captura, de acuerdo al calendario correspondiente, debidamente lotificada.

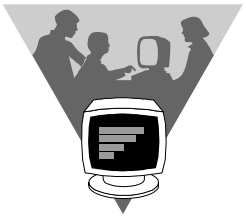
- Etc..

Específicas para informática

- Notificará al usuario la entrega de sus productos al momento que el área de proceso se lo notifique.

- Respetará la confidencialidad y seguridad de la información de acuerdo a la normas establecidas.

- Etc..



INSTITUTO MEXICANO DE INFORMATICA
Subdirección General de Finanzas

Jefatura de Servicios Informáticos

PROCEDIMIENTO

Responsable	No.	Descripción de la actividad
Áreas Usuarias	1	Prepara, lote de documentos fuente para su captura, máximo 300 registros por lote.
	2	Requisita la forma "Orden de Trabajo de captura" de acuerdo a su instructivo de llenado. (anexo 1)
	3	Entrega al Área de Control y Enlace de Informática, los documentos debidamente lotificados junto con la orden de trabajo en original y copia.
Área de Control y Enlace Informático	4	Recibe por parte del Usuario, documentos y orden de trabajo de acuerdo a los calendarios establecidos.
	5	Revisa el correcto llenado de la forma "Orden de Trabajo de captura" y que coincida con los documentos que ampara.
		Es correcto?
	6	**No.-** Aclara con el usuario las discrepancias encontradas y en su caso devuelve al usuario los documentos y la orden de trabajo, indicándole la inconsistencia en el requisitado. **continúa en el paso 1**
	7	**Si.-** Requisita en el original y copia de la "orden de trabajo de captura" la siguiente información, número de folio, fecha, hora y sello de recepción.
	8	Registra en el "Control de entradas / salidas" la información correspondiente a la solicitud.
	x	Etc.....

Formas e instrucciones de llenado (ejemplo)

<table>
<tr><td colspan="2">ATENCION A FALLAS DE HARDWARE</td><td colspan="2">TURNO:
1</td><td>FECHA:
2</td><td>FOLIO:
3</td></tr>
<tr><td colspan="2" rowspan="2">Área afectada:
4</td><td colspan="2" rowspan="2">Equipo y Unidad:
5</td><td colspan="2">HORA DE LA FALLA</td></tr>
<tr><td>Detectada</td><td>Reportada</td></tr>
<tr><td colspan="2">Reportó: (usuario)
6</td><td colspan="2">Recibió reporte: (Sop.Téc)
7</td><td>8</td><td>9</td></tr>
<tr><td>Día:</td><td>Reportó:</td><td colspan="2">A: Técnico o proveedor</td><td>Núm.Repo</td><td>Hora</td></tr>
<tr><td></td><td></td><td colspan="2"></td><td></td><td></td></tr>
<tr><td>10</td><td>11</td><td colspan="2">12</td><td>13</td><td>14</td></tr>
<tr><td></td><td></td><td colspan="2"></td><td></td><td></td></tr>
<tr><td colspan="6">Descripción de la falla:</td></tr>
<tr><td colspan="6"></td></tr>
<tr><td colspan="6">15</td></tr>
<tr><td colspan="6"></td></tr>
<tr><td colspan="6"></td></tr>
<tr><td colspan="6">Documentación que la acompaña:
16</td></tr>
<tr><td colspan="3" rowspan="2">Nombre y firma del Técnico de servicio:
17</td><td colspan="3">F e c h a y H o r a:</td></tr>
<tr><td>Presentó:
18</td><td>Inició:
19</td><td>Terminó:
20</td></tr>
<tr><td colspan="6">Solución de la falla:</td></tr>
<tr><td colspan="6"></td></tr>
<tr><td colspan="6">21</td></tr>
<tr><td colspan="6"></td></tr>
<tr><td colspan="3">Técnico que entrega: (nombre y firma)
22</td><td colspan="3">Operador que recibe: nombre y firma)
23</td></tr>
</table>

INSTRUCTIVO DE LLENADO

Nombre de la forma:	Atención a fallas de hardware
Clave o identificación:	DI004
Objetivo:	Controlar por parte del área de Soporte técnico los problemas de hardware que se presenten en los equipos de cómputo hasta su solución final.
Generado por:	Responsable del equipo de cómputo y complementado por el Técnico de servicio.
Frecuencia de elaboración:	Variable
Número de tantos:	Original
Distribución:	El original para la atención y archivo del área de Soporte Técnico.
Políticas de control:	Deberá considerarse el número de folio como prioridad de atención y no archivarse hasta su total atención.
Vigencia:	Tres meses.

INSTRUCCIONES DE LLENADO

1.- Turno:	Turno correspondiente al momento que se presentó la falla. (Mat. Vesp. Noct.)
2.- Fecha:	Día, mes y año en que se presentó la falla.
3.- Folio:	Número consecutivo correspondiente, generado para cada instalación de cómputo.
4.- Área afectada:	Número o nombre dela instalación de cómputo en dónde se encuentra el equipo afectado que se reporta.
5.- Equipo y unidad:	Modelo del equipo que presentó la falla y del dispositivo afectado.
6.- Hora de falla detectada:	Hora y minutos en que se inició la falla.

7.- Hora de falla reportada:	Hora y minutos en que se informó al centro de servicios del proveedor.
8.- Reportó: (nombre del usuario)	Nombre del responsable del equipo de cómputo que está reportando al área de apoyo a instalaciones.
9.- Recibió reporte: (personal de Sop. Téc.)	Nombre de la persona que recibió el reporte en el área de Soporte Técnico del centro de cómputo.
10.- Día:	Día en que se reporta la falla al proveedor o Técnico.
11.- Reportó:	Nombre de la persona que reportó ese día el equipo al técnico o proveedor.
12.- Técnico o proveedor:	Nombre del técnico o empleado que recibe el reporte en el centro de servicio.
13.- Núm. de reporte:	Número que el técnico o proveedor asigna al reporte.
14.- Hora:	Hora en que quedó registrado el reporte
15.- Descripción de la falla:	Síntoma o falla que esta presentando el equipo.
16.- Doc. que acompaña:	Reporte técnico del proveedor.
17.- Técnico:	Nombre y firma del técnico que se presenta a solucionar la falla.
18.- Fecha:	Fecha en que se presentó el técnico para atender la falla.
19.- Hora de inicio:	Hora y minutos en que el técnico empieza la atención de la falla.
20-. Hora de término:	Hora y minutos en que el técnico concluye la reparación.
21.- Solución de la falla:	Las acciones que realizó el técnico para dar solución a la falla.
22.- Técnico que entrega:	Nombre y firma del técnico que atendió la falla.
23.- Operador que recibe:	Nombre y firma del operador o responsable que recibe de conformidad el equipo.

II.3.3 Administración del Software.

Fuente:http://www.microsoft.com/Argentina/ PUBLIC/KIT_BASE/LICENCIAMIENTO/LICSEMGT/Contents/contents.htm

El Software Como una Inversión

La inversión en software es para una organización una parte crítica en su base total de activos[37] El software es muchas veces un componente crucial para ayudar a la organización a cumplir con su objetivo y representa cada año un componente importante en los presupuestos departamentales y de tecnología informática.

En sólo una década, las corporaciones se han enfrentado a la revolución de las PCs, que descentralizó el poder de la computación y ubicó las decisiones críticas de la tecnología informática en manos de los usuarios individuales, luego ocurrió la revolución de las telecomunicaciones que integró a las PCs y a los servicios de telefonía, descentralizando aún más el control.

A medida que los sistemas de computación proliferaron en la organización, la demanda de nuevas herramientas de hardware y software incrementó sustancialmente el dinero gastado en tecnología. Al mismo tiempo, se debilitaron los controles internos y se redujo el personal de informática centralizado en los centros de cómputo.

