Unidad IV
Control de aplicaciones y seguridad

Se aborda al control como base de la efectividad directiva, como elemento que mide el desempeño de los servicios informáticos a través de la identificación de puntos de control y áreas críticas en el marco de la seguridad total, se abordan también las implicaciones en la operación de sistemas de información, el control de calidad, el control de acceso a los servicios informáticos y las auditorias.

Introducción

Para el logro de la efectividad directiva en un centro de cómputo, deben confluir una serie de factores que van desde la definición de los objetivos, las funciones, los sistemas y los procedimientos, la asignación de recursos y responsables, la ejecución operativa de los procesos, todo esto sustentado en la plataforma del control, como auditor de lo realizado contra lo planeado.

Por lo tanto describiremos los factores centrales que dan cuerpo a la función de efectividad directiva y que es el control como elemento que permite conocer los niveles reales de desempeño y tomar decisiones basadas en un sistema de información.

Se analizarán los puntos de control y las áreas críticas en los centros de procesamiento de datos en un marco de seguridad total, por otro lado, se deben considerar algunos aspectos que nos garanticen el procesamiento de datos continuo, por lo tanto describiremos algunos ejemplos de situaciones que se pueden presentar en la operación de sistemas de información, el control de calidad y el acceso a las instalaciones y sistemas, así como aspectos relevantes de las auditorías.

IV.1 Naturaleza del control

Fuente: IMSS, "Efectividad directiva", Ed. IMSS, México, 1989.

Se ha visto la importancia y la necesidad de la planeación en los sistemas que pretenden lograr buenos niveles de efectividad en sus resultados, sin embargo la planeación por sí misma no garantiza el logro de resultados adecuados, el directivo debe entrar en otros campos del proceso administrativo, que implican al igual que la planeación, el desarrollo de actividades específicas.

Estas actividades administrativas son:

- la coordinación
- el control administrativo
- la evaluación

La coordinación

Involucra una serie de factores a considerar para que se dé adecuadamente:

- A mayor división del trabajo, corresponde mayor importancia a la unión de los componentes en una relación unificada.
- La especialización del trabajo es conveniente, en cierto modo, sin embargo requiere una alta integración y el trabajo en equipo.
- La integración de las diversas funciones, a mayor integración individual suele corresponder mayor integración de grupo.
- A mayor comprensión y aceptación de los objetivos de los sistemas por quienes colaboran en éstos, corresponderá una mayor facilidad para conseguir su cooperación voluntaria.
- A mayor perfección de los sistemas, corresponderá una disminución del concepto de autoridad en el sentido de dominación.

El control administrativo

Es el medio del que se vale la dirección para determinar que fines se están alcanzando satisfactoria y oportunamente, es el medio por el cuál los administradores miden el esfuerzo respecto a las metas propuestas y que les permiten ver si se están logrando o no.

El control se vale de informes, presupuestos, normas, limitaciones en los gastos y metas esperadas de productividad. Toda información que se va generando, se pone al servicio de la planeación misma, de la organización, del mecanismo de dirección, de la investigación, del control de presupuestos y análisis de costos y de la administración de personal.

Al poner en práctica un sistema de control, deberán tenerse en mente tres actividades principales:

- proyectar el sistema de control en función de la planeación
- establecer normas y procedimientos
- determinar el grado en que la práctica se ajusta o se aleja del plan

La evaluación

Es un concepto que se complementa con el control, pero que tienen campos bien definidos. Al control se le identifica como el instrumento encargado del funcionamiento de un sistema para que su desarrollo se efectúe de acuerdo con lo planeado. La evaluación califica si los resultados producidos por ese sistema van dirigidos a la eficacia en el logro de los objetivos últimos y a la eficiencia en la utilización de recursos escasos.

Las habilidades por ellas requeridas constituyen el reto central de la función directiva, pues se refiere al quehacer práctico y concreto de la dirección: conseguir los resultados esperados.

IV.2 Puntos de Control y áreas críticas

La situación de riesgo que deriva de la acción, actitud y circunstancia relacionadas con el personal o agentes externos no es nueva, los daños pueden ser accidentales, deliberados o producto de la negligencia. Los recursos de cómputo deben estar especialmente protegidos contra este tipo de daños. Los principales elementos de amenaza que afecta el activo informático en cualquier organización son:

- Errores y omisiones
- Incendios
- Inundaciones
- Elementos externos
- Empleados deshonestos
- Sabotaje técnico
- Destrucción de datos negligente o intencional
- Irresponsabilidad
- Falta de capacitación
- Falta de documentación
- Etc...

En la mayoría de los centros informáticos, no se cuenta con normas de seguridad efectivas y mucho menos métodos de seguridad debidamente establecidos, esto trae como consecuencia la implementación de criterios de seguridad poco confiables, parchados y de fácil vulnerabilidad que a largo plazo ocasionan grandes gastos y retrasos en los procesos, es decir se tiene una "seguridad ficticia o falsa".

Se enumeran ciertos factores críticos que necesitan atención en relación con los sistemas de cómputo, estos factores han sido el origen de muchos problemas de información en la actualidad, inclusive han sido la clave para mejorar el control de las aplicaciones.

- Adecuada identificación de funciones (usuarios, dueños e informática)
- Limitar al mínimo posible los privilegios de acceso.
- Centralización en el control de los cambios al sistema.
- Mantenimiento de librerías [50] en discos y dispositivos magnéticos.
- Establecimiento de una conciencia de seguridad física y de la información
- Plan de recuperación en caso de desastres naturales.
- Fomento de un programa vital de riesgos.
- Control de los programas en etapa de producción y de prueba.
- Empleo de utilerías y rutinas de ayuda en el software.
- Definición de una metodología del desarrollo de sistemas.
- Programa de entrenamiento.
- Monitoreo de personal.
- Identificación de Inventario.
- Pólizas de seguros y contratos.
- Control de la información de Entrada / salida.

