UNIVERSIDAD PANAMERICANA

ESCUELA DE CONTADURIA

CON ESTUDIOS INCORPORADOS A LA
UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

AUDITORIA DE SISTEMAS DE INFORMACION

TESIS

QUE PRESENTAN:

LAURA ELENA PALOMAR GUTIERREZ
OSCAR ALEJANDRO ZAVALA SANTOYO

PARA OBTENER EL TITULO DE

LICENCIADO EN CONTADURIA

DIRECTOR DE TESIS
ING. Y C.P. DAVID THIERRY CAMARGO

MEXICO, D. F. 1998

PAGINACION

DISCONTINUA

Esta tesis es un esfuerzo de más personas de las que el lector podría imaginar. Gracias a todos ellos.

Dios:
Gracias por darme la oportunidad de estar aquí. Dame la sabiduría para llevar el triunfo, pero también dámela para entender la derrota.

Mamá:
Gracias a tu integridad y fortaleza que me sirvieron de ejemplo para que juntas completáramos esta meta tan importante en nuestra vidas.

Marcela y Juan Carlos:
Gracias porque logramos este objetivo. Pero no olviden que sólo es el primer paso, ya que nos faltan dos pasos más para sembrar lo que en el futuro cosecharemos.

Abuelito:
Aunque ya no estés aquí, te agradezco infinitamente que hayas sido mi guía en los momentos más difíciles. QEPD

Abuelita:
Gracias por tu apoyo incondicional y tenacidad, sin ellos hubiera sido imposible salir adelante.

Karla:
Puedes olvidar a la gente con la que has reído, pero nunca podrás olvidar a los amigos con quiénes has llorado.¿Te acuerdas que pensamos que era imposible llegar al final? Pues parece que no. Mil gracias por tu amistad ilimitada. Peñis.

Pepe:
De ahora en adelante sé que con nuestro amor y esfuerzo, compartiremos muchos triunfos juntos. Nunca olvides que te amo.

Más que todos los agradecimientos que pudiera darles, se han llevado mi corazón. Los quiero mucho.

Reconocimientos:

Agradezco profundamente a David Thierry por sus consejos, apoyo y paciencia.

Un agradecimiento muy especial a mis amigos de Galaz e IBM porque sin ustedes hubiera sido imposible realizar esta Tesis.

Gracias a mis maestros que me han dado los conocimientos para enfrentar una nueva etapa en mi vida.

Y por último gracias a la UP por enseñarme, que en la vida profesional, más allá de los conocimientos, esta la integridad.

INTRODUCCIÓN

Dia con dia nos enfrentamos a avances tecnológicos basados siempre en un espíritu de innovación y servicios en beneficio del hombre, mismos que han llevado a la industria de la computación a límites inimaginables. Dichas evoluciones tecnológicas son producto de un intenso trabajo e inversiones de capital substanciales en investigación y desarrollo que están causando una revolución en la participación acelerada de la informática en todas las actividades humanas. El campo de aplicación o de utilización de los computadores cada vez es mayor, ya casi no hay operaciones que no sean registradas, procesadas o controladas por medios automatizados.

Con el advenimiento de las computadoras y sus amplias y desarrolladas capacidades, la mayor parte de las actividades de procesamiento de datos que previamente eran realizadas individualmente por muchos departamentos, se han consolidado a la fecha en uno o muy pocos medios magnéticos de almacenamiento de datos (cintas, discos) los cuales son procesados por un computador el cual "simultáneamente" sirve a un número de usuarios.

El resultado es que el usuario es cada vez más dependiente del computador y en general de la organización que lo administra, mas aún, el proceso ha llegado al punto de que el usuario no podria retornar a su modo manual y mantener su operación de manera efectiva y eficiente.

Hoy en dia el poder de procesamiento de una computadora central puede ser distribuido ampliamente a través de una red de comunicaciones a cientos y aun a miles de personas que trabajan en las terminales o en pequeñas computadoras conectadas al computador central. El advenimiento del microprocesador central, ha hecho posible equipar a estas estaciones de trabajo con una gran variedad de funciones, desde las más simples hasta las más complejas.

Nuestro pais no permanece ajeno a este explosivo desarrollo. El crecimiento de esta industria en México se ha manifestado en la multiplicación de empresas manufactureras

de equipos de computación, distribuidoras, proveedoras de servicio técnicos, de mantenimiento, educación y programación, proveedoras de partes. Componentes que se integran a los equipos de computo.

Lo que realmente estamos presenciando es una "revolución del computador" que tiene consecuencias potenciales más grandes que la revolución industrial. En tanto que la revolución industrial aprovechó a las máquinas para multiplicar fuerza física del hombre, los computadores pueden aprovecharse para multiplicar el poder de su mente.

Hoy es factible emplear la computadora en aplicaciones que hasta hace unos pocos años habrian sido impracticables desde un punto de vista económico.

Mientras en el pasado las computadoras solian estar protegidas por paredes de vidrios y eran usadas solamente por los especialistas, el poder de computación a través de las unidades de entrada y de salida ha ido adelante y estima que millones de usuarios tendrán sus cuentas bancarias en sus hogares.

Actualmente el uso de sistemas de información forma una parte importante en las estrategias de crecimiento de cualquier Compañia que pretenda mantenerse al dia en el mercado económico.

Es indudable que las facilidades que brinda son muchas, entre ellas:

- Rapidez en los distintos procesos
- Capacidad de memoria ilimitada (Secundaria)
- Manejo eficiente de datos, etc.

De ahí la considerable disminución de costos y el aumento de la velocidad del tiempo de acceso.

La información financiera es una de las áreas que se ha visto más beneficiada, por lo que el concepto de "arrastrar el lápiz" se ha visto desplazado por los distintos programas

existentes en la actualidad. Esto ha provocado que para la adecuada comprensión de la información financiera, sea necesario el dominio de ciertos aspectos de la informática.

El 23 de febrero de 1984, la primera pagina de Business Week presentaba el siguiente titular a toda plana "Software: The New Driving Force". Reconociendo a este titular como presagio que se empezaba a comprender la importancia del software de computadoras.

En esencia, el software es normalmente el factor que marca la diferencia. La suficiencia y oportunidad de la información dada por el software (y bases de datos relacionadas) diferencian a una compañía de sus competidoras. (Ingeniería del Software un enfoque práctico; Roger S. Pressman).

Este cambio ha traído consigo algunas serias implicaciones y ha introducido nuevos problemas así como peligros de exponerse a sufrir pérdidas potenciales. Es por eso considerab e la importancia que debemos darle a este tipo de actividades, lo que implica que los riesgos de un mal funcionamiento deben deducirse independientemente de que el uso de los equipos y sistemas sean realizados correctamente y de manera eficiente.

La circunstancia propicia para un fraude por computador que debiera causar mayor preocupación se da en la posibilidad que tiene el programador de manipular el computador como si fuese un titere. Un programador no necesita tener acceso directo al equipo de computo, y puede obtener el control de grandes cantidades de activos emitiendo programas con rutinas suficientemente interconectadas para realizar un fraude.

Se ha observado que son pocas las compañías que tienen controles internos lo suficientes eficientes para provenir o detectar confiablemente los actos de fraude o robo por computador. En comparación con los otros problemas existentes el riesgo es menor. Esto no quiere decir que carezca de importancia sino que existen otros problemas que demandan mayor consideración.

Los registros de los negocios constituyen "activos de información virtuales" de la organización, que si bien no son negociables, estos pueden ser más importantes para

operación exitosa del negocio que si llegasen a dañarse o inclusive a destruir pueden poner en peligro la existencia misma del negocio.

El riesgo que representa la concentración de estos activos no se limita a la destrucción por catástrofes. Los errores diarios de operación también pueden tener consecuencias masivas.

Las fuentes más grandes de pérdidas originadas por computadores son los errores u omisiones inocentes. Aun cuando las comptadoras son muy confiables en cuanto a lo que hacen, solo realizan aquello para lo que se les programa y, únicamente con la información que les proporciona el ser humano. Por lo tanto si se les alimenta información "basura", el resultado no podrá ser de mayor calidad. Es importante mencionar que hasta el más mínimo error en ciertos tipos de datos de entrada puede tener un efecto persistente y repetitivo.

Aun con los datos de entrada que le proporcionen a las pomputadoras sean apropiados, estas pueden producir resultados absurdos.

Los problemas de lógica en el procesamiento por computador no se derivan simultánearnente de un proceso natural. La mayoría de los problemas son originados por comunicaciones deficientes o inexistentes entre el personal de procesamiento de datos y los demás miembros de la organización. Sin embargo aún la comunicación perfecta no eliminará todos los problemas.

El porcentaje de errores en funciones programadas es excesivamente elevado, aun las aplicaciones "probadas e infalibles" pueden contener defectos sutiles que persisten por años.

Existe una gran necesidad de controles más efectivos, que se diseñen en forma más económica y confiable. El personal de diseño de sistemas puede estar entrenado en "análisis de sistemas" pero rara vez lo están en diseño de controles.

Muchos de los controles que implantan ni siquiera se reconocen como tales, simplemente representan la manera en que se hacen las cosas. Los auditores, quienes se supone son los expertos en detectar controles, listan numerosos controles que piensan deberían existir, pero pocas veces dan alguna explicación respecto a como llegan a sus conclusiones. Como resultado, los diseñadores de sistemas repiten los mismos errores y omisiones en los sistemas subsecuentes.

La administración eficiente, es lo que hace la diferencia. La administración de procesamiento de datos es una profesión muy nueva. Las normas centrales para administración efectiva de procesamiento electrónico de datos pueden no resultar muy familiares a quienes entran a la profesión.

Definitivamente decidimos aprender a controlar y auditar los computadores de una manera muy confiable y eficiente. Aun cuando las aplicaciones aparenten construir una "inteligencia artificial", no son más que un simple conjunto de instrucciones diseñadas por el hombre.

Sin embargo, si los sistemas no están manejados adecuadamente o no se encuentran debidamente protegidos todos los beneficios producto de las computadoras podrían convertirse en RIESGOS. Existen posibles riesgos por errores voluntarios o involuntarios de parte de los empleados, tales como pérdida de archivos, daños en los sistemas, robo de datos, etc. También existe el riesgo de tener sistemas de aplicación que no lleven a cabo las funciones para las que fueron creados o que contengan errores que antes habían pasado inadvertidos.

El control de este tipo de riesgos no es una tarea fácil y la gente del área de sistemas de información se encuentra ya presionada respondiendo a aquellas necesidades que surgen día con día.

Por ésta razón es indispensable mantener un control sobre los posibles riesgos, siendo uno de los medios más eficientes, la práctica de auditorías a las áreas de sistemas, para evaluar el manejo de los controles propios del área.

De lo anterior se deriva que el impacto en la auditoría de los ambientes de sistemas de información es muy significativo.

La dependencia que tiene la información financiera en los sistemas es cada vez mayor. La integridad y certeza de los Estados Financieros están aseguradas en gran parte, por los controles que se incluyan en sistemas.

Por lo mismo, el papel del auditor interno es indispensable en esta área, revisando el adecuado manejo de los controles y detectando los posibles problemas que vayan surgiendo.

El auditor interno es la comunicación más eficiente entre el área de sistemas y los usuarios de la información financiera.

La revisión o auditoria de sistemas se ha convertido en una parte estándar de los exámenes que realizan tanto los auditores internos como los externos debido a la necesidad de la organización de revisar las actividades de sistemas de información así como garantizar que se cuente con una sólida, eficiente y segura instalación informática.

Por último, los resultados de una revisión de sistemas de información, deberán darnos la pauta de como enfocar nuestras pruebas de auditoría financiera. Asimismo, en la medida como incrementemos nuestro conocimiento en el equipo de cómputo, podremos aprovechar las ventajas que este ofrece en la realización de pruebas a través del computador.