La imposibilidad de determinar qué inversiones posee la organización en materia de software y donde están ubicadas, ha contribuido a generar los siguientes problemas:

- La reducción en activos corporativos a través de la pérdida, agotamiento o robo.
- La inseguridad en el uso del software.
- La introducción de los virus en las computadoras y otras amenazas al ambiente de la tecnología informática.
- El incremento de los costos de integración como resultado de la incompatibilidad de los sistemas, diferentes versiones de software y diferentes plataformas de software.
- Incremento en gastos de entrenamiento, soporte y servicios.
- Incremento del riesgo de multas civiles y penalidades por infringir la ley de propiedad intelectual.

[37] Los Activos son los bienes que posee la Organización.

La implementación de una función para administración de software es la forma más efectiva en relación costo-beneficio para optimizar el retorno de la inversión de la organización en sus activos de software, es un medio para validar la fuerte performance[38] del departamento de informática, satisfacer a los usuarios finales y acumular los beneficios financieros en la organización.

La inversión en software es una inversión en productividad, performance y todos los demás elementos necesarios para alcanzar los objetivos de la organización. La Administración del software también ofrece los siguientes beneficios:

- √ Ahorrar dinero.
- √ Reducir el Costo Total de la Propiedad (CTP).
- √ Manejar el cambio tecnológico.
- √ Reducir las pérdidas por robos y mal uso.
- √ Reducir el riesgo y la responsabilidad.
- √ Mejorar la moral de los usuarios.
- √ Reducir los problemas de comunicaciones y de transferencia de datos.
- √ Justificar las inversiones en mejor tecnología.

Ahorrar dinero.

Sin una administración correcta del software, muchas veces las compañías perderán dinero desde el proceso de compra. Los editores de software generalmente ofrecen descuentos por la adquisición de licencias de software en cantidad. Al comprar el software en grandes cantidades y al centralizar su administración, la organización se beneficia con mejores precios.

Reducir el Costo Total de la Propiedad (CTP).

Las condiciones de uso incluidas en toda adquisición de software afectan sustancialmente el costo total de la propiedad. Este costo se determina por cada elemento de su ciclo de vida y pueden ser tan bajos cuando se consideran los costos asociados con elementos tales como entrenamiento, modificación, mantenimiento, soporte técnico, inventario y cambio de gerenciamiento.

Manejar el cambio tecnológico.

Mientras la posibilidad de obtener buenos precios en las compras por volumen es importante, la organización será capaz de identificar las necesidades de software, tratar con la vida útil de su software cada vez más corta, evitar la obsolescencia y además asegurar que tiene la tecnología que necesita para cumplir con su misión.

Reducir las pérdidas por robos y mal uso.

Las pérdidas del software no son simplemente un problema para la industria del software. Cuando el software y su documentación se pierden o se lo roban, el precio que paga la organización puede ser muy alto.

[38] Performance equivale a desempeño, rendimiento, presencia, funcionamiento, Larousse Diccionario, 1999

Reducir el riesgo y la responsabilidad.

Con el abuso intencionado o negligente de las licencias de software, se puede incurrir en penalidades económicas para la organización, adicionalmente los ejecutivos de la empresa pueden ser incriminados y encarcelados por la infracción de la ley de propiedad intelectual que pueda ocurrir en la organización.

Mejorar la moral de los usuarios.

La mayor fuente de insatisfacción de los usuarios es la frustración con las computadoras, el software, la nueva tecnología y los cuellos de botella en el flujo de trabajo, la administración de software ayuda a la organización a identificar las áreas con problemas y permite que se apliquen sistemas de soporte más efectivos que ayuden a reducir el stress de los usuarios.

Reducir los problemas de comunicaciones y de transferencia de datos.

En las organizaciones donde la tecnología ha proliferado sin controles, los recursos resultantes muchas veces operan en diferentes plataformas (por ejemplo: marketing usa Macintosh, ventas usa PCs), así como también usan diferente software o diferentes versiones del mismo software. Esto puede dificultar la transferencia de documentos y datos de un departamento a otro, aunque esos sistemas estén en la misma red. La administración de software ayuda a estandarizar la tecnología mejorando el flujo de trabajo y la eficiencia.

Justificar las inversiones en mejor tecnología.

Las organizaciones se mueven por los retornos en las inversiones y aquellas que no pueden cuantificar una inversión (aún cuando claramente existe), pueden verse forzadas a no hacerla, la administración de software permite que la organización entienda mejor el valor que recibe de la tecnología y que pueda dirigir las inversiones en tecnología a las áreas donde pueda incrementar el retorno de la inversión.

Más allá de los beneficios para la organización, los beneficios reales de la administración del Software se notarán en el área de Informática, particularmente en los grupos de desarrollo y soporte técnico de la siguiente manera:

- √ Reducir sustancialmente el soporte y los
- √ requerimientos de entrenamiento.
- √ Facilitar el mantenimiento de la red.
- √ Reducir o eliminar los virus de las computadoras.
- √ Aligerar la carga de administración de sistemas.
- √ Mejorar la evaluación del nuevo software.
- √ Evitar el "Síndrome de Grinch".

Reducir sustancialmente el soporte y los requerimientos de entrenamiento.

Como el proceso ayuda a estandarizar la tecnología, los usuarios se auto apoyarán cada vez mas y entre ellos, y menos en el personal de soporte técnico, esto libera al personal de informática para otras responsabilidades.

Facilitar el mantenimiento de la red.

La actividad primaria de la mayoría de los departamentos de informática es el mantenimiento de la red, una tarea por demás difícil debido a que los programas no son compatibles con la red o que no funcionan en un ambiente de red. La identificación y eliminación de estos programas reducirá significativamente el mantenimiento de la red y los requerimientos de operación.

Reducir o eliminar los virus de las computadoras.

La causa más importante de los ataques de virus es el software introducido desde afuera de la organización, muchas veces a través de copias no autorizadas. Una administración de software efectiva ayudará a reducir la interacción con el software no autorizado, y por lo tanto reducir el riesgo de ataques de virus.

Aligerar la carga de administración de sistemas.

Mas allá de las demandas del mantenimiento de la red, el personal de informática emplea mucho tiempo en tareas que devuelven un mínimo retorno en inversión. Los ejemplos incluyen la administración de los directorios y carpetas y la estandarización de documentos y formatos. La administración de software permite a las organizaciones reducir o eliminar muchas de estas tareas.

Mejorar la evaluación del nuevo software.

Muchos sistemas de computación y redes están atascados con software que se usa raramente. Los escritorios están muchas veces abarrotados de hardware que es obsoleto o no es útil para las necesidades de la organización, la administración de software ayuda a deshacerse de estas obstrucciones, y por otro lado reduce la necesidad de soporte. Adicionalmente, se diseñarían procedimientos mas sencillos para determinar cual es la tecnología actual y cual es la que mejores beneficios le da a la organización.

Evitar el "Síndrome de Grinch."

Muchas veces, los usuarios ven al Departamento de Informática como el cuello de botella que no aprobará nuevas adquisiciones, no ofrece el software más moderno y no responderá inmediatamente, además no soporta las necesidades de los usuarios. Una buena administración motiva a los informáticos a generar un mejor entendimiento del valor del software y su uso, adicionalmente ayuda a formar una mejor imagen departamental e incrementar la moral del personal.

Beneficio a los Usuarios

Una sólida revisión de la tecnología existente y la implementación de estándares en la organización, no solamente beneficiará a la Dirección y al Departamento de Informática, sino que también ayudará a los usuarios a:

Identificar la necesidad de mejores herramientas

El personal de Informática está generalmente más capacitado que los usuarios y otros empleados para determinar la necesidad de tecnología nueva o diferente, una buena administración de software ofrece las políticas y procedimientos para que el usuario pueda solicitar nueva tecnología y no solicitar adquisiciones motivadas por empleados frustrados por la lentitud de la red o impresora, o por la necesidad de una impresora a color, sin entender las causas de fondo ni sus soluciones y beneficios financieros.