Se debe identificar las áreas que han comprobado ser las mas críticas para el control de la información de los sistemas y equipos, es mucho más efectivo asignar recursos al manejo y protección de las áreas identificadas como vulnerables, que el estar haciendo constantes revisiones, análisis de riesgos o diseño de distintos métodos.

Adecuada identificación de funciones

Este factor asegura que exista una adecuada definición de tareas y responsabilidades para el desarrollo de nuevas aplicaciones y para los sistemas en operación, en particular cita autoridades, responsabilidades y el compromiso del personal en el procesamiento de la información. De ser posible cada una de las siguientes funciones deberá ser ejecutada por una persona distinta, alguna de estas funciones son:

- Diseño de aplicaciones.
- Administración de Bases de Datos.
- Control de librerías y archivos.
- Captura.
- Emisión de reportes.
- Distribución de reportes.
- Programación de los sistemas desarrollados.
- Mantenimiento del software desarrollado.

[50] Este concepto se refiere a los directorios creados en el disco duro, también se le conoce como biblioteca

Limitar al mínimo posible los privilegios de acceso

La manera de conducir los privilegios que serán cedidos a cada usuario, puede realizarse por medio de una sencilla pregunta: Si este reporte o archivo no fuera accesible para el usuario, ¿Podría el usuario cumplir con su trabajo?. Siempre deberá pensarse en el mínimo de privilegios que se otorgarán al usuario y no en los privilegios que él desea manejar.

Centralización en el control de los cambios del sistema

Este factor es crítico para todos los sistemas y aunque éstos hayan sido diseñados con una alto grado de integridad y control, estas consideraciones y protecciones pueden verse anuladas al presentarse una falla en cualquiera de los cambios a los que sea sometido el sistema. La mayoría de los problemas que se presentan en la actualidad son el resultado de "arreglos rápidos" al software, con el objeto de sobre llevar un problema determinado o soportar alguna necesidad determinada, al asumir que están apoyando al usuario pueden crear una ruptura o parche al momento de unir dos segmentos del programa, estas inserciones temporales de código que no han sido previamente autorizadas pueden pasar desapercibidas e introducirse de modo permanente en un programa que no fue concebido de tal manera.

Mantenimiento de librerías en discos y dispositivos magnéticos

En la mayoría de las organizaciones actuales la información almacenada en dispositivos magnéticos representa un recurso que garantiza el mantener en operación a dicha compañía, si se perdiera el acceso a estos recursos muy probablemente no podría sobrevivir, todas las organizaciones deben poseer procedimientos que les permitan tener el control de sus inventarios de librerías de información.

Establecimiento de una conciencia de seguridad física y de la información

La mayoría de las empresas que dependen de sus sistemas se preocupan por la seguridad solo en un principio, cuando se implantan los sistemas, es cuando proporcionan cierta orientación y entrenamiento a su personal, sin embargo, no existe un seguimiento de aquella primera introducción, por lo que el empleado al paso del tiempo olvida el objetivo de las normas de seguridad y aun estas mismas. Cada organización debe de tener un programa de seguridad que le permita revisar la continua responsabilidad con respecto a la seguridad en los sistemas.

Plan de recuperación en caso de desastres naturales

El propósito de estos planes es programar los pasos a seguir en caso de desastre con objeto de garantizar la continuidad de las operaciones de la empresa. Estos planes son medidas que deberán ser tomadas para restablecer la capacidad operativa de la organización en el menor tiempo posible, estos desastres comprenden catástrofes mayores como terremotos, huracanes, inundaciones, etc.

Fomento de un programa vital de registros

Con el fin de proteger la información, los datos se deberán clasificar de acuerdo al nivel que ocupan dentro de las necesidades de la empresa, la siguiente clasificación podría ser utilizada:

- Registros vitales, la pérdida de estos registros podrá terminar con la organización misma, esta información a menudo no es recuperable y es información con carácter de disponibilidad inmediata para que la organización se mantenga en operación.

- Registros esenciales, la pérdida de esta información podría ciertamente tambalear la capacidad de operación de la organización, la empresa no se vendría abajo, sin embargo, su nivel de operación seria gravemente afectado.

- Registros importantes, la pérdida de esta información causa inconvenientes, sin embargo rara vez podrá ser el origen de rupturas en la capacidad operativa de la empresa.

- Registros útiles, la pérdida de esta información produce apenas pequeñas perturbaciones en la empresa, generalmente son vistas como no esenciales y puede darse el caso de que no se presente la necesidad de tener que recuperarlos

Control de los programas en etapa de producción y de prueba

El control de las librerías de prueba y los programas en prueba del área de desarrollo de sistemas del centro de cómputo, es clave en el manejo de la integridad y seguridad de los sistemas, entiéndase como producción todos los sistemas y las aplicaciones que ya han sido probados, aprobados y hechos parte de la operación de la organización.

Empleo de utilerías y rutinas de ayuda en el software

Todas las utilerías que permitan añadir, borrar, modificar y copiar información deberán estar bajo completo control, el uso indiscriminado de tales utilerías permitiría a las personas cometer actos deshonestos motivados por intereses personales o por venganza.

Definición de una metodología del desarrollo de sistemas

El área de desarrollo de nuevas aplicaciones del centro de cómputo debe contar con una metodología para el ciclo de vida de desarrollo de sistemas que norme la secuencia lógica, los controles que se deban considerar en su administración y las actividades que se deriven en base a la naturaleza del proyecto.

Programas de entrenamiento

La mayoría de los problemas en los sistemas de procesamiento de datos son debido a errores u omisiones humanas, y puede decirse que la causa es originada por la falta de entrenamiento del personal. Cada organización deberá revisar los planes de capacitación de su personal con el objeto de lograr la máxima eficiencia en todas sus funciones.