El objetivo de esta tesis es mostrar los aspectos conceptuales básicos con relación a sistemas de información, los riesgos que los mismos implican en el trabajo de auditoría, así como algunas técnicas que se podrán emplear para verificar la existencia de controles en el área, así como definir las mínimas normas que deben ser observadas en una auditoría de sistemas de sistemas de información desde el plan de trabajo, alcances, enfoques, organización del grupo de auditoría, colección de datos, análisis organizacional

del grupo de auditoria, recopilación de datos, análisis organizacional, entrevistas, muestreos, evaluación de la operación, revisiones de áreas de seguridad, seguridad interna, controles administrativos, estándares, estaciones de trabajo, etc., así como los análisis de los resultados, la organización de las conclusiones y hallazgos, reportes a la gerencia y establecer un programa de seguimiento para la corrección de las fallas encontradas. Todo esto dentro de las condiciones más normales que existen dentro del procesamiento electrónico de datos, ya que la auditoria en informática es muy extensa y observar todas las ramas de ésta resulta muy complicado para este estudio.

1. ASPECTOS GENERALES DE AUDITORÍA DE SISTEMAS

1.1 CONCEPTO DE AUDITORIA

- Concepto

Verificar la confiabilidad, veracidad y oportunidad de la información financiera, operacional y administrativa asi como politicas y lineamientos establecidos que han sido observados y respetados para cumplir obligaciones fiscales, juridicas y reglamentos en general.

- Objetivo

Descubrir deficiencias e irregularidades en una función organizacional.
Indicar sus posibles correcciones.
Ayudar a la dirección a fin de lograr una administración eficaz y eficiente.

- Importancia

Es una herramienta especializada para evaluación continua de métodos en todas las áreas de la empresa.

- Beneficios

Determinar si los sistemas y procedimientos establecidos son efectivos para alcanzar objetivos fijados y asegurar cumplimiento de politicas establecidas.
Recomendación para el mejoramiento de políticas, procedimientos y sistemas.
Medio de proveer mayor grado de delegación de autoridad y si es necesario un medio para facilitar descentralización de operaciones.

1.2 AUDITORIA DE SISTEMAS

1.2.1 GENERALIDADES

La auditoría de los sistemas ha tomado un considerable ímpetu en los últimos años debido a:

- Los sistemas son más complejos.

- La necesidad de conocer que hacen los sistemas y como lo hacen se ha convertido en imperativa.
- Los casos de fraude, robo de datos y de grandes errores, nos inducen a ser más precavidos.
- La auditoría "a través o con" el computador es ya indispensable en oposición a la Auditoría "alrededor" del computador.
- La necesidad de preservar las pistas o rastros de auditoría se ha convertido en esencial.
- La necesidad de comprobar la validez de integridad de los sistemas, sus controles y los datos que manejan es también imperativa.

Una breve descripción de como la auditoría está cambiando fue presentada por G.B Horwitz en: "EDP Auditing, the coming of age", (international journal of government auditing, April 1976), quien establece lo siguiente:

Los pasos básicos en la ejecución de una Auditoría, se trate de un sistema computarizado o no, incluyen:

- Revisar lo adecuado de los controles para asegurar que los registros de datos contables son exactos y completos.
- Confirmar que el sistema y sus controles relativos estén funcionando como se definieron.
- Realizar pruebas adicionales a los saldos contables. En la determinación del alcance de este trabajo adicional se tomará en consideración su evaluación de la efectividad del sistema y sus controles.

En cada uno de estos pasos generales, el computador tendrá justamente un impacto en el enfoque de auditoría. Es difícil concebir que un auditor que no está familiarizado con el procesamiento electrónico de datos estará en posibilidad de realmente entender el sistema. Por ejemplo, en un sistema de inventarios perpetuos, como puede el auditor asegurarse que el registro en la cinta o en el disco ha sido actualizado correctamente a menos que "tenga conciencia del funcionamiento del manejo y organización de archivos, etiquetas frontales y de los procedimientos de la actualización de archivos"; como puede sentirse satisfecho de que todos los registros han sido procesados a menos que "él entienda la naturaleza de los controles de lotes de transacciones en BATCH y de registros o etiquetas ".

En muchos casos, especialmente donde el sistema es simple, el auditor puede estar en posibilidad de saltarse al computador y obtener seguridad en su auditoria a través de exámenes extensos de listados detallados, cuando estos existen, pero el precio que tiene que pagar es cuestionable al conducir una auditoria sin el conocimiento de los puntos fuertes y débiles en el control de sistemas.

Resulta tan obvio mencionar que el buen entendimiento de los sistemas y sus controles es tan fundamental para un buen auditor que ya no es a mi parecer una opción para el auditor que se considera un profesional, el contar con los conocimientos y herramientas para llevar a cabo revisiones a entidades y sistemas de Procesamiento Electrónico de Datos.

El auditor no siempre ha considerado toda la extensión que debe dar a los controles del sistema y raramente ha hecho cambios a los programas estándar de auditoria. En la actualidad, auditores inexpertos tienden a tratar a los sistemas computarizados como una entidad separada, y en esta forma les ha resultado sencillo detectar algunas debilidades en los puntos de transferencia de información y/o de control entre los procesadores y los grupos de usuarios. Muchos auditores han identificado debilidades de control existentes por la falta de entendimiento entre el personal de auditoria de sistemas y usuarios.

También muchos auditores revisan los controles de entrada al computador y verifican los controles entre "corridas" a través de los numerosos programas y ciclos de procesamiento, especialmente en aquellas aplicaciones que pueden contener 50 o más programas, poca atención le dan a establecer los lineamientos para identificar y seleccionar los puntos de control significativos.

A menudo los auditores que examinan los estados financieros preparados de los registros contables generados por sencillos procesos computarizados limitados, son capaces de auditar en torno al computador exitosamente, confiando completamente en los controles de usuarios. Pero a medida que aumenta la complejidad y crece la penetración de los sistemas, es cada vez más difícil auditar eficazmente en torno o alrededor del computador y se debe confiar a los controles establecidos dentro de él.

El informe primario de la auditoría está dirigido a la evaluación de la probabilidad de que existan errores o irregularidades materiales en los estados financieros. Cuando se mira en estos términos, la diferencia básica entre el sistema manual y el computarizado es que éste último contiene más puntos en los cuales pueden ocurrir errores. La clave para emplear la lógica es saber cuáles son y dónde se encuentran estos puntos y evaluar los controles internos contables relacionados.

En primer lugar, el auditor deberá identificar los importes significativos de los estados financieros que son aquellos que se espera que puedan afectar de manera material la presentación de los estados financieros. Por ejemplo, se esperaría que las cuentas por cobrar a clientes sean importes significativos para una Compañía manufacturera, mientras que las cuentas por cobrar a empleados pueden no serlo.

El auditor deberá hacer un seguimiento hacia atrás al flujo de transacciones desde los estados financieros hasta su origen, sin importar si éstas fluyen a través de un procesamiento manual o computarizado. Una vez que el auditor ha identificado el flujo de transacciones necesita identificar los puntos de procesamiento en dicho flujo. Los puntos de procesamiento son aquellos puntos en los cuales se inician, registran, cambian, resumen, analizan o informan transacciones. Es aquí donde pueden ocurrir irregularidades; el auditor debe considerar cada punto y su efecto posible sobre los estados financieros.

Después de que el auditor ha identificado los riesgos en cada punto de procesamiento, debería identificar los procedimientos específicos de control prescritos en cada punto. El sistema de control debería incluir controles sobre los puntos de procesamiento donde el flujo de la transacción ingresa y sale del procesamiento computarizado.

Los sistemas de control interno contable diseñados apropiadamente incluyen ciertas características que ayudan a asegurar que los procedimientos específicos de control se apliquen según lo prescrito (Controles Generales).

Estos Controles Generales no pueden evitar o detectar errores sin la aplicación de procedimientos específicos de control.

Evaluar la eficacia de los Controles Generales y procedimientos específicos de control diseñados para minimizar el riesgo en cada punto de procesamiento parece complejo, una razón es que dichos procedimientos pueden estar diseñados para varios o para todos los puntos de procesamiento.

Para evaluar si los controles han sido diseñados adecuadamente, el auditor necesita considerar si los errores o irregularidades potenciales para cada punto de procesamiento será adecuadamente evitado o detectado por procedimientos específicos de control.

El auditor primero enumeraría los riesgos que ha identificado en cada uno de los puntos de procesamiento para el importe significativo de los estados financieros, luego describiría los controles internos contables prescritos para la corriente o flujo de la transacción. Entonces, el auditor consideraría cada control y decidiría cuáles riesgos están parcialmente o completamente controlados por dicho procedimiento. Si el control es esencial para reducir adecuadamente el riesgo, se marcaría un símbolo en la casilla correspondiente al procedimiento específico de control y riesgo relacionado. Si el procedimiento específico de control y riesgo relacionado es esencialmente redundante, se marcaría un símbolo diferente en la casilla apropiada. No se colocaría marca alguna si el control no contribuye a reducir el riesgo. Después de considerar todos los controles, el auditor revisaría las anotaciones en la columna para cada riesgo y evaluaría si los controles prescritos son adecuados.

Si la confianza del control sobre los sistemas involucra una tecnología muy compleja de procesamiento de datos es conveniente para realizar una auditoría, la ayuda de un especialista para poder identificar alguna o toda la información que maneje en este capítulo. Si el auditor no tiene un especialista entre su personal, debería considerar obtener la ayuda de una firma de contadores o de una firma consultora de computación.

Otros puntos importantes que deben de considerarse por el auditor son las pruebas de auditoría considerando a la computadora de diferentes maneras.

El auditor necesita probar el control interno contable sobre el procesamiento computarizado sobre el cual planea confiar. Como ha señalado, algunos controles tales como los controles para la comprobación de edición y dígitos de verificación, pueden no comprobar evidencia

visible de funcionamiento. El auditor necesita diseñar procedimientos utilizando el computador para probar esos controles.

Puede ser más eficiente emplear la ayuda de un computador al realizar las pruebas sustantivas de los datos contables que están registrados en un archivo, aunque sea posible probar los datos sin su utilización. Por ejemplo, puede resultar más rápido y menos costoso utilizar los sistemas para volver a calcular los gastos de depreciación para todos los activos fijos que hacerlo en forma manual.

El sistema contable puede incluir transacciones que no se puedan probar apropiadamente sin la ayuda de un computador. Por ejemplo, si el procesamiento de transacciones no proporciona evidencia visible de lo que se realizó o si los registros contables se encuentran almacenados en medios magnéticos el auditor puede necesitar realizar pruebas sustantivas usando la máquina.

A veces aún el auditor que posee conocimientos básicos sobre computación puede considerar necesario buscar la ayuda de un especialista en computación para diseñar procedimientos técnicos complejos. Sin embargo, el auditor que primero identifica la información esencial requerida para satisfacer el objetivo de auditoria será capaz de especificar el papel del especialista, revisar la razonabilidad de dicho trabajo y evaluar los resultados de sus hallazgos.

En resumen, para comprender todo lo mencionado, es que puede aplicarse lo dicho al procesamiento manual y al procesamiento computarizado, especialmente a este último cuando existen la necesidad de evaluar el control interno o realizar pruebas sustantivas y en la Compañía existe un sistema complejo para el registro, procesamiento y obtención de la información, siendo en este caso el computador la herramienta apropiada para desarrollar el trabajo y tener un mayor nivel de detalle al determinar la probabilidad de errores e irregularidades.

Al cumplir con las normas, procedimientos y técnicas de auditoría, las tareas del Auditor de Sistemas de Información incluirán las siguientes:

- Planificar un enfoque de auditoría, preparar el programa de auditoria y la asignación de recursos.

- Obtener y documentar la evidencia de que el área auditada está controlada adecuadamente y de que las operaciones del área son eficientes y eficaces usando técnicas de auditoria apropiadas.
- Evaluar las fortalezas y debilidades del área que se audita para informar de su eficiencia, eficacia y del estado de los controles al analizar las evidencias de auditoria.
- Redactar y presentar un informe de sus hallazgos, conclusiones y recomendaciones para informar al lector del mismo de la adecuación de los controles y la eficiencia y eficacia de las operaciones.
- Evaluar las acciones realizadas por la gerencia respecto de la implementación de las recomendaciones del informe de auditoria con técnicas adecuadas de seguimiento y generación de informes.
- Cumplir con el Código de Ética y Normas Profesionales de la Fundación para asegurar la calidad y consistencia de la labor de auditoria.

1.2.2 NORMAS GENERALES [1]

No.1. ACTITUD Y APARIENCIA

En todas las cuestiones relacionadas con auditoria, el auditor de sistemas de información debe ser independiente de quien es auditado en actitud y apariencia.