Reducir la dependencia del personal de Soporte Técnico.

No importa lo bien equipado que esté, el personal de soporte nunca será capaz de resolver cada problema instantáneamente. Un procedimiento de atención a fallas bien documentado abre nuevos caminos para el soporte, porque permite a los usuarios acceder a los servicios de soporte técnico de los proveedores de hardware y software involucrados.

Clarificar las normas legales para el uso de la tecnología.

Algunos programas de software permitirán a los usuarios usar legalmente una copia en sus computadoras portátiles para proyectos relacionados con su trabajo. Al saber exactamente cuales son las reglas, se pueden reducir los riesgos de responsabilidad de los usuarios de la organización.

Entender los acuerdos de Licencia

Ayudar a justificar las nuevas adquisiciones.

No hay nada más frustrante para el usuario que no poder obtener la tecnología que creen que necesitan. Sin un marco de trabajo documentado para la adquisición y uso de software, los departamentos de informática están forzados a hacer juicios subjetivos y muchas veces erróneos. La administración del software ayuda a encauzar el sistema de compra, reduciendo las frustraciones de los usuarios, personal de Informática y directivos.

Para una organización tipo, el proceso de administración exitoso de software incluye los siguientes pasos:

1. Formación del equipo de administración de software
2. Determinación de la distribución actual y uso del software (también llamado auditoría de software).
3. Análisis de políticas y procedimientos.
4. Desarrollo de un plan de administración de software basado en la determinación.
5. Implementación y seguimiento del plan.
6. Acciones correctivas y resoluciones
7. Continuación del programa de administración de software.

El Equipo de administración de Software

Las computadoras llegan virtualmente a todos los rincones de una organización, por lo que es importante tener consenso y soporte en toda la organización, especialmente en los niveles de dirección más altos. De otra manera, el personal de informática se arriesga a ser visto como intruso, dominante o fuera de tono.

La forma de obviar este problema es implementar un equipo de administración de software, compuesto por empleados de los departamentos usuarios. La cantidad de miembros del equipo puede variar de una organización a otra, pero un equipo tipo de administración de software puede tener hasta diez miembros, un número mayor puede hacer que las reuniones sean difíciles de manejar, pero menos de cinco puede reducir las oportunidades de un soporte con amplitud de criterio.

Determinación de la distribución actual y uso del software.

Debe haber un claro entendimiento de cómo y dónde utiliza en ese momento el software. Esto requiere una auditoría de activos existentes con una conciliación de licencias y otra documentación de propiedad, deberá incluir también una revisión de los procedimientos de seguridad y recuperación ante desastres de datos, procedimientos anti-virus y otras consideraciones especiales, será necesario buscar cada pieza de software en la organización.

Análisis de Políticas y Procedimientos

El análisis de políticas y procedimientos es un paso esencial para lograr que el proceso de administración de software sea más eficiente. La cantidad de políticas y procedimientos dependerá del tamaño, alcance y cultura de la organización. Deberán tenerse en cuenta entre otras las siguientes:

- √ Uso del software y política de derechos de autor, la creación y comunicación de una política clara y obligatoria de la propiedad intelectual del software es un paso importante para atemperar la posibilidad de que la organización infrinja la ley de derechos de autor.
- √ Adquisición de software, ¿Cómo hacen los usuarios para pedir copias de software o la actualización de programas existentes? ¿Existe un procedimiento de orden o requisición de compra formal? ¿Se requiere una justificación? ¿Quién toma la decisión de adquisición, y en qué se basa? ¿A quién se le compra el software? ¿Qué esfuerzo se hace para encontrar el mejor precio?.

- √ Procedimientos de instalación de software, ¿Quién es responsable del software una vez que llega a la organización? ¿Quién lo instala? ¿Quién documenta los números de serie, envía y registra esta información?
- √ Procedimientos de entrenamiento, ¿Quién es responsable por la planificación y organización del entrenamiento? ¿Se hace internamente? ¿Se hace externamente (por outsourcing)? Si no es así, ¿debería serlo?.
- √ Uso personal de software, ¿Permite la organización el uso del software personal instalado en sus PCs? ¿Permite, si la licencia lo admite, el uso de su software en computadoras portátiles?.
- √ Disposición del software, ¿Qué pasa con las viejas copias cuando se actualiza el software? ¿Qué se hace con el software que no se usa más? ¿Hay una política al respecto?.
- √ Etc.....

Es necesario formalizar las políticas y procedimientos para evitar pérdidas y gastos. Documentar y distribuir estas políticas ayudará a los usuarios a entenderlas y usarlas correctamente. Si existen políticas y procedimientos escritos, conviene revisarlos para asegurarse de que sean vigentes y precisos y si fuera necesario decidir los cambios que se deberían hacer para alinearse con las necesidades de la organización. Si las políticas y procedimientos no existen, es conveniente que se definan como una parte de las acciones normativas del plan.

El Plan de administración de Software

Lo primero que debe hacer el equipo de administración de software es diseñar el plan de administración de software, se utiliza para esbozar los objetivos de la inversión en software; el retorno anticipado para la organización en recurso ahorrados y apoyo para la misión, políticas y procedimientos para la utilización y distribución actual de los activos de software; identificación de las áreas de necesidad (tanto para el software nuevo o adicional); las áreas en las que los programas no son efectivos o no se usan; las políticas y procedimientos a ser usados para controlar la adquisición y/o desarrollo, distribución y/o implantación, uso y seguridad del software.

La Implementación del plan y seguimiento

Con la información de los resultados auditados y la guía del plan de administración de software, el equipo puede comenzar a hacer cambios en la forma de compra / desarrollo, distribución / implantación, utilización y seguridad de los activos de software, el plan incluye la toma de cualquier acción correctiva que sea identificada como prioritaria. El plan debe ser presentado a la Dirección para su aprobación y luego coordinado con otros departamentos en la organización de forma tal que se integre con otros planes existentes, políticas y procedimientos.

Acciones correctivas y resoluciones

En la mayoría de los casos, la Auditoría de Software descubrirá por lo menos unas pocas situaciones que requerirán algún tipo de resolución, como por ejemplo una acción correctiva.

Cualesquiera de esas acciones deberán ser claramente identificadas en el plan de administración de software e implementadas tan pronto como sea posible una vez que el plan haya sido revisado y aprobado por la Dirección principal.

Las acciones correctivas pueden incluir la creación de políticas, procedimientos o tal vez un cambio estructural en cómo se adquiere y distribuye el software. En otros casos, podrán requerirse acciones más serias. Las siguientes son algunas de las acciones típicas que podría ser necesario tomar:

- √ Destrucción de copias ilegales, durante el proceso de la Auditoría, deberán destruirse todas las copias ilegales de software.
- √ Implementación de controles, debido a su relativamente bajo costo, el software informático es tratado informalmente por la organización, el resultado es que el software es adquirido e instalado con pocos o ningún control, una mejor asignación de la inversión en software dictará la necesidad de mejores controles.
- √ Modificación de los procedimientos de adquisición, a menudo se encuentra que la adquisición de software no está bien coordinada y se desaprovechan beneficios en su compra, con un procedimiento revisado de adquisición se podrían reducir los costos de inversión en software.
- √ Software perdido y reemplazo de manuales, raramente una organización con controles inadecuados podrá localizar todas las licencias, software y manuales necesarios de todas las copias en uso, esta carencia necesitará ser corregida inmediatamente.
- √ Distribución de nuevo software, la revisión del uso del software posiblemente detectará situaciones en las que el usuario no tiene el software adecuado para trabajar o carece de él.
- √ Autorización de copias adicionales, si la licencia de un programa de software permite su uso en una computadora portátil, será necesario autorizar esta utilización así como las copias efectuadas y el software instalado.