Monitoreo de personal

Es importante tener siempre presente que la información de la empresa puede verse amenazada en un momento dado por directivos, usuarios o cualquier persona que tenga un nivel preferencial y privilegios de acceso a la información, para los administradores de bases de datos y el personal de informática siempre existirá la probabilidad de accesar a los sistema sin ser detectados. La mayoría de las aplicaciones son vulnerables a su propio personal.

Identificación de inventario

Muchas organizaciones no poseen registros de los activos que representan el software y la información almacenada dentro de sus inventarios, todas las rutinas que hayan sido desarrolladas por sus programadores deberán ser declaradas como propiedad de la compañía, no se puede pensar en algún grado de protección o de seguridad si no se tiene bien definido los recursos de la organización.

Pólizas de seguros y contratos

La gerencia deberá contratar pólizas de seguro para todos los recursos informáticos dada su gran vulnerabilidad, además de pactar contratos legales que especifiquen claramente las responsabilidades del personal de informática y otras empresas relacionadas con los servicios de venta y soporte técnico de hardware, software, además servicios de consultorías, desarrollo de sistemas, programación, Internet, tiempos compartidos, etc. Deberán ser revisados en cada punto de su contenido.

Control de la información de entrada / salida

Todos los sistemas deberán contemplar algún tipo de control y validación de la información que se introduce en el sistema, así como de la que es solicitada, la asignación de la responsabilidad de recibir, transferir y monitorear toda la información que se vaya a introducir o a obtener del sistema es una manera de lograr la integridad de la información.

Los quince puntos anteriores han probado ser algunos de los factores más críticos y problemáticos dentro de un centro de cómputo con respecto a la seguridad y control de la información, antes de iniciar cualquier estudio o solicitar la implantación de alguna técnica de seguridad es conveniente revisar los factores anteriores con el objeto de tener una visión más amplia que le permitirá atacar los puntos más vulnerables sin temor a desperdiciar recursos.

Control de calidad para la organización y para los sistemas de información.

La calidad persigue y debe conseguir *hacer de una forma más sencilla lo complejo*. Esto sólo puede lograrse proponiéndose mejorar lo conseguido a cada momento. Y para ello hay que medir, señalar estándares[51] y tratar de superarlos.

Creer, querer, saber, poder y hacer.[52]

Existe un conjunto de conceptualizaciones y de premisas, sin las cuales se hace muy difícil "llevar a la práctica" lo que queremos significar como calidad en informática:

1. *Calidad como filosofía, como reto a cero errores.* No basta con lanzar proclamas ni deseos, se debe actuar inconscientemente.
2. *Establecimiento de una política de calidad.* Llevar consigo metodologías y procesos de trabajo que faciliten los servicios y coadyuven a la solución de problemas que se puedan presentar.
3. *Adecuación de la política del personal.* Venderles la idea, con frecuencia nos encontramos con escepticismos y defensas ante el reto de la calidad, reflejado en preguntas como: La calidad ¿Para qué? ¿Por qué? ¿y en que me va a beneficiar?
4. *Participación de la alta dirección en el proyecto de calidad.* La alta dirección tiene que comprometerse a participar activamente y de manera continuada durante todo el proyecto.
5. *La calidad, responsabilidad de todos*. Cada empleado en su puesto de trabajo, es responsable del trabajo que corresponde a su tarea, tanto desde el punto de vista cuantitativo como cualitativo y de las personas que dependen de él.
6. *Enfoque de "Informática hacia el usuario"*. El usuario es nuestra razón de ser como productores de servicios. El usuario finalmente es quien administra los sistemas de información y es libre de elegir, rechazar o reclamar, lo mas importante no es nuestro servicio, sino "su" satisfacción.
7. *Actitud proactiva.* No se trata de corregir errores que se hayan presentado y diseñar controles minuciosos para corregirlos; es necesario cambiar nuestra concepción de la tarea, lo que significa hacerlo bien desde la primera vez.
8. *Rentabilidad de la calidad para la empresa y para cada persona.* La calidad siempre es rentable para la empresa, aunque se tenga que invertir, equivale a la satisfacción de usuarios internos y clientes externos, y para el personal que actúa con calidad, por su satisfacción íntima y por los beneficios tangibles que pueda representar trabajar bien.
9. *La calidad inmersa en un proceso de mejora y aprendizaje continuo.* Es un proceso dinámico y continuo en donde está inmersa la organización, el área de informática y los usuarios. Exige nuevos retos, una mejora continua a los sistemas y procesos, un aprendizaje y tecnología de punta, así como aportación de nuevas ideas.

[51] Como las mundialmente utilizadas normas ISO 9000
[52] Gasalla José María, "La nueva dirección de personas, marco paradójico del talento directivo", Ed. Sicco

IV.3 Control de aplicaciones

Control de los datos fuente.

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

- Procedimientos para la preparación de datos.
- Diseño de documentos fuente.
- Control de documentos fuente.
- Procedimientos de autorización de entrada
- Procedimientos para documentación y control de la operación
- Vigencia de los documentos fuente.

Consideraciones para la Normatividad

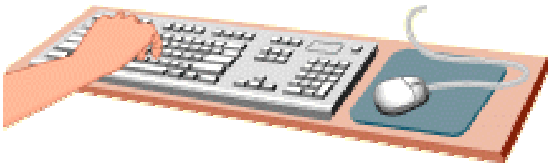
Fuente: Aguilar Castillo Gildardo, "Apuntes para la materia Administración de Recursos Informáticos", Facultad de Estadística e Informática, Universidad Veracruzana. México, 1998

La información sometida a procesamiento debe ser autorizada, integrada, preparada y transmitida, en forma adecuada.

