INGENIERÍA DE SOFTWARE AVANZADA

(SESIÓN 6)

3.ESTUDIO DEL SISTEMA DE CONTROL INTERNO

3.1 Controles en aplicaciones y sistemas de gestión

Objetivo: Conocer las principales características de un sistema de control interno que brinde seguridad ante posibles riesgos

3.1 Controles en aplicaciones y sistemas de gestión

Los principales **objetivos** que constituyen a la auditoría Informática son el **control de la función informática**, el análisis de la eficiencia de los Sistemas Informáticos que comporta, la verificación del cumplimiento de la Normativa general de la empresa en este ámbito y la revisión de la eficaz gestión de los recursos materiales y humanos informáticos.

CONTROLES

Conjunto de disposiciones metódicas, cuyo fin es vigilar las funciones y actitudes de las empresas y para ello permite verificar si todo se realiza conforme a los programas adoptados, órdenes impartidas y principios admitidos.

Clasificación general de los controles

Controles Preventivos: Son aquellos que reducen la frecuencia con que ocurren las causas del riesgo, permitiendo cierto margen de violaciones.
Ejemplos: Letrero "No fumar" para salvaguardar las instalaciones.
Sistemas de claves de acceso.

Controles detectivos: Son aquellos que no evitan que ocurran las causas del riesgo sino que los detecta luego de ocurridos. Son los más importantes para el auditor. En cierta forma sirven para evaluar la eficiencia de los controles preventivos.

Ejemplo: Archivos y procesos que sirvan como pistas de auditoría.
Procedimientos de validación.

Controles Correctivos: Ayudan a la investigación y corrección de las causas del riesgo. La corrección adecuada puede resultar difícil e ineficiente, siendo necesaria la implantación de controles detectivos sobre los controles correctivos, debido a que la corrección de errores es en si una actividad altamente propensa a errores.

Principales Controles físicos y lógicos

Controles particulares tanto en la parte física como en la lógica se detallan a continuación:

Autenticidad: Permiten verificar la identidad Passwords
Firmas digitales

Exactitud: Aseguran la coherencia de los datos
Validación de campos
Validación de excesos

Totalidad**:** Evitan la omisión de registros así como garantizan la conclusión de un proceso de envío
Conteo de registros
Cifras de control

Redundancia: Evitan la duplicidad de datos
Cancelación de lotes
Verificación de secuencias
Privacidad: Aseguran la protección de los datos
Compactación
Encriptación

Existencia: Aseguran la disponibilidad de los datos
Bitácora de estados
Mantenimiento de activos

Protección de Activos: Destrucción o corrupción de información o del hardware
Extintores
Passwords

Efectividad: Aseguran el logro de los objetivos
Encuestas de satisfacción
Medición de niveles de servicio

Eficiencia: Aseguran el uso óptimo de los recursos
Programas monitores
Análisis costo-beneficio Controles automáticos o lógicos

Periodicidad de cambio de claves de acceso

Los cambios de las claves de acceso a los programas se deben realizar periódicamente. Normalmente los usuarios se acostumbran a conservar la misma clave que le asignaron inicialmente.

El no cambiar las claves periódicamente aumenta la posibilidad de que personas no autorizadas conozcan y utilicen claves de usuarios del sistema de computación.
Por lo tanto se recomienda cambiar claves por lo menos trimestralmente.

Combinación de alfanuméricos en claves de acceso

No es conveniente que la clave este compuesta por códigos de empleados, ya que una persona no autorizada a través de pruebas simples o de deducciones puede dar con dicha clave.
Para redefinir claves es necesario considerar los tipos de claves que existen:

Individuales: Pertenecen a un solo usuario, por tanto es individual y personal. Esta clave permite al momento de efectuar las transacciones registrar a los responsables de cualquier cambio.
Confidenciales: De forma confidencial los usuarios deberán ser instruidos formalmente respecto al uso de las claves.