- √ Reasignación de Software, las copias de software que no estén en uso necesitarán ser reasignadas a otros puestos de trabajo o deberán ser extraídas para ser almacenadas.
- √ Resolución de violaciones flagrantes, típicamente, la violación de los derechos de autor de software es el resultado de la ignorancia de la Ley, de políticas inadecuadas, o de la inadecuada puesta en vigencia de las políticas existentes.

Entender la Ley de Derechos de Autor

Algunas veces, sin embargo, la auditoría de software detectará problemas más serios tales como la violación flagrante y deliberada de la Ley por parte de uno o más usuarios, o el robo directo e intencional de la propiedad de la compañía. Si estas violaciones no son detenidas, los incidentes se multiplicarán.

Un programa de administración de Software Continuo

Programa continuo de Administración de Software

Después que el Equipo de Administración de Software haya conducido la auditoría, escrito el plan, tenido la aprobación del plan, comenzado la implementación, y que se hayan tomado las acciones correctivas, el trabajo aún no está completo. En algunos casos, se necesitan nuevas o renovadas políticas y procedimientos para administrar la inversión de software. Se introducirán nuevas versiones de software existente, e inclusive algunas nuevas clases de software a la organización. Esto obligará a revisar constantemente el plan.

Deben seguirse procedimientos sistemáticos para identificar, seleccionar los programas, implantar, mantener y controlar el software adquirido y su utilización.

Fuente: David H. Li, "<u>Auditoría en centros de cómputo: Objetivos, lineamientos y procedimientos</u>", 1ª Ed. Trillas, México, 1992

- ⩾ Selección del software del sistema.
- ⩾ Análisis costo-beneficio del software del sistema.
- ⩾ Instalación del software.
- ⩾ Mantenimiento del software del sistema.
- ⩾ Procedimientos para cambios en el software del sistema.
- ⩾ Implantación de cambios en el software del sistema.
- ⩾ Registro de cambios en el software del sistema.
- ⩾ Seguridad del software del sistema.
- ⩾ Necesidades de control.

Consideraciones para la Normatividad

Fuente: Aguilar Castillo Gildardo, "Apuntes para la materia Administración de Recursos Informáticos", Facultad de Estadística e Informática, Universidad Veracruzana. México, 1998

Existen instalaciones que por no hacer una evaluación seria, compran paquetes que en poco tiempo resultan obsoletos o que son incompatibles con otros equipos de la misma instalación, los estudios técnicos de factibilidad permiten mostrar la conveniencia de la adquisición de tal o cual producto de software, no es posible comprar sin perseguir un fin específico y costeable.

- Debe establecerse un procedimiento sistemático que identifique los programas del software que son potenciales para el sistema y que satisfagan los requerimientos de la organización.
- El área de informática solo deben ser los responsables del estudio técnico de factibilidad y dar sugerencias al usuario, pero éste es el que debe tomar la decisión.

Las fases que regularmente sigue una evaluación del software son:

1. Identificar los requerimientos de información.
2. Realizar un estudio de viabilidad
3. Si la alternativa seleccionada implica la adquisición de software, elaborar el estudio técnico de factibilidad.
4. Identificar el software mas idóneo, considerando los siguientes parámetros:
   - Alcance práctico del producto
   - Compatibilidad con el software existente
   - Sencillez en la operación del producto
   - Mantenimiento para actualizaciones futuras
   - De fácil instalación
   - Soporte técnico
   - Documentación
   - Aceptación del producto en el mercado
   - Costo del software
5. Considerar al menos tres proveedores y solicitarles una prueba de rendimiento.
6. Evaluación por parte del comité de sistemas del producto seleccionado.
7. Presentar al usuario o a quién deba tomar la decisión un documento que contenga:
   - Índice
   - Objetivos que se pretenden
   - Lista de los proveedores evaluados
   - Procedimiento de selección
   - Análisis de costo beneficio
   - Observaciones y recomendaciones
   - Firmas del comité
8. Adquirir el paquete de software de acuerdo a los procedimientos establecidos por la organización.

- El software deberá ser probado en forma exhaustiva antes de que sea liberado para su utilización de acuerdo a un plan.

- El estudio costo beneficio debe contener:
  a) El costo directo financiado para la compra del software.
  b) El costo de la modificación necesaria para adaptar el software al medio ambiente de sistemas de información de la organización.
  c) Los requerimientos de equipo para este software.
  d) Los requerimientos de capacitación y entrenamiento asociados con la utilización de ese software.
  e) Los requerimientos de soporte técnico asociados con ese software.
  f) Un análisis de las facilidades del software para cumplir con los requerimientos de proceso así como los requerimientos técnicos y de seguridad.

Mantenimiento del software del sistema.

Fuente:http://www.sanmartinbaq.edu.co/cursos/sistemas/01051/guia02.htm
Nov '2000

Mantenimiento no significa sólo corregir errores, este incluye todos los cambios que debe hacerse al software para lograr que siga siendo útil a los usuarios, teniendo en cuenta nuevas necesidades y nuevas tecnologías.

Una de las características del software es que no se estropea, es decir, no hay que cambiar piezas porque se desgastan o se dañan; sin embargo, si se debe actualizar o modificar por cambios en los requerimientos, adaptaciones, correcciones, mejoras, etc. Todas estas actividades que modifican el software después de que esté ya ha sido entregado y puesto en operación se conoce con el nombre de *Mantenimiento*.

Si tomamos la definición genérica de mantenimiento como la actividad de mantener *algo* (un artefacto) en estado correcto de funcionamiento, nos damos cuenta que el mantenimiento de software no corresponde realmente a esta definición, o mejor, sólo una parte de lo que típicamente llamamos mantenimiento de software corresponde a esta definición.

La actividad de mantenimiento de software no involucra únicamente la corrección de defectos, sino un conjunto de actividades adicionales que pueden alcanzar un gran porcentaje de la labor. Estas otras actividades distintas de corregir errores, corresponden a los cambios que debe hacerse sobre el software para que, por ejemplo, este pueda satisfacer nuevos requerimientos de los clientes, pueda ser ejecutado sobre una plataforma más moderna, pueda ser conectado con otros sistemas, mejore el sistema de seguridad, permita acceso a través de Internet, etc.

Fuente: Aguilar Castillo Gildardo, "Apuntes para la materia Administración de Recursos Informáticos", Facultad de Estadística e Informática, Universidad Veracruzana. México, 1998

Las modificaciones temporales, se identifican porque sólo afectan a la corrida que se está realizando, es decir, una vez que concluye de debe eliminar la modificación, como si nunca hubiese existido, ahí esta el riesgo, es importante implementar controles estrictos, en cambio, las modificaciones permanentes, se identifican por que permanecerán en lo sucesivo, por lo que se tendrán que sujetarse a un procedimiento que incluye, solicitar el programa al área responsable de los sistemas en producción, realizar el cambio solicitado en base a la solicitud del usuario, aplicar todas las pruebas que se consideren, documentar la modificación y afectar los manuales, solicitar al área de operación la implementación de las entidades afectadas en las bibliotecas de producción.

A continuación algunas consideraciones:

- Todo el mantenimiento del software y las actividades relacionadas con éste deben documentarse de acuerdo a los estándares de la instalación.
- El mantenimiento del software y su documentación deben resguardarse a salvo de cualquier falsificación y/o alteración.
- Todos los cambios del software del sistema deben estar completamente aprobados y documentados.
- Deben estar de acuerdo a los estándares de documentación y de prueba.
- Deben realizarse de acuerdo a un plan y sus resultados deben ser revisados y probados.
- Deben llevarse a cabo por personas que no sean programadores del sistema.
- Deben existir mecanismos formales de comunicación entre los programadores del sistema y el grupo de implantación.
- Proporcionar a los usuarios del sistema la documentación necesaria para operar el sistema con estas modificaciones.
- Mantener un registro de todos los cambios al software de los sistemas actualizando los manuales de sistemas, operación y usuario.
- El acceso al software del sistema y a la documentación correspondiente debe restringirse a personal autorizado.