- El departamento usuario debe tener procedimientos establecidos para preparar los datos.
- Los documentos fuente deben ser diseñados en forma tal que minimicen los errores y las omisiones.
- Se deben considerar todas las medidas de seguridad pertinentes para documentos que impliquen un valor intrínseco.
- Los documentos fuente en blanco deben estar custodiados por personas que no están involucradas en la generación de estos documentos, las funciones de aprobación y de generación de los documentos fuente deben ser independientes una de otra.
- Deben establecerse los procedimientos de autorización adecuados para la entrada de los datos.
- Implementar procedimientos de seguridad como Password, cuentas, permisos, diferentes niveles de acceso, etc.
- Todos los procedimientos de control de información deben estar completamente documentados.
- Incluir procedimientos automáticos de control que no permitan un procesamiento erróneo o fuera de secuencia.
- Los documentos fuente deben ser retenidos para facilitar la recuperación o la reconstrucción de la información.
- Se debe establecer el periodo de retención de los documentos fuente para evitar gastos de almacenamiento.

Control de los datos de entrada

Fuente "Análisis y Diseño de Sistemas de Información", James A Senn Segunda Edición Mc Graw Hill 1992



El diseño de la entrada consiste en el desarrollo de especificaciones y procedimientos para la preparación de datos, la realización de los pasos necesarios para poner los datos de una transacción en una forma utilizable para su procesamiento. La entrada de los datos se logra al instruir a la computadora para que los lea ya sea de documentos escritos o impresos, o por personas que los escriben directamente en el sistema. Los objetivos que sirven de guía para el diseño de la entrada se abocan a controlar la cantidad de entrada requerida, a evitar los retrasos, a controlar los errores y a mantener la sencillez de los pasos necesarios.

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

- Ubicación de los datos de entrada.
- Procedimientos para conversión y entrada de datos.
- Procedimientos de conversión y entrada en línea.
- Validación y edición de datos.

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 datos de entrada para procesarse deben ser validados y editados lo más cerca posible del punto de origen.
- Los procedimientos para el manejo de errores deben colocarse en el lugar apropiado, para facilitar la reentrada oportuna y precisa, de todos los datos corregidos.
- Deben estar establecidos los procedimientos para la conversión y la entrada de los datos, que garanticen la separación de tareas, así como la rutina de verificación del trabajo realizado en el proceso de entrada de datos.
- Deben estar establecidos los procedimientos relativos a la conversión y entrada de los datos a través de terminales para disuadir el uso no autorizado o el mal uso.

Control del procesamiento de los datos.

La tecnología hoy día ha dado lugar a muchas formas de procesar datos, y las organizaciones deben seleccionar la forma que mejor convenga a sus necesidades, deben decidir qué hardware, software y qué enfoque de procesamiento de datos debe adoptar. Esta decisión regirá la operación día tras día del departamento de procesamiento de datos y la forma como los usuarios recibirán la información procesada por la computadora.

Fuente: http://www.inf.unitru.edu.pe/docs/telp

Procesamiento en lotes (Batch)

Modalidad de procesamiento en el que, el usuario envía lotes de información para ser procesados y espera por la respuesta, la que puede demorar algunos minutos, horas o quizá días, dependiendo de la instalación. Las características principales son: la no existencia de una interacción entre el usuario y la máquina y el agrupamiento de equipos de cómputo.

El procesamiento en lotes, es una técnica ampliamente empleada que implica el procesamiento regular de grandes cantidades de datos, los datos se reúnen durante un periodo pre-determinado de tiempo, después del cual se procesan. El proceso de una nómina es un buen ejemplo de procesamiento en lotes, los datos de nómina se acumulan durante un periodo de una o dos semanas y se procesan a intervalos regulares, los cheques se distribuyen a todos los empleados en periodos pre-determinados.

Procesamiento de lotes en línea .

En un típico sistema en línea, los datos se trasmiten en tiempo real a la computadora y se procesan, sin embargo un sistema de procesamiento Batch en línea, puede también realizar las actividades relativas al procesamiento de lotes, los datos se acumulan durante un tiempo y se transmiten a la computadora a intervalos regulares. El proceso de esta información puede llevarse a cabo inmediatamente o retrazarse hasta que el sistema esté desocupado, en cualquier caso, la aceptación de estos datos acumulados será una señal para la computadora de que puede iniciarse el proceso.

Administración de procesos

Los sistemas operativos actuales proveen mecanismos y herramientas para manejar de manera eficiente, segura y amigable éste tipo de trabajos. En vez de ser ejecutados inmediatamente después de ser ingresados, los trabajos quedan en colas de procesos y van siendo atendidos a medida que los recursos requeridos están disponibles. Se asegura así que un trabajo es procesado con los recursos que necesita.

Las colas pueden acceder a todos los servidores o sólo a algunos de ellos si el administrador lo estima conveniente. Se configuran además de acuerdo a los tipos de trabajos que deben procesar y políticas de uso local, etc.

Por ejemplo existen colas para trabajos de alto riesgo que requieran mucho recurso de disco o memoria, largas impresiones, etc. También existen colas con prioridades, horarios tales como cola nocturna, etc. Mediante el uso de colas, se pueden enviar gran cantidad de trabajos sin recargar excesivamente el sistema.

Procesamiento de tiempo real.

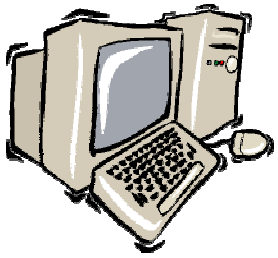
Esta modalidad está diseñada para responder en forma inmediata a las transacciones del usuario. Tiempo real significa sin demora y respuesta instantánea, se procesa cada transacción, según va entrando a la computadora, y le transmite la información resultante al operador, es decir, actualiza la información, requiere archivos de acceso directo. Ejemplo: muchas agencias de viajes utilizan este proceso para hacer las reservaciones porque los precios y los espacios disponibles están cambiando constantemente y hay que actualizarlos. Otro ejemplo son los cajeros automáticos de los bancos.

Control de procesamiento

El procesamiento de los datos por programas aplicativos individuales, debe ser controlado para asegurar que ningún dato es agregado, removido o alterado durante el proceso.