No.2. RELACIÓN EN LA ORGANIZACIÓN

La función de auditoria de sistemas ha de estar lo suficientemente independiente del área que se audita para permitir una relación objetiva de la auditoria.

No.3. CÓDIGO DE ÉTICA PROFESIONAL

El auditor de sistemas de información debe cumplir el Código de Ética Profesional.

No.4. DESTREZAS Y CONOCIMIENTOS

El auditor de sistemas de información ha de ser competente técnicamente, con las destrezas y conocimientos necesarios para la realización de las tareas de auditoria.

[1] Normas Generales de Auditoría de Sistemas de Información de "*The Information Sistem Audit and Control Foundation*".

No.5. EDUCACIÓN PROFESIONAL PERMANENTE

El auditor de sistemas de información ha de mantener su competencia técnica por medio de la correspondiente capacitación permanente.

No.6. PLANIFICACION Y SUPERVICIÓN

Las auditorias de sistemas de información han de ser planificadas y supervisadas para brindar seguridad de que se alcanzan los objetivos de auditoria y se cumplen estas normas.

No.7. EXIGENCIA DE EVIDENCIA

Durante la realización de la auditoria, el auditor de sistemas de información ha de obtener evidencia que por su naturaleza y suficiencia respalden los hallazgos y conclusiones informadas.

No.8. DEBIDO CUIDADO PROFESIONAL

Debe observarse el debido cuidado profesional en todos los aspectos de la tarea del auditor de sistemas de información, incluyendo el cumplimiento de normas de auditoria aplicables.

No.9. INFORME DE LA EXTENSIÓNDE LA AUDITORÍA

Al preparar los informes, el auditor de sistemas de información ha de expresar los objetivos de la auditoria, el periodo que cubre y la naturaleza y extensión de las tareas llevadas a cabo.

No.10. INFORME DE LOS HALLAZGOS Y DE LAS CONCLUSIONES

Al preparar los informes, el auditor de sistemas ha de expresar las observaciones y conclusiones respecto de las tareas de auditoria llevadas a cabo, y cualquier reserva o salvedad que el auditor tenga respecto de la auditoria.

RESOLUCIONES SOBRE NORMAS GENERALES PARA AUDITORÍA DE SISTEMAS DE INFORMACIÓN.

No 1	INDEPENDENCIA	Actitud y apariencia, Relación Organizacional
No. 2	INDEPENDENCIA	Participación en el proceso de desarrollo de sistemas

No. 3	REALIZACIÓN DEL TRABAJO	Requisito de evidencia
No. 4	REALIZACIÓN DEL TRABAJO	Debido cuidado profesional
No. 5	REALIZACIÓN DEL TRABAJO	Utilización de la evaluación del riesgo en la planificación de auditoría
No. 6	REALIZACIÓN DEL TRABAJO	Documentación de la auditoría
No. 7	REALIZACIÓN DEL TRABAJO	Informes del auditor
No. 8	REALIZACIÓN DEL TRABAJO	Consideración de las irregularidades para la Auditoría
No. 9	REALIZACIÓN DEL TRABAJO	Uso de herramientas del Software de auditoría

1.2.3 CÓDIGO DE ÉTICA[2].

El Código de ética Profesional constituye una directiva para la actuación profesional y personal de los auditores de sistemas.

El Código de Ética establece lo siguiente:

- Apoyar el establecimiento y cumplimiento de normas, procedimientos y controles para los sistemas de información.
- Cumplir con las Normas de Auditoría de Sistemas de Información.
- Actuar en interés de sus empleados, accionistas, clientes y el público en general en forma diligente, leal y honesta y a sabiendas de no contribuir en actividades ilícitas o incorrectas.
- Mantener la confidencialidad de la información obtenida en el curso de sus deberes. La información no será utilizada para propio beneficio o divulgada a terceros no legitimados.
- Cumplir con sus deberes en forma independiente y objetiva, y evitar toda actividad que comprometa, o parezca comprometer, su independencia.
- Mantener su capacidad y conocimientos en los campos interrelacionados de la auditoría y los sistemas de información por medio de su participación en actividades de capacitación.
- Ejercer sumo cuidado al obtener y documentar material suficiente sobre el cual basar sus conclusiones y recomendaciones.
- Informar a las partes involucradas del resultado de las tareas de auditoría llevadas a cabo.

[2] El Código de ética profesional de la ISACF

- Apoyar la educación de la gerencia, los clientes y al público en general para mejorar la comprensión de la auditoría y los sistemas de información.

1.2.4 REQUERIMIETOS EXTERNOS

- Identificar los requerimientos gubernamentales u otros externos, que sean relevantes, que atañe a:
  - Prácticas y controles de sistemas computarizados.
  - La forma en que almacenan las computadoras, programas y los datos que son pertinentes a la organización o a las actividades del departamento/función/actividad de los Servicios de Información.
- Documentar las leyes, reglamentaciones, etc.
- Evaluar si la gerencia de la organización y la función de Sistemas de Información han tenido en cuenta los requerimientos externos relevantes al trazar los planes y establecer políticas, estándares y procedimientos.
- Revisar los documentos del departamento / función / actividad interna de Servicios de Información que tratan el cumplimiento de leyes aplicables a la industria.
- Determinar el cumplimiento de los procedimientos establecidos que tratan tales requerimientos.

1.2.5 REALIZACIÓN DE UNA AUDITORIA DE SISTEMAS[3].

El auditor de sistemas debe evaluar los riesgos globales y luego desarrollar un programa de auditoría que consta de objetivos de control y procedimientos de auditoría que deben satisfacer esos objetivos. El proceso de auditoría exige que el auditor de sistemas reúna evidencias, evalúe las fortalezas y debilidades de controles basados en las evidencias recopiladas, y que prepare un informe de auditoría que presente esos temas de auditoría en forma objetiva a la gerencia.

[3] *IS Audit and Control Journal*; Vol. III, 1995, Página 43-46 y Vol. IV, 1996, Página 6-7.

Una planificación adecuada es el primer paso necesario para realizar auditorias de Sistemas de Información eficaces. El auditor de sistemas debe comprender el ambiente del negocio en el que se ha de realizar la auditoría asi como los riesgos del negocio y los controles asociados.

1.2.5.1 NORMATIVIDAD.[4]

BOLETIN 3050; ESTUDIO Y EVALUACION DEL CONTROL INTERNO

El procesamiento electrónico de datos al evaluar la estructura del control interno.

Por la importancia que han adquirido los sistemas de Procesamiento electrónico de datos en la información contable,
Así como el volumen de las operaciones procesadas en ellos, la perdida de huellas visibles y concentración de funciones contables que frecuentemente se dan en ambientes de este tipo, el auditor debe de conocer, evaluar y en su caso, probar el sistema de PED, como parte fundamental del estudio y evaluación del control interno y documentar adecuadamente sus conclusiones sobre el efecto en la información financiera y el grado de confianza que depositará en los controles. Los lineamientos para llevar a cabo esta función se establecen en el Boletín 5080.

BOLETÍN 5080; EFECTOS DEL PROCESAMIENTO ELECTRONICO DE DATOS (PED) EN EL EXAMEN DEL CONTROL INTERNO

Generalidades

De conformidad con las Normas de Auditoria relativas a la ejecución del trabajo "el auditor debe efectuar un estudio y evaluación adecuados del control interno que le sirva de base para determinar el grado de confianza que va a depositar en él; asimismo, que le permita determinar la naturaleza, extensión y oportunidad que va a dar los procedimientos de auditoría" (boletín 1010).

El estudio del control interno incluye el análisis y la comprensión de los métodos que se utilizan para procesar la información financiera, con objeto de determinar si las técnicas establecidas

[4] *Normas y Procedimientos de auditoría*, IMCP, Boletines 3010 y 5080.

cumplen con los objetivos del control interno; por lo tanto, cuando el PED forma parte del control interno contable y de éste se deriva información sujeta a examen, el auditor debe realizar su estudio, evaluación y como resultado de dicho trabajo, deberá documentar adecuadamente sus conclusiones sobre el efecto del PED en sus pruebas de auditoría.
El alcance al efectuar el examen del control interno establecido en el PED, dependerá de la importancia de las aplicaciones en el proceso de la información financiera.
El PED por su complejidad y su constante evolución, requiere para el estudio y evaluación de su control interno de personal con entrenamiento técnico y capacidad profesional adecuados.

El impacto que eventualmente puede tener una deficiencia o desviación del control interno en el área de PED puede ser menos evidente y, sin embargo, tener mayor repercusión en errores en los estados financieros que pasen inadvertidos; lo anterior significa que el auditor esté obligado a efectuar su revisión utilizando todos los elementos que le permitan asegurarse de que la información financiera a dictaminar se procesa adecuadamente.

Objetivo

Señalar los principales objetivos del control interno en un ambiente de PED y los procedimientos de auditoría sugeridos para evaluar y revisar el control interno en empresas que lo utilicen.

Alcance

Este boletín se refiere únicamente al estudio y evaluación del control interno del PED llevado a cabo por el auditor para determinar la naturaleza, extensión y oportunidad que va a dar a sus procedimientos específicos para evaluar la eficiencia en la operación del equipo de cómputo ni a las técnicas de auditoría utilizadas con ayuda del mismo computador para probar los sistemas (programas) y/o el contenido de los archivos; sin embargo, dado que existe interrelación entre los procedimientos de auditoría y las técnicas de auditoría para efectuar pruebas del PED hechos con ayuda del computador, en el Apéndice II de este boletín se incluyen ilustraciones de algunas de esas técnicas de auditoría tanto para probar sistemas como el contenido de los archivos.

Control interno en un ambiente de PED

Objetivos

Los objetivos de los controles establecidos en la empresa deben enfocarse a la creación, a través de políticas y procedimientos adecuados, de un sistema que asegure que toda la información que deba ser procesada se procese en forma correcta y oportuna y que de dicho proceso se obtenga la información financiera esperada. Los objetivos generales del control interno son los siguientes:

1.- Objetivos de autorización

Todas las operaciones deben realizarse de acuerdo con autorizaciones generales o específicas de la administración.

2.- Objetivos de procesamiento y clasificación de transacciones

Todas las operaciones deben registrarse para permitir la preparación de estados financieros de conformidad con principios de contabilidad generalmente aceptados o de cualquier otro criterio aplicable a dichos estados y para mantener en archivos apropiados datos relativos a los activos sujetos a custodia.

3.- Objetivos de salvaguarda física

El acceso a los activos solo debe permitirse de acuerdo con autorizaciones de la administración, y

4.- Objetivos de verificación y evaluación

Los datos registrados relativos a los activos sujetos a custodia deben compararse con los activos existentes a intervalos razonables y tomarse las medidas apropiadas respecto a las diferencias que existan. Asimismo, deben existir controles relativos a la verificación y evaluación periódica de los saldos que se informan en los estados financieros, ya que estos objetivos complementan en forma importante a los mencionados anteriormente.

Características

En primer lugar debe mencionarse que, para que el control interno funcione en una empresa determinada, es necesario que su estructura organizacional esté diseñada para que quienes son responsables del establecimiento de los procedimientos de control y de su supervisión, tengan las autoridad necesaria para hacer cumplir sus objetivos; esto es particularmente importante en el área del PED, ya que ocasionalmente estas funciones en las empresas serán nuevas o recientes y quizá no se les haya asignado un nivel adecuado en la estructura de organización.

Los controles generales se enfocan a la organización general del departamento y a las funciones de quienes intervienen en el desarrollo de sistemas. Los controles de aplicación o específicos se refieren a los establecidos en la operación del computador que incluye la entrada, el proceso y la salida de datos, o sea, que todos los datos se procesan una sola vez oportunamente (entrada), sujetos a un proceso de validación (proceso), y que sean la base para producir información confiable y completa (salida).

A medida que el uso del computador se ha generalizado debido a la reducción real en los costos de los equipos y a la facilidad en su operación, algunos controles de los que se describen en esta sección son de aplicación limitada, tratándose de computadores conocidos como "microcomputadores" o "minicomputadores", de tal forma que, por ejemplo, los controles relativos a la preinstalación o a la organización del departamento de PED se ven, en las circunstancias, modificados a trámites menores, o bien, a departamentos PED compuestos de una o dos personas donde la segregación de labores puede ser ortodoxa, requiriéndose de controles adicionales.