No significativas: Las claves no deben corresponder a números secuenciales ni a

nombres o fechas.

Verificación de datos de entrada

Incluir rutinas que verifiquen la compatibilidad de los datos mas no su exactitud o precisión; tal es el caso de la validación del tipo de datos que contienen los campos o verificar si se encuentran dentro de un rango.

Conteo de registros

Consiste en crear campos de memoria para ir acumulando cada registro que se ingresa y verificar con los totales ya registrados.

Totales de Control

Se realiza mediante la creación de totales de línea, columnas, cantidad de formularios, cifras de control, etc., y automáticamente verificar con un campo en el cual se van acumulando los registros, separando solo aquellos formularios o registros con diferencias.

Verificación de límites

Consiste en la verificación automática de tablas, códigos, límites mínimos y máximos o bajo determinadas condiciones dadas previamente.

Verificación de secuencias

En ciertos procesos los registros deben observar cierta secuencia numérica o alfabética, ascendente o descendente, esta verificación debe hacerse mediante rutinas independientes del programa en si.

Dígito auto verificador

Consiste en incluir un dígito adicional a una codificación, el mismo que es resultado de la aplicación de un algoritmo o formula, conocido como MODULOS, que detecta la corrección o no del código. Tal es el caso por ejemplo del décimo dígito de la cédula de identidad, calculado con el modulo 6 o el ultimo dígito del RFC calculado con el módulo 7.

Utilizar software de seguridad en los microcomputadores

El software de seguridad permite restringir el acceso al microcomputador, de tal modo que solo el personal autorizado pueda utilizarlo.

Adicionalmente, este software permite reforzar la segregación de funciones y la confidencialidad de la información mediante controles para que los usuarios puedan acceder solo a los programas y datos para los que están autorizados.
Programas de este tipo son: WACHDOG, LATTICE, SECRET DISK, entre otros.

Controles administrativos en un ambiente de Procesamiento de Datos

La máxima autoridad del Área de Informática de una empresa o institución debe implantar los siguientes controles que se agruparan de la siguiente forma:

1.- Controles de Preinstalación
2.- Controles de Organización y Planificación
3.- Controles de Sistemas en Desarrollo y Producción 4.- Controles de Procesamiento
5.- Controles de Operación
6.- Controles de uso de Microcomputadores

1.- Controles de Preinstalación

Hacen referencia a procesos y actividades previas a la adquisición e instalación de un equipo de computación y obviamente a la automatización de los sistemas existentes.

Objetivos:

• Garantizar que el hardware y software se adquieran siempre y cuando tengan la seguridad de que los
sistemas computarizados proporcionaran mayores beneficios que cualquier otra alternativa.
• Garantizar la selección adecuada de equipos y sistemas de computación
• Asegurar la elaboración de un plan de actividades previo a la instalación

Acciones a seguir:

• Elaboración de un informe técnico en el que se justifique la adquisición del equipo, software y servicios de computación, incluyendo un estudio costo-beneficio.
• Formación de un comité que coordine y se responsabilice de todo el proceso de adquisición e instalación

• Elaborar un plan de instalación de equipo y software (fechas, actividades, responsables) el mismo que debe
contar con la aprobación de los proveedores del equipo.
• Elaborar un instructivo con procedimientos a seguir para la selección y adquisición de equipos, programas y
servicios computacionales. Este proceso debe enmarcarse en normas y disposiciones legales.
• Efectuar las acciones necesarias para una mayor participación de proveedores.
• Asegurar respaldo de mantenimiento y asistencia técnica.