Los controles, como la seguridad, rara vez constituyen un objetivo primario por lo que generalmente se requiere de grandes revisiones para incorporarlos, las necesidades de control se incluyen en dos categorías:

- Los controles del usuario
- Los controles detallados de cada proceso, de los datos y los archivos.

El Costo del Mantenimiento de Software

Fuente:http://www.sanmartinbaq.edu.co/cursos/sistemas/01051/guia02.htm
Nov '2000

La gran mayoría de los sistemas deben ser operacionales por mucho tiempo, incluso años. Si decimos que la vida de un software es el intervalo de tiempo desde cuando se define el problema hasta cuando el sistema se retira de operación, un gran porcentaje de este tiempo corresponde a la operación del sistema y por tanto, sobre este tiempo, se realizan actividades de mantenimiento.

Se podría pensar que en términos de esfuerzo y costos, la actividad de desarrollo es la más costosa ya que se trata de construir un software a partir de la definición de un problema, mientras que las otras actividades "sólo" modifican algo que ya esta hecho. Desafortunadamente, las estadísticas muestran que de los costos relacionados con la vida de un software el mayor porcentaje corresponden a las actividades de mantenimiento.

Asociados a las actividades de mantenimiento hay dos tipos de costos que vale la pena describir para entender mejor el problema. Por un lado están los *costos directos* que corresponden básicamente al tiempo que invierten las personas en realizar la labor. Por otro lado están los *costos indirectos* que aunque difíciles de estimar son reales y tienen impacto sobre los costos directos.

Los costos indirectos corresponden a las consecuencias de los errores detectados cuando el sistema ya está en operación (pueden ser catastróficos), el deterioro del software hasta su muerte, clientes insatisfechos debido a la dificultad para satisfacer los nuevos requerimientos, dificultades para tratar todas las solicitudes de modificación

A continuación veremos un poco más en detalle los costos de los errores y los costos del deterioro del software.

Costos de los Errores

Aunque no podemos decir cuanto cuesta un error, si podemos hablar de algunas causas de aparición de errores como consecuencia de las actividades de mantenimiento, según estudios realizados, las modificaciones de código aparentemente más simples son las que tienen más probabilidad de introducir nuevos errores. La razón de esto es que dada su aparente simplicidad, los programadores no "*pierden el tiempo*" planificando la modificación ni, una vez hecha, verificando que no hay regresión en el sistema (las pruebas son omitidas). Esto quiere decir que la corrección de un error puede implicar la introducción de muchos más!!

Costos del deterioro del Software

La naturaleza de los errores de hardware y los errores de software difieren en al menos una característica fundamental: el hardware se deteriora a causa de la falta de mantenimiento y el software se deteriora a causa del mantenimiento. El deterioro del software se refiere a que a medida que se hacen los cambios se hace más complicado entender su estructura y como consecuencia, será más difícil hacer cambios subsiguientes.

Dentro de los costos asociados a las actividades de mantenimiento, el más alto es el costo de *comprender* un software para saber dónde hacer el cambio. Esto se agrava con el tamaño del sistema y con su edad. A través de los años, lo único que queda del sistema es el código fuente ya que con el deterioro se pierde también la correspondencia entre la documentación del sistema y el código. Eso significa que para que un programador pueda entender el sistema, con lo único que cuenta es con las líneas de código (que pueden ser cientos, miles o miles de cientos!!!)

Es entonces, difícil entender el sistema para saber dónde hacer el cambio y también es difícil entender el impacto del cambio sobre todo el sistema. Esto último implica, por un lado, la introducción de errores y por otro, entramos en un ciclo de cambios y deterioro continuo hasta la muerte del sistema. Las causas son múltiples las causas de que el mantenimiento sea difícil y costoso. A continuación se enumeran algunas de ellas:

- Herencia del Desarrollo. Gran parte de los problemas del mantenimiento empiezan desde el momento mismo de la puesta en operación del software ya que con las presiones de tiempo, éste se entrega antes de ser terminado y debidamente probado. En otra palabras, *software sin terminar,* significa también que no se tiene la documentación del sistema. Es decir, cuando se empiezan las actividades de mantenimiento el único medio para entender el software es a través de las líneas de código. Si, además, estas líneas de código han sido escritas por varias personas, cada una con estilos y convenciones distintas, será aún más difícil entender el software.

  No hay que olvidar que parte de las características de los procesos de software es la movilidad del personal a lo largo del tiempo y, por consiguiente, la desaparición de conocimientos, hay otros problemas heredados del desarrollo, que van a agravar las actividades de mantenimiento, que corresponden a la manera misma como el producto fue construido. Típicamente el problema se refiere a malos diseños (o ausencia de ellos) que se traducen en software poco flexible, difícil de extender o adaptar.

- Deficiente Proceso de Cambio. En un deficiente procesos de cambio, los cambios son hechos sin evaluar su impacto, causando inconsistencias con otros productos, creando conflictos con solicitudes previas, etc.. Esto se agrava en la medida que los cambios se realizan concurrentemente por desarrolladores distintos. Además, bajo la presión de tiempo, es difícil mantener actualizados los demás productos asociados del software como la documentación, los manuales, las pruebas, etc.

- Factores Humanos. Hay algunos factores humanos que causan que el mantenimiento sea difícil y costoso. Quizás el más importante es el menosprecio hacia estas actividades que genera una falta de interés de quienes practican el mantenimiento y de los grupos dirigentes. Típicamente, los costos del mantenimiento son a menudo subestimados. Esto se evidencia en que las personas menos expertas son designadas para mantener software, los equipos de mantenimiento trabajan en malas condiciones (las nuevas tecnologías y herramientas son dejadas para los proyectos nuevos!) y en general, las soluciones rápidas son a menudo adoptadas.

II.3.4 Control de acceso y seguridad física.

Fuente: http://www.planeta-redvista.com.ar
Nov/2000

La protección mediante el control de acceso es fundamental en un esquema integral de seguridad, si una persona que pretende acceder ilegalmente no logra obtener acceso a las instalaciones de computo, entonces la probabilidad de daño se ve reducida notablemente. Ahora bien, la consecución del éxito en tal aspecto queda en función de una normativa apropiada en cuanto a las responsabilidades involucradas para el control de acceso a las instalaciones.

Es claro que, en un ambiente organizacional donde el centro de procesamiento de datos se encuentra distribuido, las normas y procedimientos para los accesos se formularan adecuadamente para cada sector de la compañía, y el personal involucrado en cada una de ellas será responsable de su conocimiento y aplicación según el caso que se presente.

Para lograr lo antes mencionado, será necesario realizar las siguientes actividades:

- Revisar el organigrama de la compañía para determinar posibles sectores poros, siendo éstos aquellos puntos donde es más probable que se pueda quebrar el segmento protectivo de acceso.

- Revisar los procedimientos de seguridad para determinar la responsabilidad de cada aspecto de seguridad y de este modo demarcar los correspondientes a accesos.
- Verificar si la comunicación del administrador de seguridad con las demás áreas propicia de manera efectiva la comprensión de las responsabilidades involucradas y si su interpretación es acorde con los planes de seguridad de la organización.
- Entrevistar a personal seleccionado del departamento de sistemas para evaluar el grado de conciencia sobre la importancia del control de acceso y su incidencia en la seguridad física.
- Definir los procedimientos de accesos y forma de registro entrada / salida tanto para el departamento de sistemas como para cualquier otro sector de la organización.

Establecer en función de los procedimientos de accesos definidos, su incidencia en los responsables directos, para el caso de no cumplirlos.