1.2.5.2 COMPRENSIÓN DEL NEGOCIO Y DE SU AMBIENTE

Al planificar una auditoria, el auditor de sistemas debe tener una comprensión suficiente del ambiente total que revisará. Debe incluir una comprensión general de las diversas prácticas comerciales y funcionales relacionadas con el tema de auditoría, así como los tiempos de sistemas de información que se utilizan. Debe comprender el ambiente normativo en que opera el negocio.

Los pasos para la comprensión del negocio pueden incluir:

- Recorrer las instalaciones de la organización.
- Lectura de material sobre antecedentes que incluyan publicaciones sobres esta industria, memorias e informes financieros independientes.
- Entrevistas a gerentes claves para comprender los temas comerciales esenciales.
- Estudio de los informes sobre reglamentos.
- Revisión de informes de auditorias previas y planes estratégicos a largo plazo.

1.2.5.3 RIESGO Y MATERIALIDAD DE AUDITORÍA.

Los riesgos de auditoria se clasifican de la siguiente manera:

- Riesgo inherente

  El riesgo de que un error pueda ser material o significativo cuando se combina con otros errores encontrados durante la auditoria, no existiendo controles compensatorios relacionados.

- Riesgo de control

  El riesgo de existir un error material que no pueda ser detectado en forma oportuna por el sistema de control interno.

- Riesgo de detección

  El riesgo global de auditoría es la combinación de categorías individuales de riesgos de auditoría evaluados para cada objetivo de control individual específico. Se debe evaluar y controlar esos riesgos para lograr el nivel deseado de seguridad tan eficientemente como sea posible. El auditor debe tener una cabal comprensión de estos riesgos de auditoría al planificar una auditoría.

  Las consideraciones de materialidad, combinados con una comprensión de riesgo de auditoría, son conceptos esenciales para planificar las áreas a auditar así como las pruebas específicas que se han realizado en una auditoria determinada.

- Riesgo del negocio

  El riesgo del negocio son aquellos riesgos que pueden afectar la viabilidad a largo plazo de un determinado negocio o de la empresa en su conjunto. La naturaleza de esos riesgos puede ser financiera, normativa, u orientada a los controles.

1.2.5.3.1 TÉCNICAS DE EVALUACIÓN DE RIESGOS[5].

El auditor puede enfrentarse ante una gran variedad de temas sujetos a ser auditados. Cada uno de ellos puede representar diferentes tipos de riesgo de auditoría. El auditor de sistemas debe evaluar esos riesgos posibles y determinar cuáles de esas áreas de alto riesgo debe ser auditada.

Existen cuatro razones para utilizar la evaluación de riesgos para determinar las áreas de alto riesgo de auditoria. Ellas son:

1. Permitir que la gerencia asigne eficientemente los limitados recursos de auditoria.
2. Asegurarse de que se ha obtenido la información pertinente de todos los niveles gerenciales, incluyendo del director, auditores de sistemas, y gerencia de áreas funcionales. Generalmente, la información incluye áreas que colaboran con la gerencia para cumplir eficazmente sus responsabilidades y aseguran que las actividades de la función de auditoria se dirigen correctamente a las áreas de alto riesgo y constituyen un valor agregado para la gerencia.
3. 3.Constituir la base para la organización de la auditoría a fin de administrar eficazmente el departamento.
4. - Proveer un resumen que describa cómo un tema individual de auditoría se relaciona con la organización global de la auditoria así como con los planes del negocio.

1.2.5.4 OBJETIVOS DE CONTROL INTERNO[6].

Un sistema computarizado bien diseñado debe tener controles incorporados sobre todas sus funciones principales, además debe comprender los objetivos básicos de control que deben existir para todas las aplicaciones de un determinado tipo.

Los componentes de un sistema de control interno incluyen:

[5] *Handbook of IT Auditing*, Cap. A Computer Audit, Control and Security, Cap VII, IS Audit and Control Journal, Vol.VII, 1995, Pag. 20-29 y Vol.I. 1996Página 44-48, Vol.III, 1996 págs. 14-18.
[6] *Handbook of IT Auditing*, Cap. D.2.

- **Controles contables internos** que están dirigidos primordialmente a contabilizar las operaciones. Estos conciernen a la salvaguarda de los activos y la confiabilidad de los registros contables.
- **Controles operativos** que se dedican a las operaciones, funciones y actividades diarias y a garantizar que las operaciones satisfacen los objetivos del negocio.
- **Controles administrativos** que se dedican a la eficiencia operativa en una área funcional y al cumplimiento de las políticas gerenciales, incluyendo los controles operativos. Puede describirse los controles administrativos como aquéllos que respaldan los controles operativos relacionados con la eficiencia operativa y el cumplimiento de las políticas de la organización.

Los objetivos de control incluyen:

- Salvaguarda de activos
- Cumplimiento de políticas de la empresa o exigencias legales
- Autorización / entrada
- Las transacciones son exactas y complejas
- Salida
- Confiabilidad del proceso
- Respaldos/recuperación
- Eficiencia y economía de las operaciones

Los objetivos de control interno valen para todas las áreas, tanto de sistemas manuales como computarizados. El auditor de sistemas debe tomar los objetivos de control interno y traducirlos a procedimientos especificos de auditoria de sistemas de información.

1.2.5.5 OBJETIVOS GENERALES DE AUDITORÍA[7].

Un objetivo de control se refiere a como debe funcionar el control interno, en tanto el objetivo de auditoria se refiere a la meta especifica de la auditoria. Los objetivos de auditoria a menudo están centrados en verificar si existen los controles internos para minimizar los riesgos del negocio.

[7] *Handbook of IT Auditing*, Cap. A.2.; *Computer Audit Control and Security*, Cap. 2

El auditor de sistemas debe tener una comprensión general de cómo los objetivos generales de auditoría pueden ser traducidos a objetivos específicos de control de sistemas de información.

1.2.5.6 PROCEDIMIENTOS GENERALES DE CONTROL[8].

Los controles generales son controles globales interdependientes válidos para todas las áreas de la organización. Los procedimientos de control incluyen políticas y procedimientos establecidos por la gerencia para proveer una razonable garantía de que se han alcanzado los objetivos particulares. Los procedimientos de control son:

- Políticas y procedimientos de seguridad lógica para garantizar la adecuada autorización de transacciones y actividades
- Políticas globales para el diseño y utilización de documentos y registros adecuados para contribuir a garantizar el registro correcto de las transacciones
- Procedimientos y funciones para garantizar salvaguardias adecuadas respecto del acceso a los activos e instalaciones y su uso
- Políticas de seguridad física válidas para todos los centros de cómputo

Los controles generalmente se clasifican en tres grandes categorías:

a) Controles preventivos

Son aquéllos controles diseñados para evitar que se produzca un error, omisión o acto malicioso.

b) Controles de detección

Son aquellos que detectan que se ha producido un error, omisión o acto malicioso e informan de su aparición.

c) Controles correctivos

Son aquéllos que corrigen errores, omisiones o actos maliciosos una vez detectados.

[8] *Handbook of IT Auditing*, Cap. D.4.

1.2.5.7 PROCEDIMIENTOS GENERALES DE AUDITORÍA[9]

Los procedimientos generales de auditoria son los pasos básicos en la realización de una auditoria e incluyen los siguientes:

- Evaluación anual de riesgos y planificación de auditoria
- Planificación de auditoria individual
- Revisión preliminar del área / tema de auditoria
- Obtención y registro de la comprensión del área/ tema de auditoria
- Evaluación del área /tema de auditoria
- Pruebas de cumplimiento
- Pruebas sustantivas
- Generación del informe de auditoria
- Seguimiento

El auditor de sistemas debe comprender los procedimientos para probar y evaluar los controles de los sistemas de información. Tales procedimientos incluyen:

- Utilización de software generalizado de auditoría para revisar el contenido de los archivos de datos.
- Utilización de software especializado para evaluar el contenido de los archivos de parámetros de los sistemas operativos
- Técnicas de diagramas de flujo para documentar aplicaciones automatizadas.

El auditor de sistemas debe llegar a comprender estos procedimientos como para poder planificar las pruebas de auditoría apropiadas.

1.2.5.7.1 PLANIFICACIÓN.

El auditor debe comprender qué otras consideraciones pueden afectar el enfoque global de la auditoría y deben tenerse en cuenta, tales como:

- Fechas límites de implementaciones de sistemas / cambios de versiones

9 *Normas Generales de la ISACF*, Sección 1.9

- Tecnologías actuales y futuras
- Limitaciones en cuanto a recursos de sistemas.

1.2.5.7.2 ESTRUCTURA Y FASES DEL PROGRAMA DE AUDITORIA.

Un programa de auditoría es un conjunto documentado de procedimientos de auditoría diseñados para alcanzar los objetivos de auditoria planificados.

Un programa de auditoría típico incluye lo siguiente:

- Tema de auditoría. Identificar el área a ser auditada
- Objetivo de auditoría. Identificar el propósito de auditoría
- Alcance de la auditoria. Identificar los sistemas específicos o unidades de la organización que se han de incluir en la revisión.
- Planificación previa a la auditoría.
  - Identificar las destrezas técnicas y recursos que se necesitan
  - Identificar las fuentes de información para pruebas o revisión tales como un flujograma funcional, políticas, normas, procedimientos o papeles de trabajo de auditorías previas.
  - Identificar los lugares físicos o instalaciones a auditar
  - Actualizar los programas de auditorias existentes
- Procedimientos de auditoría pasos para:
  - Recopilación de datos
  - Identificación y selección del enfoque de auditoria para verificar y probar los controles
  - Identificación de una lista de personas a ser entrevistadas en la auditoría
  - Identificación y obtención de políticas, normas y directivas del departamento para su revisión, y
  - Desarrollo de herramientas y metodología de auditorias para probar y verificar los controles.
- Procedimiento para evaluar los resultados de pruebas y revisiones
- Procedimiento de comunicación con la gerencia
- Preparación del informe de auditoría
- Procedimientos de seguimiento
  - Procedimientos para evaluar/probar la eficiencia y eficacia de la operación
  - Procedimientos para probar controles

- Revisar y evaluar la razonabilidad de los documentos, políticas y procedimientos

El programa de auditoría también se convierte en una guía para documentar los diversos pasos de auditoría y para señalar la evidencia revisada y también dejar documentado el proceso usado para realizar la auditoría y la responsabilidad del trabajo.

1.2.5.7.3 PRUEBAS DE CUMPLIMIENTO Y PRUEBAS SUSTANTIVAS[10].

Una prueba de cumplimiento determina si los controles se aplican como tal como se describe en la documentación del programa o según lo describe personal del ente auditado, así mismo determina si los controles se aplican en una manera que cumplan las políticas y procedimientos de la gerencia.

Una prueba sustantiva sustenta la adecuación de los controles existentes para proteger a la organización de la actividad fraudulenta. Los auditores contables utilizarían pruebas sustantivas para probar los errores monetarios que afectan en forma directa los saldos de los estados contables.

1.2.5.7.4 CONTROLES CLAVES.

Un propósito básico de cualquier auditoría de sistemas es identificar los controles clave y realizar procedimientos de auditoría para probar los controles clave básicos y los controles disciplinarios dentro de esas categorías. Estos controles entran en tres categorías.

- Controles de detección
- Controles preventivos
- Controles correctivos

Dentro de estas categorías de control existen una multitud de controles básicos y de controles disciplinarios que incluyen:

[10] *Handbook of IT Auditing*, Cap. A.5 y A.6.; *Computer Audit Control and Security*, Cap. 5

- Controles básicos.
  - Controles de edición por programa o manuales
  - Conciliación de totales de control de archivos
  - Procedimientos de copias de resguardo y recuperación

- Controles disciplinarios:
  - Segregación de tareas
  - Restricciones físicas/lógicas de acceso
  - Autorizaciones de transacciones

1.2.5.7.5 REGLAS DE EVIDENCIA

Evidencia es toda la información que utiliza el auditor de sistemas para determinar si el ente o los datos auditados siguen los criterios u objetivos de auditoria. La evidencia de auditoria puede incluir las observaciones del auditor de sistemas, notas tomadas en las entrevistas, documentación interna, o los resultados de procedimientos de pruebas de auditoria.

Si bien toda la evidencia ayudará al auditor a llegar a las conclusiones de auditoría, cierta evidencia es más confiable que otra.