2.- Controles de organización y Planificación

Se refiere a la definición clara de funciones, línea de autoridad y responsabilidad de las diferentes unidades del área PAD, en labores tales como:

□□Diseñar un sistema
□□Elaborar los programas □□Operar el sistema
□□Control de calidad

Se debe evitar que una misma persona tenga el control de toda una operación.
Es importante la utilización óptima de recursos en el PAD mediante la preparación de planes a ser evaluados continuamente

Acciones a seguir

• La unidad informática debe estar al mas alto nivel de la pirámide administrativa de manera que cumpla con sus objetivos, cuente con el apoyo necesario y la dirección efectiva.
• Las funciones de operación, programación y diseño de sistemas deben estar claramente delimitadas.
• Deben existir mecanismos necesarios a fin de asegurar que los programadores y analistas no tengan acceso a
la operación del computador y los operadores a su vez no conozcan la documentación de programas y
sistemas.
• Debe existir una unidad de control de calidad, tanto de datos de entrada como de los resultado del
procesamiento.

• El manejo y custodia de dispositivos y archivos magnéticos deben estar expresamente definidos por escrito.
• Las actividades del PAD deben obedecer a planificaciones a corto, mediano y largo plazo sujetos a
evaluación y ajustes periódicos "Plan Maestro de Informática"
• Debe existir una participación efectiva de directivos, usuarios y personal del PAD en la planificación y
evaluación del cumplimiento del plan.
• Las instrucciones deben impartirse por escrito.

3.- Controles de Sistema en Desarrollo y Producción

Se debe justificar que los sistemas han sido la mejor opción para la empresa, bajo una relación costo-beneficio que proporcionen oportuna y efectiva información, que los sistemas se han desarrollado bajo un proceso planificado y se encuentren debidamente documentados.

Acciones a seguir:

Los usuarios deben participar en el diseño e implantación de los sistemas pues aportan conocimiento y experiencia de su área y esta actividad facilita el proceso de cambio
• El personal de auditoría interna/control debe formar parte del grupo de diseño para sugerir y solicitar la
implantación de rutinas de control
• El desarrollo, diseño y mantenimiento de sistemas obedece a planes específicos, metodologías estándares,
procedimientos y en general a normatividad escrita y aprobada.
• Cada fase concluida debe ser aprobada documentadamente por los usuarios mediante actas u otros
mecanismos a fin de evitar reclamos posteriores.
• Los programas antes de pasar a Producción deben ser probados con datos que agoten todas las excepciones
posibles.
• Todos los sistemas deben estar debidamente documentados y actualizados. La documentación deberá contener:
□□Informe de factibilidad

□□Diagrama de bloque
□□Diagrama de lógica del programa
□□Objetivos del programa
□□Listado original del programa y versiones que incluyan los
cambios efectuados con antecedentes
□□de pedido y aprobación de modificaciones
□□Formatos de salida
□□Resultados de pruebas realizadas

• Implantar procedimientos de solicitud, aprobación y ejecución de cambios a programas, formatos de los sistemas en desarrollo.

• El sistema concluido será entregado al usuario previo entrenamiento y elaboración de los manuales de operación respectivos

4.- Controles de Procesamiento

Los controles de procesamiento se refieren al ciclo que sigue la información desde la entrada hasta la salida de la información, lo que conlleva al establecimiento de una serie de seguridades para:

• Asegurar que todos los datos sean procesados • Garantizar la exactitud de los datos procesados

• Garantizar que se grabe un archivo para uso de la gerencia y con fines de auditoría

• Asegurar que los resultados sean entregados a los usuarios en forma oportuna y en las mejores condiciones.

Acciones a seguir:

• Validación de datos de entrada previo procesamiento debe ser realizada en forma automática: clave, dígito
autoverificador, totales de lotes, etc.

• Preparación de datos de entrada debe ser responsabilidad de usuarios y consecuentemente su corrección.

• Recepción de datos de entrada y distribución de información de salida debe obedecer a un horario elaborado
en coordinación con el usuario, realizando un debido control de calidad.

• Adoptar acciones necesarias para correcciones de errores.

• Analizar conveniencia costo-beneficio de estandarización de formularios, fuente para

agilitar la captura de datos y minimizar errores.