Acceso al Area de Sistemas

El propósito de las normativas para el control de acceso es garantizar que solo personal autorizado podrá ingresar al área de sistemas, con lo cual se disminuirá considerablemente el riesgo de robo, destrucción o manipulación no autorizada de equipos e información. Los siguientes elementos deben ser tenidos en cuenta a la hora de controlar los accesos al centro de cómputos:

- Registro de firma de entrada / firma de salida: Se debe requerir a toda persona que desee ingresar a las instalaciones que firmen un registro, indicando la hora de entrada, el propósito, y la hora de partida.
- Tarjetas de Acceso: El equipo de control de entrada mediante tarjetas, es probablemente el dispositivo más popular para el control del acceso. Las puertas pueden abrirse ya sea mediante tarjetas ópticas o con códigos magnéticos. La autorización de la entrada debe controlarse dinámicamente mediante una clasificación de seguridad por medio de un código a quienes se les entregue la tarjeta. Las autorizaciones deberán poder ser dadas de altas, actualizadas, y dadas de baja en forma automática, y se podrá preparar reportes e informes de la actividad de entrada y exhibirse en la pantalla de un oficial de control.
- Distintivos o Gafetes: Los gafetes son plaquillas metálicas o de plástico o tarjetas de cartulina, en la que constan ciertos datos; se sujetan a la ropa por cualquier medio, y son instrumento muy eficaz para la identificación de las personas a quienes por su trabajo se les observa preponderantemente de frente, como es el caso de los ejecutivos, oficinistas, cajeros, etc.

En la actualidad, estos recursos son una forma muy popular de control de acceso. No obstante, los gafetes integrados con sistemas de tarjetas de acceso constituyen un valor adicional. Sin embargo, es común en casi todas las instituciones el hecho de que otras personas entren detrás de las que portan gafete. Los sistemas electrónicos recientes ofrecen formas de control adicionales, aunque nunca serán totalmente efectivas, si no se mantiene una disciplina razonable.

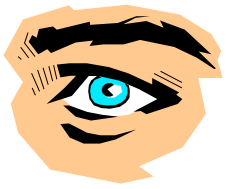
Aunque se puede hacer mucho para elevar los estándares de protección respecto al acceso físico, quizá, como en todas las cosas, exista la probabilidad de riesgo en la seguridad, por tanto, el acceso físico se debe reforzar y apoyar mediante otros elementos de seguridad. Seria muy aventurado confiar en un solo elemento de seguridad para tal fin.

Se han diseñado muchos productos para evitar la entrada de personal no autorizado a las salas de computo, una tecnología novedosa en tal aspecto es la medición o comprobación de factores físicos de la persona que intenta ingresar al centro de cómputo. *Sistemas Biométricos:*

La necesidad de un buen sistema de identificación es por lo que muchas organizaciones adquieren sistemas de tal naturaleza, pero debe saberse que estos no son el 100% exactos todo el tiempo. Estos dispositivos en ocasiones rechaza a una persona cuya identidad es valida y por otro lado también podría aceptar a un impostor.

En la actualidad existen cinco tecnologías biométricas disponibles en el mercado de dispositivos de seguridad de alta tecnología, que a continuación se mencionaran brevemente:

- *Patrón de Huellas Digitales*: Es una técnica de identificación personal muy difundida en la actualidad. Por medio de un dispositivo electrónico de alta sensibilidad se comparan exhaustivamente los patrones que conforman la huella dactilar del individuo que quiere ingresar a la instalación protegida, suelen implementar esta tecnología aquellos entes que requieren un alto grado de credibilidad en la protección y resguardo en cuanto a accesos a sus instalaciones de cómputos.
- *Geometría de la Mano:* Estos sistemas miden, graban, y comparan longitud de dedos, translucidez de la piel, grosor de la mano y forma de la palma.
- *Escaneo Retinal:* Los patrones de arterias y venas que se encuentran en el ojo humano son únicos. Un scanner retinal analiza esas configuraciones oculares para determinar la identidad de una persona.



- *Verificación de voz:* Esta técnica se desarrollo a principios de la década de 1970. Los primeros sistemas tenían tasas de error muy altos, tal es el caso por ejemplo de que un usuario con una congestión nasal o un simple estado de resfrió le alterara la voz, quedando en consecuencia sin posibilidad de ser aceptado. Actualmente esto se ha solucionado casi en su totalidad.
- *Dinámica de Firma:* Una firma queda expuesta a ser falsificada, y los que realizan tal duplicación ilícita suelen ser muy hábiles en su quehacer. Una técnica que suele implementarse a los fines de salvaguardar incursiones por parte de estos falsificadores consiste en un censado electrónico y medición de los movimientos y tiempos en estampar la firma. Este método es aplicable para controlar el acceso en aquellas áreas en donde se encuentren instalaciones de alta seguridad que tengan poco trafico de personas.

Fuente: http://www.planeta-redvista.com.ar
Por Néstor O. de los Santos

Acceso al sistema

La individualidad de las cuentas es la clave para poder asegurar y controlar cualquier sistema que procese información sobre los intereses de individuos o grupos de individuos. En consecuencia, deben cumplirse ordenadamente ciertos requerimientos para satisfacer ese objetivo. El primero de esos requerimientos es para la identificación individual de los usuarios. Segundo, hay una necesidad de autenticación. Sin esta, la identificación de cualquier usuario no tiene credibilidad.

Sin una identidad creíble, las políticas de seguridad no pueden ser invocadas apropiadamente puesto que no se asegura que una autorización de cuenta sea efectuada legítimamente. Los usuarios deben iniciar su sesión de trabajo identificándose mediante un sistema de ingreso (login) conformado por:

a. Nombre de Usuario: Identifica unívocamente la cuenta del usuario.
b. Password: Contraseña o "llave secreta" que autentifica inequívocamente la identidad del usuario para su acceso.

La seguridad provista por este sistema depende del compromiso que se obtenga por parte de los usuarios como del Administrador de Sistemas y del grado de secreto con el que se mantenga la Password.

Uno de los métodos mas utilizados de intrusión a los sistemas es el robo de Password. Robando un nombre de usuario y su correspondiente Password un intruso puede lograr el acceso al sistema, modificar privilegios de cuentas y acceder a datos sensitivos, además de poder utilizar dicho acceso como trampolín para vulnerar otros sistemas. Por lo tanto, habrá que ser muy estricto al momento de generar una contraseña y se deberá tener en cuenta los siguientes factores que se citan a continuación:

En la generación:

1. Elegir claves con una longitud mínima de 9(nueve) caracteres.
2. No elegir palabras del diccionario.
3. No elegir sustantivos, adjetivos y cualquier otro tipo de información de fácil relación con su persona.
4. No elegir nombres y/o apodos personales, de familiares, de amigos o de compañeros de trabajo.
5. No elegir nombres de marcas conocidas, palabras de moda y lugares geográficos o similares.
6. No utilizar patrones típicos, como 123456789, abcdefgh o similares.
7. Intercalar por lo menos un carácter especial.
8. Evitar utilizar muchos caracteres repetidos, únicamente números, letras o letras seguidas de un único dígito.

En el uso:

1. No almacenar información sobre su cuenta/password en archivos bajo ningún pretexto.
2. Cambiar su Password antes del período de expiración de la misma (2 meses).
3. Evitar que otras personas conozcan y utilicen su Password.
4. No escribir la Password mientras otra persona mire como lo hace.
5. No reutilizar passwords antiguos.
6. No ingresar su Password en aplicaciones no autorizadas.

Reportar inmediatamente al Administrador de Sistemas cambios en los derechos de acceso a aplicaciones y bases de datos, pérdida u olvido de la Password y sospecha de intentos de violaciones a la seguridad de sus cuentas.