1.2.5.7.6 ASIGNACIÓN DE LOS RECURSOS DE AUDITORÍA.

El auditor debe conocer técnicas para administrar los proyectos de auditoría con personal de auditoría adecuadamente entrenados.

La asignación de recursos humanos debe comprender los recursos disponibles dentro de una organización para realizar auditorías. Los auditores pueden tener diversos antecedentes, como haber sido programadores o auditores contables y graduados terciarios.

1.2.5.7.7 ENTRENAMIENTO DEL PERSONAL.

La tecnología de sistemas está en constante cambio. El entrenamiento debe mantener el nivel de capacidad del auditor de sistemas por medio de actualizaciones de destrezas ya existentes

así como entrenamiento dirigido hacia nuevas técnicas de auditoria y áreas tecnológicas. A fin de mantener tal nivel de competencia, los profesionales deben cumplir con el Programa de Educación Continua.

1.2.5.7.8 REVISIÓN DE ESTRUCTURAS ORGANIZACIONALES[11].

Un sólido plan de organización con una adecuada segregación de funciones es un control general clave en una función de sistemas de información. El auditor debe comprender los controles organizativos generales y estar en condiciones de evaluar esos controles en la organización auditada.

Las funciones de sistemas de información, en las que existe un importante énfasis sobre procesamiento distribuido cooperativo o en computación por parte de los usuarios finales, pueden estar organizadas de manera distinta de la organización de sistemas de información clásica con funciones separadas de sistemas y operaciones. El auditor de sistemas debe estar en condiciones de revisar esas estructuras organizacionales y evaluar sus controles organizativos.

1.2.5.7.9 REVISIÓN DE NORMAS DE DOCUMENTACIÓN DE SISTEMAS[12].

Un primer paso para revisar la documentación de un sistema de información es comprender las normas vigentes sobre documentación dentro de la organización. El auditor de Sistemas de Información debe buscar un nivel mínimo de documentación que incluirá:

- Documentos que inician el desarrollo de sistemas,
- Especificaciones de diseño funcional,
- Historia de cambios a programas,
- Manuales de documentación de usuarios.

[11] *Handbook of IT Auditing*, Cap. B.2.; *Computer Audit Control and Security*, Cap. 2
[12] *Computer Audit Control and Security*, Cap. 6

El auditor debe estar en condiciones de revisar la documentación de un determinado sistema y evaluar si cumple los estándares de documentación de la organización. Asimismo, el auditor debe comprender los enfoques más modernos del desarrollo de sistemas. El auditor debe reconocer otros componentes de documentación de sistemas de información tales como especificaciones de bases de datos, arquitectura de archivos o listados de programas autodocumentados.

1.2.5.7.10 ENTREVISTAS DEL PERSONAL APROPIADO.

Las entrevistas de auditoría deben organizarse de antemano, deben seguir un determinado esquema y deben documentarse con notas.

1.2.5.7.11 APLICACIÓN DE TÉCNICAS DE MUESTREO[13].

Se utiliza el muestreo cuando cuestiones de tiempo y costo hacen prohibitiva una verificación del 100% de las transacciones o sucesos en un universo determinado.

Se utiliza el muestreo para inferir las características de un universo, el muestreo por lo general no es aplicable cuando el universo se refiere a un control o función intangible o no documental, tal como segregación de funciones, existencia de una supervisión, o autorizaciones verbales de una transacción.

Existen dos enfoques generales para el muestreo de auditoría:

- **Muestreo Estadistico**. Es un método objetivo para determinar el tamaño de la muestra y los criterios de selección. Con el muestreo estadístico, el auditor decide cuantitativamente con qué ajuste la muestra debe representar el universo, y el número de veces en 100 que la muestra representa el universo.
- **Muestreo no Estadistico**. Utiliza el criterio del auditor para determinar el método de muestreo, el tamaño de la muestra a utilizar, y cuáles de esos se seleccionaran. Estas decisiones se basan en juicios subjetivos del auditor sobre cuáles partidas son materiales y más riesgosas.

[13] AICPA, Accounting and Auditing Guide AU, Section 350/Audit Sampling

Tanto el muestreo estadístico como el no estadístico exigen que el auditor utilice su propio juicio al definir las características del muestreo, y por lo tanto sufren del riesgo de que el auditor llegue a una conclusión errónea a partir de la muestra. Sin embargo, el muestreo estadístico permite que el auditor cuantifique la probabilidad de error.

El auditor tiene a su disposición estos dos enfoques generales para el muestreo de auditoria con dos métodos básicos de muestreo.

1. **Muestreo de Atributos**. También denominado muestreo estimativo, es la técnica utilizada para estimar el valor de ocurrencia de un control dado o un conjunto de controles relacionados (los atributos). Este muestreo es útil para realizar pruebas de cumplimiento.
2. **Muestreo de Variables.** también denominado estimación dólar o muestreo de estimación media, es la técnica que se utiliza para estimar el valor del dólar u alguna unidad de medida, como el peso, la población, etc.

1.2.5.7.12 TÉCNICAS DE AUDITORÍA ASISTIDA POR COMPUTADOR.[14]

El auditor de sistemas debe tener una cabal comprensión de las técnicas de auditoria asistida por computador y dónde deben ser aplicadas. Esta comprensión debe incluir tanto la utilización del software genérico de auditoría técnica más avanzadas tales como generadores de datos de prueba y técnicas para efectuar una prueba integrada. Además de seleccionar la técnica correcta, el auditor de sistemas debe comprender la importancia de documentar los resultados de tales pruebas con fines de evidencia de auditoría.

En consenso, ya no es suficiente auditar "alrededor del computador" ahora debemos considerar la auditoría de sistemas "a través" del computador y en el proceso usar al computador como una herramienta para revisar el sistema ya que es virtualmente imposible manejar los grandes volúmenes de datos y las transacciones de los modernos sistemas por los ahora antiguos medios manuales.

Las técnicas de auditoria asistidas por computador pueden eliminar parte de las rutinas mecánicas de trabajo de Auditoría y utilizarse para aplicar:

14 "La Auditoria asistida por Computadora, Seminario de la CNBV, Abril 1998

- Pruebas de Control,
- Procedimientos Analíticos (pruebas de razonabilidad, análisis de tendencias y análisis de relaciones),
- Pruebas de detalles,
- Pistas de Auditoria (monitoreo continuo),
- Muestreo estadístico.

Ventajas de las pruebas:

- Mayor alcance y eficiencia en la obtención de evidencia
- Reducción de costos
- Manejo de un alto volumen de transacciones
- Facilidad en procesos de consulta y/o análisis, facilidad al adoptar cambios
- Reducción del nivel de riesgo de la auditoria
- Cobertura más amplia y coherente de la auditoria
- Mayor disponibilidad de la información
- Ahorro de tiempo
- Precisión de los resultados
- Incremento de la productividad

1.2.5.7.13 EVALUACIÓN DE FORTALEZAS Y DEBILIDADES DE AUDITORÍA.[15]

Luego de desarrollar un programa de auditoria y recopilar evidencia de auditoría, el siguiente paso es evaluar la información recopilada a fin de desarrollar una opinión de auditoría.
El auditor debe evaluar los resultados de la evidencia recopilada para el cumplimiento de los requerimientos de control o de objetivos establecidos en la etapa de planificación de la auditoria. El auditor debe tener una comprensión de las técnicas para analizar las evidencias recogidas a partir de la revisión.

El auditor debe usar su juicio profesional al decidir cuáles observaciones ha de presentar a los diversos niveles gerenciales.

[15] *Handbook of IT Auditing*, Apéndice A y B.

1.2.5.7.14 INFORME DE AUDITORÍA

Los informes de auditoria son el producto final del auditor de sistemas. Ése es el vehículo que el auditor utiliza para informar sus observaciones y recomendaciones a la gerencia. El formato exacto del informe de auditoría variará según la organización. Sin embargo, el auditor de sistemas experto debe comprender los componentes básicos de un informe de auditoría y cómo comunicar adecuadamente las observaciones de auditoría a la gerencia.

- **Estructura y contenido del informe**. No existe un formato especifico para un informe de auditoria de sistemas de información, y las normas de auditoria de la organización normalmente marcarán el formato. Sin embargo, los informes de auditoria, por lo general, tienen la siguiente estructura y contenido:
  1. Introducción, incluyendo los objetivos y alcance de la auditoría, el periodo cubierto y un resumen sobre la naturaleza y extensión de los procedimientos de auditoría realizados.
  2. Conclusión global de auditor de sistemas expresando una opinión sobre la adecuación de los controles o procedimientos revisados durante la auditoria.
  3. Observaciones y recomendaciones detalladas de auditoría.
  4. Respuestas de la gerencia a las observaciones con las acciones correctivas a llevar a cabo y la oportunidad de implementación de tales acciones correctivas.
- **Inclusión de las observaciones en los informes de auditoria**. La decisión de incluir o no las observaciones en un informe de auditoría dependerá de su materialidad y el destinatario a quien va dirigido el informe de auditoria. La decisión de qué incluir en varios niveles del informe depende de las directivas dadas por la gerencia superior. Sin embargo, el auditor debe tomar la decisión final de qué incluir u omitir del informe.
- **Implementación de recomendaciones**. El auditor de sistemas debe reconocer que tal vez la gerencia no esté en condiciones de implementar todas las recomendaciones de auditoria en forma inmediata. El auditor debe tratar las recomendaciones y las posibles fechas de implantación durante el proceso de divulgación del informe de auditoría. El auditor se debe dar cuenta de la limitación de implementar dichas recomendaciones como limitaciones de personal, presupuestos, u otro proyecto.

1.2.5.7.15 CONCLUSIONES Y OPINIONES.

El informe de auditoria debe incluir una sección con la opinión respecto de las observaciones de auditoría. Se debe poner en conocimiento cualquier salvedad respecto de auditoría. Puede expresarse como que los controles o procedimientos examinados son adecuados o no. El informe de auditoria debe respaldar esa conclusión, y la evidencia global recopilada durante la auditoría debe brindar un nivel mayor de respaldo.

Dentro de la profesión de contador independiente, existen cuatro tipos de informes:

- **Informe sin salvedades**. Este informe implica una auditoria limpia en la que no se hallan problemas materiales o declaraciones erróneas. Esta opinión normalmente dice que los estados contables de la organización auditada están de acuerdo con principios de contabilidad generalmente aceptados.
- **Informe con salvedades**. Los auditores externos utilizan un informe con salvedades para indicar que la información contable de la organización auditada cumple con las normas de auditoría generalmente aceptadas, salvo por una excepción de condiciones o situaciones mencionadas expresamente. Estas excepciones no tienen que tener una importancia que afecte materialmente la situación patrimonial de la organización.
- **Opinión adversa**. Los auditores externos emiten una opinión adversa cuando consideran que los estados contables de la organización auditada están mal expuestos o significativamente no cumplen con los principios contables generalmente aceptados.
- **Renuncia de opinión**. Se emite tal tipo de informe cuando los auditores externos consideran que la situación financiera de la organización auditada es muy precaria y puede conllevar en la disolución de la misma. Tal tipo de informe también puede emitirse cuando los auditores no son independientes de la organización auditada, o cuando el alcance de la auditoría es tan limitado que no pueda emitirse un informe.

1.2.5.7.16 ENTREVISTA DE FINALIZACIÓN O SALIDA.

La entrevista de finalización, que se lleva a cabo al final de la auditoria, le brinda al auditor los medios para discutir los hallazgos y recomendaciones con la gerencia. Asimismo, durante esta entrevista, el auditor puede asegurarse de que los hechos que se presentan en el informe son

correctos, asegurarse de que las recomendaciones son realistas y efectivas en términos de costos, y de no ser asi, buscar alternativas a través de la negociación con el área auditada y tratar de obtener fechas de implementación para las recomendaciones sobre las que se ha llegado a un acuerdo.

1.2.5.7.17 IMPLEMENTACIÓN DE RECOMENDACIONES.

Los auditores de sistemas deben darse cuenta que la auditoría es un proceso continuo. Si se realizan las auditorías, se emiten los informes, pero no se hace su seguimiento para comprobar si la gerencia ha tomado las acciones correctivas correspondientes. Los auditores de sistemas deben tener un programa de seguimiento para determinar si se han tomado las acciones correctivas prometidas según las recomendaciones de auditoría.