• Los procesos interactivos deben garantizar una adecuada interrelación entre usuario y sistema.

• Planificar el mantenimiento del hardware y software, tomando todas las seguridades para garantizar la integridad de la información y el buen

5.- Controles de Operación

Abarcan todo el ambiente de la operación del equipo central de computación y dispositivos de almacenamiento, la administración de la cintoteca y la operación de terminales y equipos de comunicación por parte de los usuarios de sistemas online.

Los controles tienen como fin:

• Prevenir o detectar errores accidentales que puedan ocurrir en el Centro de Cómputo durante un proceso

• Evitar o detectar el manejo de datos con fines fraudulentos por parte de funcionarios del PAD

• Garantizar la integridad de los recursos informáticos.

• Asegurar la utilización adecuada de equipos acorde a planes y objetivos.

Acciones a seguir:

• El acceso al centro de cómputo debe contar con las seguridades necesarias para reservar el ingreso al personal autorizado

• Implantar claves o password para garantizar operación de consola y equipo central (mainframe), a personal autorizado.

• Formular políticas respecto a seguridad, privacidad y protección de las facilidades de procesamiento ante eventos como: incendio, vandalismo, robo y uso indebido, intentos de violación y como responder ante esos eventos.

• Mantener un registro permanente (bitácora) de todos los procesos realizados, dejando constancia de suspensiones o cancelaciones de procesos.

• Los operadores del equipo central deben estar entrenados para recuperar o restaurar información en caso de destrucción de archivos.

• Los backups no deben ser menores de dos (padres e hijos) y deben guardarse en lugares seguros y adecuados, preferentemente en bóvedas de bancos.

• Se deben implantar calendarios de operación a fin de establecer prioridades de proceso.

• Todas las actividades del Centro de Computo deben normarse mediante manuales, instructivos, normas, reglamentos, etc.

• El proveedor de hardware y software deberá proporcionar lo siguiente:

- Manual de operación de equipos
- Manual de lenguaje de programación
- Manual de utilitarios disponibles
- Manual de Sistemas operativos

• Las instalaciones deben contar con sistema de alarma por presencia de fuego, humo, así como extintores de incendio, conexiones eléctricas seguras, entre otras.

• Instalar equipos que protejan la información y los dispositivos en caso de variación de voltaje como: reguladores de voltaje, supresores pico, UPS, generadores de energía.

• Contratar pólizas de seguros para proteger la información, equipos, personal y todo riesgo que se produzca por casos fortuitos o mala operación.

6.- Controles en el uso del Microcomputador

Es la tarea más difícil pues son equipos mas vulnerables, de fácil acceso, de fácil explotación pero los controles que se implanten ayudaran a garantizar la integridad y confidencialidad de la información.

Acciones a seguir:

• Adquisición de equipos de protección como supresores de pico, reguladores de voltaje y de ser posible UPS previo a la adquisición del equipo

• Vencida la garantía de mantenimiento del proveedor se debe contratar mantenimiento preventivo y correctivo.

• Establecer procedimientos para obtención de backups de paquetes y de archivos de datos.

• Revisión periódica y sorpresiva del contenido del disco para verificar la instalación de aplicaciones no relacionadas a la gestión de la empresa.

• Mantener programas y procedimientos de detección e inmunización de virus en copias no autorizadas o datos procesados en otros equipos.

• Propender a la estandarización del Sistema Operativo, software utilizado como procesadores de palabras, hojas electrónicas, manejadores de base de datos y mantener actualizadas las versiones y la capacitación sobre modificaciones incluidas.

Analizados los distintos tipos de controles que se aplican en la Auditoría de Sistemas efectuaremos a continuación el análisis de casos de situaciones hipotéticas planteadas

como problemáticas en distintas empresas, con la finalidad de efectuar el análisis del caso e identificar las acciones que se deberían implementar