Seguridad total

Fuente: Aguilar Castillo Gildardo, "Apuntes para la materia Administración de Recursos Informáticos", Facultad de Estadística e Informática, Universidad Veracruzana. México, 1998

El acceso a los recursos de cómputo debe ser controlado; debe estar prevista la seguridad física de los recursos humanos y de cómputo, para protegerlos contra cualquier uso no permitido, daño, pérdida o modificaciones. En estos términos se requiere un enfoque amplio que abarque los dos aspectos importantes en la administración de centros de cómputo.

1. Aspectos administrativos
- Políticas definidas sobre seguridad en computación
- Organización y división de las responsabilidades
- Seguridad física y contra incendios
- Políticas hacia el personal
- Seguros

2. Aspectos técnicos y de procedimiento
- Seguridad de los sistemas (equipo y programación)
- Seguridad de las aplicaciones (datos y archivos)
- Estándares de programación y operación de sistemas (controles)
- Función de auditoría y control de calidad (evaluación operativa)
- Plan y simulacros para desastres (contingencias)

No existe un sistema completamente seguro y, en última instancia, se depende en gran medida de la integridad de las personas en un centro de cómputo, la aplicación significativa de la seguridad requiere:

a) Clasificar cada instalación en términos de riesgo alto, medio o bajo
b) Identificar las aplicaciones de alto riesgo y sus programas y archivos
c) Cuantificar el riesgo, de preferencia en términos financieros.
d) Evaluar estrategias opcionales de seguridad
e) Seleccionar la estrategia que resulte más apropiada para la institución.
f) Justificar ante la gerencia el costo de la estrategia seleccionada.

El compromiso de la gerencia con la política de seguridad es primordial, es recomendable que exista la función de encargado de seguridad o se integre un comité de seguridad con los responsables de las diferentes áreas que conduzca a un mayor seguimiento de rutinas y a niveles de compromisos mas altos.

Fuente: David H. Li, "<u>Auditoría en centros de cómputo: Objetivos, lineamientos y procedimientos</u>", 1ª Ed. Trillas, México, 1992

- Responsabilidades para la seguridad física.
- Acceso al centro de cómputo.
- Acceso a bibliotecas, archivos y bases de datos
- Acceso a equipos, estaciones de trabajo, redes.
- Prácticas de seguridad.
- Planes de seguridad.

<u>Consideraciones para la Normatividad</u>

Fuente: Aguilar Castillo Gildardo, "<u>Apuntes para la materia Administración de Recursos Informáticos</u>", Facultad de Estadística e Informática, Universidad Veracruzana. México, 1998

Responsabilidades para la seguridad física.

- Las responsabilidades para la seguridad física deben estar asignadas e incluidas en la descripción de puestos.
- A medida que se desciende la jerarquía de gerencia, las responsabilidades son progresivamente más operativas y detalladas.
- Todo el personal del centro de cómputo debe estar involucrado en las prácticas de seguridad.

Acceso al centro de cómputo.

- Deben revisarse los procedimientos de acceso al centro de cómputo, el lugar dónde residen los equipos se debe considerar área de acceso restringido.
- Los controles del acceso varían según las distintas horas de la jornada de trabajo, es importante considerar controles nocturnos, durante los descansos y cambios de turno.
- Cualquier persona que no sea del área de cómputo, debe ser escoltada y vigilada cuando se encuentre en el área de operación.
- En instalaciones de alta seguridad, se debe utilizar dispositivos automáticos, circuito cerrado, alarmas, blindajes o cualquier procedimiento de alta tecnología.
- Definir niveles de seguridad para las diferentes áreas, desde el acceso a las oficinas, Cintoteca, área de captura, programación, proceso, corte y desencarbonado, almacén de papelería, etc.
- Dotar de tarjetas de acceso y gafetes al personal autorizado al centro de cómputo en función de los diferentes niveles de seguridad.

Acceso a directorios, archivos y bases de datos

- El acceso a los directorios debe ser restringido a personal autorizado, los archivos de cómputo deben ser protegidos contra accidentes, destrucción y utilización por personal no autorizado.
- En un medio ambiente de acceso en línea, debe existir una seguridad de acceso y un control basado en la clasificación de la información del archivo, de las llaves de acceso, del software, del hardware o de las transacciones.
- Los operadores no deben tener acceso rutinario a los dispositivos magnéticos donde residen archivos y bibliotecas, éstos deben ser responsabilidad de un encargado y obedecer a un procedimiento administrativo para su acceso.
- Implementar registros de evidencias que reflejen la transferencia de datos entre usuarios.
- Definir estándares para la identificación y control de archivos, programas y bases de datos.

Acceso a equipos, estaciones de trabajo, redes.

- El acceso a las estaciones de trabajo debe ser controlado; el acceso a las terminales conectadas que estén manejando información confidencial, debe tener las horas de operación específicamente programadas.
- Deben registrarse los accesos de la terminal a los datos y deben revisarse periódicamente los reportes de actividades de las terminales.
- La ubicación de las terminales de trabajo debe ser considerada para no permitir su fácil acceso.
- Implementar métodos de identificación como claves físicas, cuentas personales, Password, códigos u otros métodos de identificación.
- Restringir el acceso a las redes, pues su mayor riesgo reside en su acceso no autorizado a fin de obtener información confidencial o hacer uso indebido de los recursos de cómputo.
- Utilizar medidas de seguridad realistas como códigos o la criptografía para conservar la confidencialidad de la información.
- Implementar procedimientos de monitoreo a las estaciones de trabajo para detectar posibles accesos no permitidos.

Prácticas de seguridad.

- Deben efectuarse prácticas adecuadas de seguridad, tales como identificar la ubicación de las instalaciones de los equipos de cómputo.
- La protección contra incendio de las instalaciones debe estar de acuerdo con los estándares generalmente aceptados.
- Los detectores de fuego y humo se deben colocar en relación con los aparatos de aire acondicionado, para no entorpecer su función.
- Colocar detectores de calor y humo bajo el piso falso, plafones y ductos de aire acondicionado.
- Las medidas de seguridad deben prever que todos los documentos fuente y las formas se mantengan en forma privada, confidencial, vigentes y disponibles para respaldo.
- El personal de operaciones del centro de cómputo debe estar entrenado para la aplicación de controles y procedimientos de seguridad.
- El personal debe estar capacitado para saber como actuar cuando ocurra alguna contingencia que ponga en riesgo su persona.
- Implantar planes de mantenimiento a equipos e instalaciones que reflejen una actitud mental positiva de administración y seguridad de alto nivel.

Planes de seguridad.

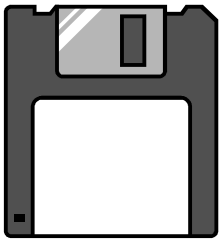
La mayoría de los planes de seguridad son superficiales, no estructurados e inadecuados para afrontar las complicaciones que surgen de un desastre real, regularmente no se llevan a cabo simulacros para probar estos planes y casi siempre la objeción es el costo, por lo que no se tiene plena garantía que los planes funcionarán, se dice que se tiene una seguridad ficticia.

- Al considerar los planes y los simulacros de desastre, se necesita delinear primeramente, los distintos tipos de desastres que pueden ocurrir; Destrucción completa o parcial de los recursos informáticos (gente, hardware, software, insumos, instalaciones, equipos auxiliares técnicos...), interrupciones no planeadas por fallas, sabotajes, huelgas...etc.
- Para cada suceso se requiere estructurar planes específicos y éstos deben ser probados periódicamente. Los simulacros de desastres son importantes por las razones siguientes:
  1. Se prueba la conciencia y preparación del personal para afrontar el desastre
  2. Se identifican las omisiones en los planes contra desastres.
  3. Constituye una buena verificación del grado de seguridad que se tiene.