Los resultados del seguimiento deben ser comunicados a los niveles gerenciales correspondientes.

El auditor tendrá que realizar ciertos pasos de auditoría para determinar si la gerencia ha implementado las acciones correctivas acordadas.

2. CONTROLES DE LOS SISTEMAS DE CÓMPUTO

El objetivo primordial de una auditoria es formarse una opinión sobre los Estados Financieros de una entidad. Las condiciones observadas y el material de evidencia obtenido, necesita evaluarse objetivamente para determinar si los Estados Financieros están presentados apropiadamente en todos los aspectos. Si hay indicaciones de posible deshonestidad, deberemos evaluar su impacto sobre la auditoria financiera.

Los controles por computadora soportan la efectividad y apoyan la eficiencia de los controles que se ejecutan en relación con los sistemas de aplicaciones automatizados. Estos controles deben incluir todos los elementos que hagan efectivo el control interno.

Los sistemas de cómputo frecuentemente tienen controles, llamados controles generales de cómputo y que directa o indirectamente afectan a todos los sistemas que operan dentro de un ambiente de procesamiento dado. Los controles y procedimientos de monitoreo que utiliza cada compañía serán distintos y por lo tanto debemos aplicar el criterio correcto para la situación de cada uno.

Cuando el cliente tiene instalaciones múltiples de procesamiento, los controles pueden ser comunes a todas las instalaciones, muy diferentes para cada una de ellas, dependiendo de las funciones que desempeñen en los distintos sitios. Adicionalmente, necesitamos comprender las funciones importantes de controles generales de la computadora que se realizan fuera del alcance de la organización.

Los sistemas computarizados frecuentemente tienen áreas comunes de control y procedimientos de control relacionados, frecuentemente referidos como controles generales, que afectan los sistemas dentro de un ambiente de procesamiento dado. Estos controles tipicamente nos interesan debido a que:

- Contribuyen a la confiabilidad de los sistemas que procesan clases de transacciones importantes, y por lo mismo, son una parte integral de nuestra base de rolación

- Podrían directa o indirectamente atenuar riesgos específicos identificados
- Contribuyen directamente a la efectividad de otros controles

Los controles generales están divididos en las siguientes áreas funcionales:

- Conocimiento del Negocio
- Organización
- Operaciones del computador
- Soporte Técnico a los Sistemas de Información
- Seguridad de la Información
- Adquisición, Desarrollo y Mantenimiento de Sistemas

Cuando el cliente tiene múltiples ambientes de procesamiento, los tipos de controles generales y su efectividad pueden variar de un ambiente a otro. Las diferentes áreas para los diversos ambientes de procesamiento pueden ser útiles en estos casos. También podría ser necesario que consideremos la existencia de diferentes ambientes de control en diferentes ubicaciones al identificar los controles generales que contribuyen a la confiabilidad de los sistemas en un ambiente de procesamiento dado.

Las rutinas y procedimientos establecidos que conforman algunos controles generales, podrían ser formales o informales, dependiendo del tamaño y complejidad del ambiente de procesamiento. En muchas organizaciones, sucede que no existe documentación para soportar muchas de las actividades de control que lleva a cabo el personal del cliente. La ausencia de documentación, no necesariamente excluye de antemano que tengamos confianza en esos controles. Especialmente cuando se seleccionan procedimientos de control informales para probar un cierto año, debemos seguir los pasos apropiados para evaluar la competencia y experiencia del personal que realiza tales procedimientos y lo adecuado de la supervisión de dicho personal.

Cuando pretendemos confiar en los controles y nuestra evaluación de alto nivel de los controles generales indica que los controles pueden ser efectivos, podemos usar las áreas básicas para obtener una mejor comprensión de los controles generales. Podemos obtener esta mejor comprensión, reuniendo información adicional más detallada sobre los

controles en un ambiente de procesamiento dado. Esta información proporciona una base para identificar y documentar las descripciones de determinados controles generales que contribuyen a un procesamiento confiable, atenúan riesgos específicos identificados o contribuyen a la efectividad de otros controles.

No se pretende que todos los controles mencionados en cada área se deban probar o que la ausencia o debilidad de controles individuales signifique que no podemos reducir el riesgo de control abajo del máximo. Podemos usar estas las áreas como ayuda para identificar los controles generales de los que buscamos seguridad.

Debemos involucrar a especialistas en auditorías por computadora o de personas con habilidades equivalentes en la obtención de la comprensión de los controles generales que se mencionan en cada área, para ver si se van a probar controles programados muy complejos.

Los controles generales descritos en cada área podrían no ser de nuestro interés, en ambientes de procesamiento muy sencillos con procedimientos adecuados de control manuales. Consecuentemente, este perfil generalmente no es aplicable en tales casos.

Podemos usar cada área para identificar y documentar nuestra comprensión de los controles generales que creemos contribuyen a la confiabilidad de los sistemas.

3. CONOCIMIENTO DEL NEGOCIO

Para obtener una comprensión de alto nivel de la estructura de control, podemos realizar entrevistas con uno o más de los gerentes de cada área de control general de la computadora para determinar la importancia de los sistemas de cómputo dentro de los planes estratégicos de la compañía, así como determinar la organización del departamento de informática y las funciones que realiza, la integración de los sistemas de controles generales de la computadora y de aplicación.

Podemos reunir la información necesaria a través de visitas a las instalaciones principales para identificar las instalaciones más importantes, así como la obtención de una visión general de la organización y su operación, pláticas con la gerencia de finanzas y de procesamiento de datos.

Generalmente la ayuda de un especialista en auditorias por computadora puede ser necesaria para lograr la comprensión del ambiente de las computadoras y su estructura de control, especialmente para clientes de computación compleja.

3.1 Clasificación del uso de las computadoras en el negocio

Describa los siguientes factores

- Grado de Uso: Volumen de transacciones
  Número de usuarios
  Información clave

- Complejidad: Tipo de actualización en línea o por lote
  Conexiones entre sistemas
  Complejidad en los cálculos
  Generación automática de transacciones

- Importancia: Dependencia
  Pérdida de control en caso de contingencia

Continuidad en la operación

3.2 Configuración del Hardware (indicar vendedor y modelo)

- Unidad central de procesamiento (CPU). Otras unidades de procesamiento(s) y localidad Número aproximado de terminales, impresoras y microcomputadoras enlazadas a la unidad central (CPU) (incluyendo las principales localidades)

3.3 Software (indicar vendedor y versión)

- Sistema operativo
- Herramientas para el desarrollo de programas
- Control de acceso
- Compiladores para los lenguajes de programación
- Comunicación de información
- Administración de base de datos
- Recuperación de datos/paqueteria para elaboración de reportes

3.4 Microcomputadoras

- Descripción del hardware (vendedor, modelo, etc.).
- Resumen de las principales aplicaciones contables de la microcomputadora y del software
- ¿Están en red las microcomputadoras o independientes?. Si están en red, describa la red

3.5 Service Bureau

- ¿Utiliza el cliente un service?
- Nombre del service
- Aplicaciones que procesa el service
- ¿Están disponibles los reportes para los auditores? Si así es, ¿cuáles son las fechas de esos reportes?

3.6 Personal Asignado al Procesamiento de Datos (Indicar el Número de Personas)

- Administración General
- Operaciones Computarizadas
- Adquisición, Desarrollo y Mantenimiento de Sistemas
- Seguridad de la Información
- Apoyo al Sistema de Información
- Otros
- Total de personas
- Anote los nombres y puestos del personal clave para el procesamiento de datos
- Describa la aparente experiencia y competencia del personal de procesamiento de datos, con relación al tamaño, complejidad y necesidades aparentes del cliente

3.7 Políticas y Procedimientos

- Describa las rutinas establecidas (v.g. manuales de política y procedimientos) que proporcionan el adecuado funcionamiento de los controles
- Describa el entrenamiento y supervisión del personal para el procesamiento de datos
- Describa los cambios significativos en el personal para el procesamiento de datos durante el año pasado
- Describa las preocupaciones de la gerencia del cliente con relación al procesamiento de datos

3.8 Describa los Eventos Significativos en el Procesamiento de Datos del Año Pasado

- Adquisiciones, cambios o bajas de hardware
- Sistemas desarrollados, adquiridos o modificados
- Cambios en la organización, políticas o prácticas del procesamiento de datos Planes del cliente para mejorar o reemplazar el hardware o software
- Problemas identificados del usuario con el procesamiento de datos en el año pasado, como:

- Fallas del sistema o errores significativos en los resultados del procesamiento
- Retrasos o pérdidas de información significativos
- Dificultad para hacer cambios en los sistemas
- Falta de entrenamiento o soporte al usuario
- Dificultades con las conversiones o cambios a los sistemas nuevos
- Limitaciones de los sistemas que resultan en procedimientos manuales adicionales
- Cambios a los sistemas sin la aprobación del usuario
- Otros (describa)

3.9 Otra información

- ¿Se involucró a auditoria interna en las revisiones del procesamiento de datos el año pasado? Si así es, describa brevemente el alcance del trabajo y los hallazgos significativos
- ¿Realizaron consultores externos trabajo relacionado con las operaciones computarizadas del cliente que pueda afectar nuestra comprensión? Si así es, describa brevemente el trabajo y anote el nombre del grupo de consultores
- Determinar el punto de vista de la gerencia acerca de los sistemas de información
- Identificar aspectos de computación que sean de particular interés para la gerencia
- Compromiso de la gerencia en cuanto los sistemas
- Si los planes de sistemas son compatibles con otros planes estratégicos de la compañia
- El nivel de inversión de la compañía es adecuado

Sistema de Aplicación

Obtener una lista de las aplicaciones contables más importantes (sistemas de aplicación) que alimentan al libro mayor (v.g. ventas/cuentas por cobrar, inventario/compras) y las cuentas de los estados financieros con las que se relacionan. El sistema del libro mayor también se puede listar con la anotación de todas las cuentas relacionadas.

Descripción del Sistema

- Propósito de negocio del sistema (incluyendo la importancia del sistema a las operaciones del negocio)
- Enfoque general para el control del sistema (controles de usuario y programados)
- Función en el inicio de las transacciones y control de movimientos de los activos
- Historia de los errores de procesamiento
- Volúmenes aproximados de transacciones
- ¿Desarrollados internamente? Si así es, ¿En qué lenguaje? ¿Bajo qué ambiente corre?
- ¿Comprados? (especificar)
- Naturaleza del procesamiento (en linea o por lote)
- Describa el nivel de complejidad del procesamiento
- Las funciones clave del procesamiento del sistema y la frecuencia de uso (v.g. diariamente, semanalmente, mensualmente). Tales funciones de procesamiento pueden ser:

- Preparación de facturas, órdenes de compra, etc.
- Actualización de archivos maestros
- Emisión de reportes para la gerencia

- Flujo General de Transacciones (Los diagramas de flujo preimpresos pueden ser útiles para documentar el flujo de las transacciones a través del sistema)
- Entradas claves (fuente de entrada principales)
- Salidas clave (reportes y archivos, ya sea en pantalla, en forma electrónica o impresos, y los usos de cada uno)
- Tabuladores y archivos maestros importantes
- Conexiones con otros sistemas

Historia del Sistema

Año	Instalaciones o modificaciones significativas al sistema

4. ORGANIZACIÓN DEL DEPARTAMENTO DE SISTEMAS.

La posición de este departamento está en función directa de las características particulares de cada empresa. Lo más probable es que este departamento esté reportando directamente al contralor de la empresa, ya que la principal función de ambos es producir información para la mejor dirección y control de las operaciones.

El alcance de la revisión generalmente se concreta a examinar el control interno existente en el centro de cómputo y áreas de sistemas sin evaluar a detalle la calidad y efectividad de las operaciones del computador, concretándose a verificar la existencia de una estructura organizacional lógica del área de sistemas, donde cada una de las áreas funcionales depende de una jefatura y no directamente de la cabeza del departamento, contando además con una supervisión adecuada de toda el área, así como contar con el personal suficiente para cubrir las cargas de trabajo.

Así mismo se verificará la existencia de descripciones de puestos las cuales se adecuen a las necesidades actuales de la organización, dichas descripciones deberán ser del conocimiento del personal responsable de las diferentes funciones, así como encontrarse debidamente autorizadas por la gerencia responsable.