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

- Integridad del procesamiento de los datos.
- Manejo de errores en procesamiento de los datos.
- Procedimientos de reproceso.
- Bitácora del sistema o de la consola.



<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 establecerse procedimientos para el procesamiento de los datos que garanticen la separación de tareas, así como una rutina de verificación del trabajo realizado.

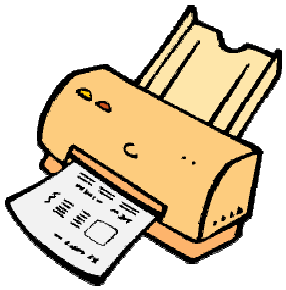
- Cuando sea pertinente, los programas aplicativos deben contener condiciones que en forma rutinaria verifiquen el trabajo realizado durante el proceso de los datos, para promover la integridad de los mismos.
- Los procedimientos para el manejo de errores durante el procesamiento de los datos, deben identificar las transacciones erróneas sin que sean procesadas y sin que haya interrupciones excesivas del procesamiento de otras transacciones válidas.
- Los procedimientos deben prohibir que un operador anule etiquetas o errores de dispositivos.
- La intervención del operador debe ser restringida tanto como sea posible.
- Debe existir un método para reiniciar o reprocesar un trabajo después de que se han detectado errores de procesamiento.
- Las fallas del equipo, la recuperación de errores y los procedimientos de reinicio y de alto, deben estar claramente documentados y deben ser revisados periódicamente.
- Debe mantenerse una bitácora del sistema o de la consola, con todas las actividades de cómputo, para la revisión y resolución de errores del sistema o del operador.

BITACORA DE CONTROL			**SISTEMA:**			**FECHA:**		
FOL:	SIST:	FUN:	NOMBRE:	INI:	TER:	DUR:	N.DISP:	CIFRAS

Control de la salida de la información.

Los reportes de salida resultantes del procedimiento deben ser revisados en cuanto a su racionabilidad y distribución oportuna a los destinatarios autorizados.

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



- Revisión de la salida
- Conciliación y balanceo de resultados
- Distribución de las salidas o resultado
- Manejo de errores en salidas
- Manejo y retención de la salida
- Medidas de seguridad para los reportes de salida

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 reportes de salida deben ser revisados en cuanto a forma e integridad.
- La salida debe ser balanceada contra los totales de control, las pistas de auditoría deben estar disponibles para facilitar el rastreo y la conciliación.
- La distribución de las salidas debe estar de acuerdo con las instrucciones escritas.
- Deben existir procedimientos para reportar y controlar los errores contenidos en las salidas.
- Deben estar establecidos los procedimientos para manejo y retención de la salida.
- Deben estar documentadas las medidas de seguridad de los reportes de salida que están esperando ser distribuidos.

Sistemas soportados en bases de datos

Una base de datos es una colección de datos o archivos relacionados de una manera estructurada, almacenados electrónicamente y pueden ser editados, unidos, organizados y hasta permite hacer búsqueda. Es un método de organizar información en un formato uniforme.

Las personas desarrollan las bases de datos para organizar, hacer búsqueda, desarrollar informes y accesar información. Para poder llevar a cabo estas funciones, controladas por los usuarios, se diseñó un programa llamado sistema de manejo de bases de datos,[53] es un programa de aplicación que ayuda a manejar los datos en más de un archivo a la vez. También permite definir la relación entre los tipos de registros.

La clave para que una base de datos sea efectiva está en el diseño de la estructura. Esta debe permitir que los datos puedan ser manipulados con flexibilidad y que suministre la información requerida que ayude a tomar decisiones correctas.

En el desarrollo de sistemas soportados en bases de datos, el control, la integridad y la seguridad de los datos compartidos por múltiples usuarios deben ser considerados, todos los componentes que integran un medio ambiente de bases de datos deberán ser descritos.

[53] Se reconoce también como "Database Management System (DBMS)"

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

- Sistemas de administración de bases de datos (dbms).
- Responsabilidad de la administración de las bases de datos.
- Descripciones y cambios de datos.
- Procedimientos de recuperación de bases de datos.
- Integridad de las bases de datos.

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

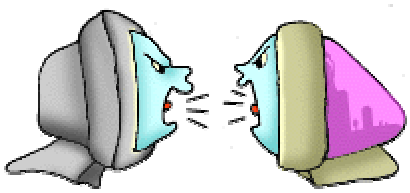
- Debe instalarse el software que proporciona el acceso, la organización y el control sobre los datos compartidos, el sistema de administración de bases de datos.
- Debe instalarse y mantenerse el software de tal manera que asegure la integridad de la base de datos y de los parámetros de control que definen el medio ambiente.
- Debe estar claramente definidas las funciones del administrador de la base de datos y su ubicación en la estructura orgánica que garantice su independencia.
- Deberán estar definidos por escrito los procedimientos relacionados con la descripción, accesos, cambios y mantenimiento del directorio de datos.
- Deberán estar definidas las políticas de respaldo y recuperación de la base de datos a fin de garantizar la integridad de la información.
- Los procedimientos de respaldo y recuperación deben estar por escrito.

Procesamiento distribuido y redes

Procesamiento Distribuido

Fuente: http://www.itlp.edu.mx/publica/tutoriales/telepro/

En el inicio de la era de la informática las computadoras eran grandes y costosas, éstas funcionaban de forma independiente y muy pocas organizaciones contaban con esta herramienta, pero a partir de que los equipos se compactaron y se redujeron costos, los sistemas y la información empezó a descentralizarse, apareció el procesamiento distribuido. El gran salto de un sistema centralizado a un sistema distribuido fue el desarrollo de las comunicaciones y de las redes.



El procesamiento distribuido es una técnica que alivia el gigantesco trabajo de tratamiento masivo de datos que debería hacer una única computadora repartiéndolo entre varias. Y cuantas más, mejor.