Inventario de riesgos de seguridad en computación	Aspecto clave SI / NO	Adecuado SI / NO
Política de seguridad • Existe una política de seguridad definida • La responsabilidad de la formulación de política está asignada • Conciencia y compromiso por parte de la alta gerencia • El alcance de las pérdidas se ha definido		
Organización y división de responsabilidades • La responsabilidad de la seguridad se ha asignado • Descripciones claras de puestos • Inclusión de la seguridad en la descripción de puestos • División de responsabilidades entre las áreas claves • Sistemas de verificación interna bien definidos		
Seguridad de los sistemas • Las fallas en el equipo están definidas • Las fallas en los programas están definidas • Seguridad de terminales • Seguridad de redes • Equipo de respaldo		

Inventario de riesgos de seguridad en computación	Aspecto clave SI / NO	Adecuado SI / NO
Seguridad de las aplicaciones • Controles del usuario • Controles del área de procesamiento • Planes de contingencia en la aplicación • Seguridad de datos y archivos		
Seguridad física • Acceso del personal • Alarmas • Ubicación • Construcción • Disposición		
Seguridad contra incendios • Detección de incendios • Extinción de incendios • Nexos con el cuartel de bomberos • Rutina contra incendios		
Estándares • Métodos y supervisión • Documentación • Duplicado de respaldos		
Políticas hacia el personal • Políticas de contratación • Procedimiento para evaluar el desempeño • Permisos • Rotación de puestos		
Seguros • Equipo • Programas • Personal • Pérdida de utilidades		
Auditoría • Habilidades • Técnicas especializadas • Nexos con el desarrollo de sistemas • Claridad de la función		

II.3.5 Respaldo y recuperación



Una de las responsabilidades que más deben quedar claras en la normatividad es la que se refiere al respaldo de información, establecer que el personal es responsable de mantener, por un plazo determinado, toda la información que se genere, modifique o que se dé de baja.

Existen diversos métodos, la mayoría de ellos basados en herramientas de respaldo de uso común, generalmente utilerías de sistema operativo.

Fuente: David H. Li, "<u>Auditoría en centros de cómputo: Objetivos, lineamientos y procedimientos</u>", 1ª Ed. Trillas, México, 1992

- Plan para recuperación en caso de siniestro.
- Aplicaciones críticas.
- Recursos críticos.
- Procedimientos para respaldo de archivos.
- Suministro de respaldo
- Pruebas del plan de respaldo.
- Reconstrucción del centro de sistemas de información.
- Procedimientos manuales para respaldo.

<u>Consideraciones para la Normatividad</u>

Fuente: Aguilar Castillo Gildardo, "<u>Apuntes para la materia Administración de Recursos Informáticos</u>", Facultad de Estadística e Informática, Universidad Veracruzana. México, 1998

Deben existir planes adecuados para el respaldo de recursos críticos del equipo de cómputo y para el restablecimiento de los servicios de sistemas de información en caso de una interrupción no planeada.

Plan para recuperación en caso de siniestro.

- Debe de existir un plan documentado de respaldo para el procesamiento de trabajos críticos, para casos en que se presente una falla mayor en el equipo o en el software, o de que exista una destrucción permanente o temporal de las instalaciones del centro de cómputo.

Aplicaciones críticas.

- El plan de respaldo debe contener una prioridad preestablecida para el procesamiento de las aplicaciones, primeramente se procede a la identificación de las aplicaciones de riesgo alto, medio y bajo

Recursos críticos.

- El plan de respaldo debe contener instrucciones para restablecer las comunicaciones.
- El plan de respaldo debe prever un procesador de respaldo o cualquier otro tipo de recurso de cómputo.

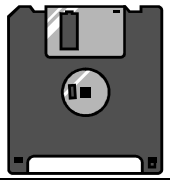
Procedimientos para respaldo de archivos.

- Deben establecerse los procedimientos para respaldo de archivos, para minimizar los requerimientos de recuperación.
- El plan de respaldo debe identificar la producción crítica, sistemas operativos y los archivos necesarios para restablecer la operación.
- Se deben programar respaldos por sistema y respaldos de la instalación.

Fuente: Revista PC MAGAZINE Junio 11, 1991.

Lo que siempre y nunca debe hacer con sus respaldos

SIEMPRE	**NUNCA**
√ debe crear una estrategia de respaldo y seguirla al pie de la letra. Ya que si se acumulan muchos discos de respaldo sin control, se pueden estar desperdiciando discos y se puede perder mucho tiempo buscando un archivo que se desea recuperar.	√ utilice caracteres gráficos (o raros) en los nombres de archivos, esto puede ocasionar que la utilería que se encargue de respaldar crea que es un archivo dañado y no lo respalde. Nunca utilice este tipo de caracteres en los nombres de sus archivos.
√ debe guardar un respaldo completo de su disco duro por lo menos de 6 a 12 meses aunque tenga varios juegos de respaldo, ya que si desea recuperar un archivo de hace tres meses puede que no exista en los juegos de respaldo.	√ guarde todos sus respaldos en el mismo sitio o a un lado de la computadora ya que si un ladrón se la roba, también se robará los discos o en un incendio se quemarán los disco junto con la computadora.
√ utilice utilerías para comprimir archivos que ya se comprimieron con anterioridad, esto únicamente hace perder tiempo al forzar a la utilería a realizar la comprensión sobre estos archivos.	√ ponga la opción de verificar y corrección de errores en la utilería que use para respaldar. Muchas de estas utilerías pueden detectar y corregir errores. Además pueden recuperar respaldos de discos dañados.

SIEMPRE	**NUNCA**
√ pruebe su utilería de respaldo cuando instale o le instalen algún programa nuevo en su computadora (con más razón si se trata de un nuevo programa que queda residente en memoria).	√ trate de economizar comprando discos marca "DuckTales" o de formatear discos de baja densidad (720K) como si fueran de alta densidad (1.44M). El dinero que se ahorra es poco comparado con la información que se pierde.
√ corra el comando CHKDSK del sistema operativo antes de hacer algún respaldo. Este comando le permite encontrar archivos dañados y corregirlos antes de que haga su respaldo ya que si lo hace con el archivo o archivos dañados ya no los podrá recuperar.	√ olvide que usted es la única persona que sabe que tan valiosa es la información que tiene en su computadora. 

Suministro de respaldo

- El plan de respaldo debe prever que exista mas de una fuente de abastecimiento para la recuperación de lo necesario y también de formas especiales.
- El surtido continuo de papelería requiere considerar un lapso de tiempo entre el pedido y la entrega, por lo que se tienen que considerar márgenes de seguridad.
- Se requiere considerar el almacenamiento de una remesa de papelería especial en otro lugar diferente al normalmente utilizado.

Pruebas del plan de respaldo.

- El plan de respaldo debe ser periódicamente probado, para asegurar que es funcional.

Reconstrucción del centro de sistemas de información.

- El plan de respaldo debe contener procedimientos definidos para la reconstrucción del centro de información.

Procedimientos manuales para respaldo.

- El plan de respaldo debe considerar los procedimientos manuales necesarios, que deben operar hasta que se lleve a cabo el respaldo para los servicios de cómputo o estos sean restablecidos.

Bibliografía de este capítulo:

1. David H. Li, "Auditoría en centros de cómputo: Objetivos, lineamientos y procedimientos", 1ª Ed. Trillas, México, 1992
2. Aguilar Castillo Gildardo, "Apuntes para la materia Administración de Recursos Informáticos", Facultad de Estadística e Informática, Universidad Veracruzana. México, 1998
3. http://www.microsoft.com/Argentina/PUBLIC/KIT_BASE/LICENCIAMIENTO/LICSEMGT/Contents/contents.htm
4. http://www.sanmartinbaq.edu.co/cursos/sistemas/01051/guia02.htm, Nov '2000
5. http://www.planeta-redvista.com.ar, Nov/2000
6. http://www.planeta-redvista.com.ar, Por Néstor O. de los Santos
7. Revista PC MAGAZINE Junio 11, 1991.