4.1 ESTRUCTURA ORGANIZACIONAL

En la práctica las estructuras encontradas en los departamentos de sistemas de información son muy variadas, ya que dependen en gran medida del tamaño y desarrollo organizacionales, de forma enunciativa mas no limitativa podemos identificar los siguientes puestos caracteristicos en toda área de sistemas en una organización:

- Comité de Sistemas.
- Dirección de Sistemas
- Gerente de Programas de aplicación
- Lider de Proyecto
- Analista Programador
- Jefe de Operaciones

- Operadores
- Administración de Base de Datos
- Gerente de Métodos y Procedimientos
- Gerente de Soporte Técnico
- Gerente de Telecomunicaciones
- Administrador de Seguridad

4.1.2 Comité de Sistemas

Es el mecanismo de la alta gerencia en el área de sistemas de información, y esta integrado por personas que tienen autoridad para disponer de capital y otros recursos de la compañía para los objetivos y proyectos de sistemas asi como evaluar los resultados obtenidos.

La gerencia debe designar un comité de planificación o dirección para supervisar las actividades del Departamento de sistemas. El comité debe incluir representantes de la Gerencia Senior, el Departamento de Sistemas de Información y las Gerencias de los Departamentos de usurarios.

Su objetivo es revisar y actuar ante las solicitudes de nuevos sistemas, de acuerdo con los objetivos de la empresa. Es responsabilidad del comité asegurarse de la utilización eficiente de los recursos de procesamiento de datos y fijar prioridades, examinar los costos y brindar respaldo para los diversos proyectos.

El comité debe tomar decisiones como:

- Los objetivos de sistemas
- Las políticas de procesamiento de datos
- Aprobación de nuevas aplicaciones o modificación a las ya existentes
- Determinación de prioridades para la implantación de nuevas aplicaciones
- Control de proyectos y grado de avance
- Resolución de conflictos interdepartamentales

- Procedimientos y lineamientos a seguir en lo que se refiere a presupuestos de inversión, prioridades, administración de funciones, asignación de recursos, controles y organización
- Instalación e implementación del hardware y software
- Documentación
- Mantenimiento del equipo e insumos
- Seguridad de datos y programas
- Entrenamiento de usuarios y soporte técnico
- Normas, políticas y procedimientos que se refieren a las áreas mencionadas, incluyendo aspectos jurídicos como cumplimiento de las leyes, utilización no autorizada de datos y programas de la empresa
- Justificación de compras
- Selección, compra, prueba y adquisición de hardware y software
- Programación, es decir, nuevos programas y cambios a los existentes

El comité de sistemas está constituido por:

a) Director General o Contralor (Presidente)
b) Jefe de Procesamiento de datos (Vice-Presidente)
c) Ejecutivo de otras áreas funcionales cuando se requiera
d) Funcionarios de los departamentos usuarios, cundo se requiera
e) Personal de análisis de sistemas cuando sea conveniente.

4.1.3 Director de Sistemas

Este organiza, dirige y administra los diferentes recursos del área como son: hardware, software, personal, etc. Busca que este manejo sea lo más eficiente posible para cubrir las necesidades de información de la compañía. Entre sus actividades están:

- Coordinación:

Mantener un equipo de personas técnicamente competentes.

Participar en el comité de sistemas recomendando e implementando planes de sistemas, políticas y procedimientos.

- En producción y operaciones para llevar a cabo funciones como:

Operación del computador
Conversión de datos
Controles de entradas y salidas
Distribución de reportes de salida

- Orientación de proyectos:

Estudio de viabilidad
Análisis de sistemas
Diseño de sistemas
Programación
Analiza los requerimientos de su área y prepara recomendaciones para los presupuestos de gastos e inversiones.
Es responsable del comportamiento y seguridad del software y hardware de la Compañía.

- Investigación:

Se mantiene informado de los avances tecnológicos, tendencias y desarrollos de la industria de su ramo.
Evalúa las diferentes alternativas de hardware y software que puedan servir mejor a las necesidades de la Compañía y los somete a consideración del Comité de Sistemas.

4.1.4 Gerente de programas de aplicación.

Organiza y dirige todo lo relacionado con programas de aplicación: desarrollo (utilización de nuevos programas) y mantenimiento (modificación de los programas existentes) de sistemas de aplicación.

Ejemplo: Programa para nóminas, cuentas por cobrar, etc.

Es responsable de:

- Realizar un plan de desarrollo con los proyectos realizados y por realizar
- Evaluar las solicitudes de los usuarios
- Realizar presupuestos considerando tiempos estimados y personal responsable
- Supervisión de la programación de las diferentes aplicaciones en proceso de desarrollo con cada líder del proyecto
- Evaluar las pruebas de las aplicaciones terminadas antes de transferirse a producción
- Establecer metodología estándar y verificar que se cumplan

4.1.5 Líder de proyecto

Organiza y coordina los proyectos a su cargo, participa en la asignación de tareas de los programadores.
Es responsable de:

- Calendarización de los programadores
- Preparación de flujogramas, paquetes de programación, etc.
- Revisar el diseño lógico de los programas
- Revisar y corregir programas de producción solicitados por los usuarios

4.1.6 Analista Programador

Asiste al líder de proyecto en el establecimiento de requerimientos de archivos. Diseña la lógica de los programas de aplicación, auxilia a los usuarios durante la implementación y da algunos servicios de mantenimiento. Es responsable de:

- Análisis de las necesidades de sistematización
- Diseño de modelos conceptuales y/o aplicaciones para satisfacer dichos requerimientos

- Desarrollo de programas y/o sistemas
- Consultoría al usuario utilizando el enfoque de sistema
- Asesoría para optimizar los métodos y procedimientos

4.1.7 Jefe de operación

Dirige al operador dentro del SITE, que es el lugar en donde se encuentra el equipo y que cuenta con las instalaciones adecuadas. Está encargado del puntual y correcto manejo de las operaciones, impresión de reportes y mantenimiento preventivo del hardware. Sus responsabilidades son:

- Brindar un adecuado servicio a los sistemas de prueba y producción
- Establecer horarios para el eficiente uso del equipo
- Desarrolla e implementa procesos estándar de operación, como por ejemplo: la elaboración diaria de respaldos
- Revisa que los mantenimientos o desarrollos estén debidamente autorizados para aceptarlos en el ambiente de producción
- Está al día en cuanto a las tendencias tecnológicas y capacidad de los distintos equipos

4.1.8 Operadores

Es responsable de:

- La continúa operación del equipo; se encarga de echar a andar y apagar el equipo. Analiza los distintos problemas operativos y los corrige
- Interpretar los distintos mensajes del computador e iniciar la acción requerida
- Identificar las fallas en el sistema, así como proteger la integridad de los archivos de producción y los reportes

4.1.9 Administrador de la base de datos

Dirige las actividades relacionadas con la administración de las bases de datos. Esto incluye definiciones, organización, documentación, etc. Es responsable de la seguridad e integridad de esta información. Sus responsabilidades son:

- Definir el contenido y estructura de las bases de datos, así como, instruir a los programadores para usarla eficientemente
- Mantener al día la documentación relevante
- Mantener un diccionario de los elementos de la base de datos, evitar redundancia y coordinar entre los usuarios las definiciones de los elementos
- Establecer estándares y procedimientos para la salvaguarda del software

Es común encontrar en la organización del departamento de sistemas otros puestos distintos a los enunciados anteriormente; ya que la organización de esta área es tan distinta como necesidades se tengan en ella. Algunos otros puestos que se pueden encontrar son los siguientes:

4.1.10 Gerente de Métodos y Procedimientos

- Documenta todo lo relativo a la metodología, desarrollos, plan de contingencias, etc.
- Establece y optimista los métodos y procedimientos administrativos e identifica su interrelación con los sistemas
- Actualiza junto con el usuario respecto a los manuales administrativos y documentación de los sistemas

4.1.11 Gerente de Soporte Técnico

Brinda el soporte en casos de problemas técnicos tanto en el centro de cómputo como con los usuarios. También efectúa las siguientes actividades:

- Soporte técnico a los usuarios

- Soporte basándose en datos
- Soporte a comunicaciones
- Evaluación de harware y software
- Mantenimiento de hardware
- Administración del sistema
- Administración de la base de datos

4.1.12 Gerente de Telecomunicaciones

Está a cargo de:

- Adecuado manejo y seguridad de las telecomunicaciones y el equipo relevante
- Identificación de los requerimientos de la información de los usuarios, para diseñar las aplicaciones de sistemas
- Asesoria a los usuarios
- Coordinar el análisis y diseño de los sistemas

4.1.13 Administrador de Seguridad.

Es responsable de implementar y mantener la seguridad tanto de la información como de los diferentes recursos que permiten el proceso de la misma.

4.2 CONTROLES ORGANIZATIVOS

Para determinar el grado de control de cada una de estas áreas debemos investigar:

- Enfoque de la gerencia
- Importancia relativa
- Gerencia responsable
- Métodos que utiliza la gerencia para monitorear los procedimientos de control
- La manera en que la función del área de sistemas respalda a las funciones operativas y contables del cliente
  - Si la función de sistemas se maneja centralizada o descentralizada
  - Si existen factores que afecten la estructura de control de computación del cliente

- Si la estructura refuerza los planes estratégicos
- Los sistemas de cómputo proporcionan información correcta y puntual
- Si la compañía cuenta con un plan de contingencias para que los sistemas de información y los usuarios prosigan con sus actividades

- Políticas de personal y prácticas gerenciales razonables
- Segregación de funciones entre el ambiente de procesamiento de información y otros ambientes o funciones organizativas
- Segregación de funciones dentro del ambiente de procesamiento de información
- Procesamiento de información
- Técnicas que faciliten la adecuada segregación de funciones
- Controles compensatorios
- Métodos para evaluar operaciones eficaces y eficientes

4.3 PROCEDIMIETNOS Y TECNICAS DE AUDITORIA

4.3.1 Las tareas del auditor deben incluir lo siguiente[16]:

- Obtener las estrategias políticas globales, y así identificar las áreas involucradas en el procesamiento de información, y lograr una comprensión de las prácticas comerciales y funcionales del negocio.
- Identificar las áreas funcionales, tareas y responsabilidades de información significativas delos departamentos que procesan información en computadoras para obtener una comprensión del ambiente de procesamiento de la información de la organización por medio de la revisión de la documentación pertinente, indagación y observación.
- Evaluar la estructura organizativa de los procedimientos de los departamentos que utilizan computadores a fin de evaluar su adecuación al determinar si son eficientes y eficaces e incluyen los controles adecuados.
- Probar los controles para determinar el cumplimiento de las normas, aplicando técnicas de auditoria correspondientes.

[16] Handbook of IT Auditing, Cap.B.2.; EDP Auditing: Conceptual Foundations and Practice, Cap.3

- Evaluar el ambiente de control de la organización para determinar que se alcanzaron los objetivos de control al analizar los resultados de pruebas y otra evidencia de auditoría.

4.3.2 Técnicas de auditoria y evaluación.

- Estrategias, Planes y Presupuestos de Tecnología Informática:
  Estos documentos dan evidencia de la planificación y el control gerencial de los ambientes de sistemas de información.

- Organigramas, diagramas de funciones:
  Los organigramas le brindan al auditor una clara comprensión de las líneas de comunicación jerárquica de un departamento u organización como un todo. Muestran una división de funciones y dan una indicación del grado de segregación de funciones dentro e la organización.

- Informes del Comité de sistemas
  Los informes del comité brindan información documentada acerca de los nuevos proyectos de sistemas. Esos informase son revisados por la gerencia de nivel superior distribuido entre las diversas unidades funcionales de la empresa.

- Políticas y Procedimeintos:
  Estas deben ser claras y concisas para permitir su cumplimiento y vigencia.
  Todas las políticas y procedimientos deben existir por escrito. Las políticas y procedimientos constituyen normas para ser cumplidas. En forma periódica debe comunicarse a todo el personal una política de seguridad. Deben obtenerse evidencia de que cada empleado ha leído y comprendido los pronunciamientos sobre seguridad. El nivel detallado no debe estar disponible para todo el mundo y debe considerarse confidencial.

- Perfiles de puestos
  Definen las funciones y responsabilidades de las diversas tareas de una organización. También brindan a la organización la capacidad de agrupar tareas similares en diferentes niveles de puestos para garantizar una remuneración justa para su personal.