Un servidor central le da al procesador de cada máquina de la red una pequeña parte del trabajo y de esta manera, todos los chips trabajan en forma simultánea. En este tipo de procesamiento la terminal se convierte en una estación de trabajo que con el auxilio de un servidor, ejecutan las instrucciones y almacenan los archivos. Al procesarse un programa en una estación de trabajo, se guarda en el servidor para que otros puedan tener acceso a él. Podríamos resumir que el procesamiento distribuido es el uso de varias computadoras para hacer el trabajo de una.

Sistemas Distribuidos

Fuente: http://www.inf.udec.el/~sistcom/sistemas-Distribuidos.htm

Un sistema distribuido es un conjunto de computadoras autónomas ligadas en red que aparecen ante los usuarios del sistema como una única computadora, aunque los sistemas de red solucionan parte de las necesidades actuales de comunicación entre computadoras, tienen importantes limitaciones, y no son aplicables a una gran cantidad de problemas. Por ello surge la necesidad de crear Sistemas distribuidos que sustituyan a los actuales sistemas de red o a los sistemas multiprocesadores

Los sistemas distribuidos están basados en las ideas básicas de:

- Transparencia
- Eficacia
- Flexibilidad
- Escalabilidad
- Fiabilidad

Transparencia

El concepto de transparencia de un sistema distribuido va ligado a la idea de que todo el sistema funcione de forma similar en todos los puntos de la red, independientemente de la posición del usuario.

Eficacia

La idea base de los sistemas distribuidos es la de obtener sistemas mucho más rápidos que los ordenadores actuales. Es en este punto cuando nos encontramos de nuevo con el paralelismo. Para lograr un sistema eficiente hay que descartar la idea de ejecutar un programa en un único procesador de todo el sistema, y pensar en distribuir las tareas a los procesadores libres más rápidos en cada momento.

Flexibilidad

Un proyecto en desarrollo como el diseño de un sistema operativo distribuido debe estar abierto a cambios y actualizaciones que mejoren el funcionamiento del sistema.

Fiabilidad

Un sistema distribuido puede construirse de forma que sea más fiable que un sistema centralizado, al no depender de un solo nodo y facilitar la replicación de funciones y de datos en los distintos nodos de la red.

Procesamiento en Paralelo

Fuente:http://www.espe.edu.ec/websites/sistemas/tema/paralelo.htm

Parece claro que a pesar de los avances tecnológicos conseguidos en los últimos años, la tecnología del silicio está llegando a su límite. Si se quieren resolver problemas más complejos y de mayores dimensiones se deben buscar nuevas alternativas tecnológicas.

Una de estas alternativas en desarrollo es el paralelismo. Mediante el paralelismo se pretende conseguir la distribución del trabajo entre las diversas CPU's disponibles en el sistema de forma que realicen el trabajo simultáneamente, con el objetivo de aumentar considerablemente el rendimiento total.

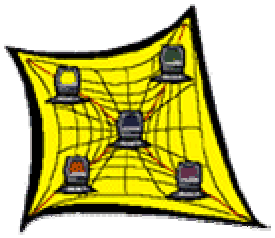
Procesar en paralelo consiste esencialmente en usar más de dos procesadores para que trabajen de manera cooperativa y simultánea en la solución de un problema. La distribución de tareas y de datos están íntimamente relacionadas; generalmente la distribución de tareas indica como deben distribuirse los datos.

Cabe aclarar que muchas veces en un sistema de multiprogramación, la CPU alterna de un programa a otro, ejecutando cada uno durante milisegundos, y conmutando a otro inmediatamente, de tal forma que al usuario se le proporciona cierta sensación de ejecución paralela, como si el ordenador realizase varias tareas al mismo tiempo. Aunque, estrictamente, la CPU ejecuta en un determinado instante un solo programa, durante un segundo puede haber trabajado con varios de ellos, dando una apariencia de paralelismo.

Es en estos casos cuando se tiende a hablar de seudo paralelismo, indicando la rápida conmutación entre los programas en la CPU, distinguiéndolo del paralelismo real de hardware, donde se realizan cálculos en la CPU a la vez que operan los dispositivos de E/S. Ya que es complicado controlar las distintas actividades paralelas, los diseñadores de sistemas emplean el modelo de procesos para facilitar la utilización del paralelismo.

Operación de procesamiento distribuido y de redes.

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



- Comprensión de los objetivos del modo de procesamiento.
- Instalación de la red
- Estándares para el control de operación de las redes.
- Políticas de seguridad respecto a la red.
- Revisión post-implantación de la red.

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

Comprensión de los objetivos del modo de procesamiento.

- El procesamiento distribuido debe promover el abastecimiento de información sobre una base descentralizada.
- Deben estar definidos los procedimientos para operar con procesamiento distribuido, en forma controlada y segura.
- Las decisiones de la gerencia para emprender procesamiento distribuido deben estar documentadas y soportadas en análisis de costo-beneficio.
- Deben haber sido desarrollados planes para la implantación, conversión y prueba de aceptación adecuadas de la red.
- El uso actual o planeado de los datos y de las bases de datos debe estar clasificado de acuerdo con el grado de distribución, como base para una evaluación posterior de los controles y de la seguridad requerida.

Instalación de la red

- Debe preverse la preparación de un local que incluya aspectos como la ventilación del local, una fuente de energía amplia, y una buena elección del cable.
- La configuración debe incluir la preparación del disco duro, la instalación de las tarjetas de interfaz de la red, la instalación del sistema operativo y la configuración y verificación de las impresoras de la red

Estándares para el control de operación de las redes.

- Los estándares y políticas para el control general de la red deben estar claramente establecidos, actualizados y ser operativos.

- Los estándares deben reflejar los mismos objetivos del sistema, así como la capacidad de distribución y la arquitectura general de la red.
- Las facilidades de control del software y de hardware requerido, deben estar documentadas, adquiridas o desarrolladas, las ya existentes deben utilizarse.
- Debe haber controles y entrenamiento adecuados respecto de los datos distribuidos, para asegurar la compatibilidad, la integridad y el uso efectivo de los datos.
- Deben estar totalmente establecidos los requerimientos de salida de la red, la secuencia de operación, los procedimientos del proceso y las políticas de coordinación de localidades.
- Debe existir dentro de la red, un software de comunicaciones efectivo y controlado.
- Los recursos de la red y el mantenimiento preventivo deberán ser adecuadamente administrados y controlados.
- Debe proporcionarse la documentación y el entrenamiento adecuado a todo el personal de operaciones de la red.

Políticas de seguridad respecto a la red.

- Debe existir la seguridad adecuada sobre los datos controlados por los sistemas de administración de la base de datos de la red.
- Seguridad sobre los procesadores de aplicaciones y transacciones.
- Seguridad sobre los datos manejados en las instalaciones de procesamiento de la red y en las localidades remotas.
- Debe existir un procedimiento para asegurar el control continuo sobre los activos y los recursos físicos, en todas las localidades de la red.
- Deben existir políticas de respaldo de software y hardware para la red.
- Debemos considerar aspectos como la seguridad del login y Password, la seguridad del directorio, los atributos de seguridad de los ficheros y directorios
- Debe existir la seguridad adecuada para el acceso y para los cambios a los sistemas operativos del software de la red.
- Deben estar previstos los mecanismos de seguridad adecuados para restringir el acceso a las instalaciones de procesamiento de la red, a terminales y a sistemas.
- Cuando es apropiado debe considerarse la protección de los datos altamente sensitivos, por medio de la decodificación.
- Las operaciones de la red deben estar garantizadas por planes de respaldo y contingencia apropiados.
- Deben ser efectuadas revisiones regulares de seguridad por los usuarios de la red.

Revisión post-implantación de la red.

- Debe haber un mecanismo para asegurar las revisiones de post-implantación de la red y determinar si todos los sistemas de la red y los requerimientos del usuario se han logrado.
- Deben establecerse los mecanismos de control del funcionamiento de la red, para garantizar su efectiva utilización, el nivel de carga, el control y el reporte completo de su rendimiento.

Sistemas en micro computadoras

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

- Políticas de la Gerencia General.
- Estándares para el control de operación.
- Acceso a los recursos de micro computación y políticas de seguridad..
- Evaluaciones operativas.

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

Políticas de la Gerencia General.

- La adquisición y la utilización de micro computadoras debe ser planeada con la participación de la gerencia usuaria.
- La gerencia debe establecer políticas de la adquisición y utilización de micro computadoras en la organización.
- La gerencia debe establecer un criterio de adquisición de micro computadoras y aprobar estas adquisiciones, con base en consideraciones de costo-beneficio.
- La gerencia debe establecer lineamientos relacionados con el desarrollo y adquisición de software aplicativo.

Estándares para el control de operación.

- Los programas aplicativos deben ser catalogados y los listados de programas deben ser documentados.
- Cuando los programas aplicativos son compartidos entre usuarios de micro computadoras, los procedimientos deben proveer el registro de la actividad del usuario.

Acceso a los recursos de micro computación y políticas de seguridad..

- Se deben establecer los procedimientos relacionados con la obtención del acceso a micro computadoras y a otros recursos de cómputo.
- Debe existir una evaluación de los riesgos asociados con el uso de micro computadoras.
- Deben existir lineamientos para el respaldo de programas y archivos, así como para su resguardo.
- Deben existir controles adecuados para evitar que las micro computadoras sean robadas o sufran actos de vandalismo.

Evaluaciones operativas.

- La gerencia debe revisar periódicamente la utilización de las micro computadoras.
- Debe haber un mecanismo para asegurar las revisiones de post-implantación de las micro computadoras y determinar si todos los requerimientos del usuario se han logrado.
- Deben establecerse los mecanismos de control de la operación de las micro computadoras, para garantizar su efectiva utilización y el reporte completo de su rendimiento.

Sistemas de tiempo compartido

El uso de un servicio de tiempo compartido e Internet, debe estar basado en consideraciones de costo-beneficio. Debe mantenerse un nivel satisfactorio de seguridad y control sobre todas las personas que tienen acceso a los servicios.

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

- Análisis de costo-beneficio.
- Selección del proveedor de servicios.
- Contrato de servicios de tiempo compartido e Internet.
- Identificación y verificación del usuario.
- Controles para la protección.
- Manual del usuario.
- Facturación del servicio.

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 análisis de costo-beneficio que justifican la utilización de las facilidades de tiempo compartido deben realizarse antes de la contratación de tales servicios.
- Deben establecerse los criterios para la selección del proveedor de servicios de tiempo compartido e Internet y debe documentarse la decisión para seleccionar a un proveedor específico.
- Los términos de los servicios que va a proporcionar el proveedor de servicios de tiempo compartido e Internet deben establecerse a través de un contrato.
- Deben existir controles de verificación de usuarios para asegurar que las funciones realizadas por cada usuario estén debidamente autorizadas
- Los controles para la protección de programas deben ser diseñados para prevenir que un usuario dañe y/o destruya los trabajos, programas y archivos de otro usuario.
- El sistema operativo deberá proporcionar seguridad de manera tal que los usuarios puedan proteger sus propios archivos.
- Debe haber las instalaciones de cómputo adecuadas para proporcionar un tiempo de respuesta, eficiente y efectivo para el usuario.
- Deben existir procedimientos de respaldo para mantener respaldos adecuados de archivos y programas.
- Debe existir un manual del usuario que propiamente especifique las operaciones del sistema, procedimientos de navegación y de utilización de utilerías.
- Las facturas presentadas por servicio de tiempo compartido e Internet deben ser verificadas contra los registros de actividad de estaciones de trabajo antes de que se apruebe su pago.

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 Área 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: Nombre de Usuario: Identifica unívocamente la cuenta del usuario., 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:

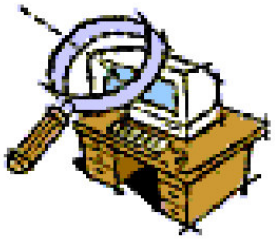
1. Elegir claves con una longitud mínima de 9(nueve) caracteres.
2. No elegir palabras del diccionario.
3. No elegir sustantivos, adjetivos y cualquier otro tipo de información de fácil relación con su persona.
4. No elegir nombres y/o apodos personales, de familiares, de amigos o de compañeros de trabajo.
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.

IV.5 Auditorías.



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

Auditoría externa.- Las responsabilidades de los auditores externos se refieren de manera fundamental a estatutos legales, sus responsabilidades están claramente definidas por la ley,[54] su función principal es revisar las funciones de un centro de cómputo y expresar su opinión acerca de la actuación que tienen cada una de las áreas con respecto a la normatividad gubernamental.[55]

Auditoría interna.- Las responsabilidades de los auditores internos varían de una empresa a otra, pues sus función es realizar evaluaciones operativas cuyos hallazgos y recomendaciones se reportan a la gerencia sin que trascienda de la institución.[56] Dentro de la estructura organizacional, el área de Auditoría interna regularmente se encuentra a nivel staff, dependiendo directamente de la alta gerencia, este grupo realizará supervisiones independientes y reporta sus hallazgos y recomendaciones a la alta gerencia. Las funciones y responsabilidades de la Auditoría interna deben estar claramente definidas y diferenciadas con respecto a las funciones de control de calidad, debe establecerse por escrito, el alcance, el programa de trabajo y las recomendaciones de las revisiones que se realicen, además de establecerse un procedimiento para el seguimiento y atención a las recomendaciones que se presenten.

La función de auditoria interna en los sistemas debe ser muy activa, en el proceso de desarrollo, su diseño debe garantizar la incorporación de medidas adecuadas de seguridad y puntos de verificación. En los sistemas ya implantados, debe revisar que en las áreas usuarias y en el centro de cómputo existan controles de proceso y de seguridad para las aplicaciones. Otras funciones consisten en la revisión de las políticas y procedimientos de seguridad para con los datos, equipo y gente. Revisar las pruebas y simulacros a los procedimientos de seguridad, respaldos y recuperaciones, las instalaciones eléctricas y de acondicionamiento, los mantenimientos preventivos y correctivos de los equipos de cómputo y auxiliares.

La función de auditoria interna en la administración incluye evaluar la estructura orgánica y la descripción de los puestos con respecto a la realidad, revisar los programas de trabajo y la aplicación del presupuesto de operación asignado, evaluar los procedimientos establecidos en cuanto al enlace con los usuarios para los sistemas en producción, asesoría y atención a fallas de software y hardware, solicitud de mantenimiento a sistemas implantados, desarrollo de nuevas aplicaciones. Evaluar las estrategias de administración de los recursos de personal, técnicos y materiales.

[54] Entiéndase a las instituciones gubernamentales tales como la Secretaria de Hacienda, Comercio, Salud...
[55] Es importante no confundir a los auditores externos contratados para las revisiones de auditoría, se llaman externos porque no pertenecen a la organización, sin embargo sus funciones corresponden a las de auditoría interna.
[56] En Instituciones Gubernamentales trascienden los hallazgos a otras instituciones normativas tales como la Contraloría de la Federación, Programación y Presupuesto etc.

Informe final

La función de la Auditoría se materializa exclusivamente por escrito, resulta evidente la necesidad de redactar borradores e informes parciales previos al informe final, los que son elementos de contraste entre opinión entre auditor y auditado y que pueden descubrir fallos de apreciación en el auditor.

El informe comienza con la fecha de inicio de la Auditoría y la fecha de redacción del mismo, se incluyen los nombres del equipo auditor y los nombres de todas las personas entrevistadas, con indicación de la jefatura, responsabilidad y puesto de trabajo que ostente. Se debe incluir la definición de objetivos y alcance de la Auditoría, se enumeran los temas objeto de la auditoría lo más exhaustivamente posible. En el cuerpo expositivo, para cada tema, se seguirá el siguiente orden a saber:

a. Situación actual. Cuando se trate de una revisión periódica, en la que se analiza no solamente una situación sino además su evolución en el tiempo, se expondrá la situación prevista y la situación real.
b. Tendencias. Se tratarán de hallar parámetros que permitan establecer tendencias futuras.
c. Puntos débiles y amenazas.
d. Recomendaciones y planes de acción. Constituyen junto con la exposición de puntos débiles, el verdadero objetivo de la Auditoría interna.

La carta de introducción, tiene especial importancia porque en ella ha de resumirse la Auditoría realizada. Se destina exclusivamente al responsable máximo de la empresa, o a la persona concreta que encargó o contrató la Auditoría, proporcionará una conclusión general, presentará las debilidades en orden de importancia y gravedad, en la carta de Introducción no se escribirán nunca recomendaciones.

Bibliografía de este capítulo:

1. IMSS, "Efectividad directiva", Ed. IMSS, México, 1989.
2. David H. Li, "Auditoría en centros de cómputo: Objetivos, lineamientos y procedimientos", 1ª Ed. Trillas, México, 1992
3. Aguilar Castillo Gildardo, "Apuntes para la materia Administración de Recursos Informáticos", Facultad de Estadística e Informática, Universidad Veracruzana. México, 1998
4. James A Senn, "Análisis y Diseño de Sistemas de Información", Segunda Edición Mc Graw Hill 1992
5. http://www.inf.unitru.edu.pe/docs/telp
6. http://www.itlp.edu.mx/publica/tutoriales/telepro/
7. http://www.inf.udec.el/~sistcom/sistemas-Distribuidos.htm
8. http://www.espe.edu.ec/websites/sistemas/tema/paralelo.htm
9. http://www.planeta-redvista.com.ar (Nov/2000)
10. Fuente: http://www.planeta-redvista.com.ar (Por Néstor O. de los Santos)