Asimismo, los perfiles de puestos dan indicación del grado de segregación de funciones dentro de la organización y puede contribuir a identificar funciones incompatibles.

Los perfiles de puesto y los organigramas brindan una clara comprensión de las funciones y responsabilidades y definen la línea de comunicación jerárquica. Con esta información el auditor podrá identificar las funciones, responsabilidades y autoridades de manera de evaluar la segregación entre diversas funciones.
Los perfiles deben poder utilizarse para realizar las evaluaciones de rendimiento laboral.

El área de informática debe contar con personas que ofrezcan su experiencia, habilidades y conocimientos para ayudar a la organización y usuarios a contar con información, decisiones y soluciones que faciliten el logro de la productividad de los sistemas.

Por último, los perfiles de puestos deben identificar el puesto al que estos empleados reportan. El auditor debe verificar que el nivel de relaciones de dependencia funcional se basa en principios gerenciales apropiados y no pone en peligro la segregación de funciones.

- Manuales y políticas de personal.
  Los manuales de políticas de personal dan las reglas y reglamentaciones determinadas por la organización sobre cómo espera que se comporten los empleados.

- Autorización.
  Los diversos documentos que se revisan deben también ser evaluados para determianrse: 1) se crearon tal como fue autorizado y fue la intención de la gerencia; 2) son actuales y actualizados.

- Entrevistas al personal

  Personal y gerencia de procesamiento de información.

  La realización de entrevistas al personal y gerencia de procesamiento de información debe incorporar garantías adecuadas de que el candidato tiene las destrezas técnicas para realizar sus tareas. Este es un importante factor que contribuye a una operación eficaz y eficiente.

- Personal y gerencia del departamento usuario

  El personal y la gerencia del departamento usuario deben ser entrevistados y contratados de acuerdo con las exigencias de esa área específica. Los candidatos deben cumplir los estándares de la empresa y también poseer las destrezas técnicas necesarias para realizar eficazmente la función específica de sus tareas.

- Otro personal pertinente.

  Todo personal pertinente debe cumplir los mismos estándares básicos e la empresa y dar el mismo nivel de lealtad y confianza.

4.4 INDICADORES DE RIESGO.

Si bien existen innumerables condiciones de incumbencia para el auditor, algunos de los indicadores más significativos de problemas potenciales son:

- Actitudes desfavorables de los usuarios finales
- Costos excesivos
- Desvíos del presupuesto
- Alta rotación de personal
- Personal inexperto
- Frecuentes errores de los computadores
- Atraso excesivo de solicitudes de usuarios no satisfechas
- Bajo tiempo de respuesta del computador
- Numerosos proyectos de desarrollo abortados o suspendidos
- Compras de hadware/software sin respaldo o autorización.

- Cambios frecuentes a versiones superiores de hardware/software
- Informes con muchas excepciones
- Informes con excepciones no seguidas
- Motivación pobre
- Falta de planes de sucesión
- Confianza en una o dos personas claves.

4.5 EJEMPLO DE REVISION.

Los riesgos relacionados en general con la administración de funciones del personal de sistemas son discutidos a continuación:

1. - Incompetencia del personal:

Riesgo: El que personal incompetente asuma responsabilidades del área para las cuales no se encuentre debidamente capacitado o no cuente con el conocimiento requerido, resultará en la ocurrencia de errores, los cuales pueden quedar sin ser detectados.

Controles: Para asegurar que la debida competencia del personal sistemas, se deben emplear técnicas como:

- Adopción de políticas de contratación de personal que cumpla con la calificación adecuada para asumir las responsabilidades y funciones correspondientes a cada cargo.
- Impulsar programas de entrenamiento y desarrollo del personal que permitan su capacitación para responsabilidades actuales y futuras.
- Requerir que se lleve a cabo la evaluación del desempeño del personal a fin de asegurar que se alcance el nivel satisfactorio requerido para una promoción.

2. - Control gerencial inadecuado:

Riesgo: El control ejercido en el área puede ser superficial, inconsistente, o sujeto a falta de cumplimiento. Asimismo, la falta de comprensión de instrucciones, carencia de una supervisión apropiada, existencia de malos hábitos de trabajo y realización de las tareas

asignadas tomando atajos, propicia que se cometan errores en el desempeño de las funciones del área.

Controles: A fin de definir y comunicar las responsabilidades relacionadas, deben emplearse las siguientes técnicas:

- Ubicación apropiada del departamento sistemas dentro de la organización de la Compañía.
- Elaborar y mantener actualizado el organigrama del departamento.
- Mantener niveles de supervisión y autorización adecuados en todas las áreas funciona es del departamento.
- Elaborar descripciones de puestos y mantenerlas actualizadas, así como llevar a cabo su difusión correspondiente.
- Existencia y apego a manuales de políticas y procedimientos del departamento.

3. - Segregación de funciones incompatibles:

Riesgo: En caso de que el personal de sistemas tenga acceso directo o indirecto a los activos de la empresa y exista una falta de segregación de funciones incompatibles, se presenta la oportunidad de cometer y ocultar fraudes a través del computador, ya sea en forma individual o en colusión con terceros, tanto internos como externos a la compañía.

Controles: Se deben emplear técnicas tales como las mencionadas a continuación para permitir una apropiada segregación de las funciones incompatibles:

- Mantener separadas las funciones de operación, programación, soporte técnico, mesa de control y captura de la información.
- Retirar responsabilidades sobre funciones y controles pertenecientes a las áreas usuarias.
- Prohibir al personal de sistemas que inicie, modifique o corrija los datos de archivos maestros y de transacciones por iniciativa propia.
- Restringir el acceso a la documentación de los sistemas.

- En su caso, Segregar las funciones de administración de base de datos y comunicaciones.
- Realizar rotaciones periódicas de turnos y cargos para una función.
- Requerir que el personal tome vacaciones periódicas.[17]

[17] Handbook of It Aditing, Cap b.2; EDP Auditing: Conceptuals, Foundations and practice, Cap. 8

5. OPERACIÓN DEL COMPUTADOR.

Las operaciones de Sistemas de Información controlan el funcionamiento normal diario del hardware y software. Los ambientes de procesamiento del CPU varían en las distintas organizaciones según el tamaño de la instalación del computador y la carga de trabajo.

El personal de operaciones por computadora es responsable de las actividades diarias de procesamiento del sistema del cliente.

Aseguran que las tareas se programen y procesen de acuerdo con las rutinas establecidas.

Los controles de programación de procesos y control de la biblioteca permite asegurar que únicamente las personas autorizadas procesen las tareas en el orden correcto.

Los controles de entrada/salida incluyen de manera característica, verificaciones de las autorizaciones y aprobaciones adecuadas para permitir que las transacciones sean válidas.

La función de operaciones tiene un efecto directo en la integridad de las transacciones. Las operaciones por computadora verifican que los programas se ejecuten adecuadamente sin la existencia de errores,

También son responsables de verificar los totales de control. Permiten asegurar que las transacciones estén incluidas en el ciclo de procesamiento.

La programación de procesos y administración de la biblioteca asegura que las versiones apropiadas del software y archivos de datos se utilicen durante el procesamiento y que las tareas se procesen en el orden correcto.

Permite asegurar que se suministren fechas correctas a los programas de sistemas de aplicación para lograr controles correctos durante el procesamiento de fin de mes, de fin de año.

Adecuados procedimientos operativos por computadora llevados a cabo consistenternente por personal competente, contribuyen a la confiabilidad del procesamiento; en cambio, inadecuados procedimientos operativos de computadora pueden causar procesamiento incompleto, inoportuno e inexacto.

Las operaciones del sistema de información se organizan generalmente según las siguientes áreas funcionales:

- Administración de operaciones de sistemas de información.
- Asignación de trabajos
- Control de cambio a programas
- Procedimientos de administración de problemas
- Procedimiento para monitorear la utilización eficiente y eficaz de los recursos

5.1 ADMINISTRACIÓN DE LAS OPERACIONES DE SISTEMAS DE INFORMACION.[18]

La gerencia de Sistemas de Información tiene la responsabilidad global de todas las operaciones dentro del ámbito del CENTRO DE PROCESO DE LA INFORMACIÓN, éstas pueden dividirse en distintos grupos:

Asignación de recursos: La gerencia tiene la responsabilidad de asegurarse de que se dispone de los recursos necesarios para cumplir las actividades planificadas dentro de la función del CENTRO DE PROCESO DE LA INFORMACIÓN.

Normas y Procedimientos: La gerencia tiene la responsabilidad de establecer las normas y procedimientos necesarios para todos los procedimientos de acuerdo con las estrategias y políticas globales del negocio.

Funciones de aprobación: La gerencia debe aprobar todas las actividades planificadas así como los cambios a las mismas dentro del área del CENTRO DE PROCESO DE LA INFORMACIÓN. Entre ellas se incluyen:

[18] Handbook of It Aduiting, Cap b.2; EDP Auditing: Conceptuals, Foundations and practice, Cap. 8

- Cronogramas detallados de cada turno de operaciones:
  - Monitorear las operaciones para garantizar el cumplimiento de estándares.
  - Revisar el registro de actividades de consola durante el tiempo del computados desconectado y reinicialización de hadware/software.
  - Revisar el registro diario de actividades del operador par identificar variaciones.
  - Asegurarse de que el procesamiento de los sistemas de información pueden recuperarse en forma oportuna de interrupciones de las operaciones, sean tanto menores como mayores. Ello incluye poseer un plan concienzudo y probado de recuperación de desastres.
  - Monitorear el rendimiento del sistema y de la utilización de los recursos a fin de optimizar la utilización de los recursos computarizados.
  - Anticipar el reemplazo/capacidad del equipamiento para maximizar el procesamiento de los trabajos actuales a través del sistema y planificar estratégicamente el plan de futuras adquisiciones.
  - Monitorear el ambiente y la seguridad del centro del cómputo para mantener condiciones adecuadas de rendimiento del equipamiento.
- Cronogramas de operaciones del computador
- Cambios a la capacidad/hadware
- Informes de contabilización de los jobs
- Acceso físico a los recursos computarizados

Los operadores son responsables del funcionamiento correcto y eficiente de los trabajos asignados en el computador.

Los procedimientos que detallen las instrucciones de operaciones, tareas y procedimientos, preparados de acuerdo con la autorización y deseos de la Gerencia de Sistemas, junto con la adecuada supervisión de la Gerencia de CENTRO DE PROCESO DE LA INFORMACIÓN, son elementos esenciales del ambiente de control.

Tal documentación debe contener:

- Procedimientos para el operador, basados en instrucciones para la operación del computador y el equipo periférico.

- Procedimientos ante fallas de máquinas o programas.
- Instrucciones para la distribución de los listados emitidos
- Procedimientos para obtención de archivos que se encuentran en bibliotecas fuera de línea y su devolución.
- Procedimientos para informar demoras en la corrida de programas, y
- Procedimientos para informar las fallas del computador, demoras en el procesamiento de trabajos y el registro de las acciones correctivas emprendidas.

Tareas de los operadores

Las tareas de los operadores incluyen:

- Reinicie las aplicaciones del computador luego de que el departamento usuario final responsable del mismo ha investigado y resuelto una terminación normal.
- Participar en las pruebas de los planes de recuperación ante desastres.
- Facilitar la toma diaria de copias de respaldo de los archivos computarizados sensibles.
- Observar que no haya ingresos no autorizados al CENTRO DE PROCESO DE LA INFORMACIÓN.
- Vigilar el cumplimiento de los cronogramas de asignación de trabajos documentados establecidos por las gerencias de Sistemas de Información y usuario final.

Los operadores no deben tener acceso irrestricto al software de aplicación, los datos y utilitarios. Asimismo debe resguardarse la consola del operador.

5.2 FUNCIONES DE ASIGNACIÓN DE TRABAJOS.

Debe darse a los trabajos con alta prioridad una disponibilidad óptima de recursos en tanto que las tareas de mantenimiento tales como copias de respaldo de información (back-up) y reorganización de sistemas deben ser realizadas en momentos que no sean picos de utilización crítica.

La introducción de sistemas de asignaciones de trabajos ayuda a asegurarse de que los trabajos se ejecuten en la secuencia correcta.

- Procedimientos para monitorear el uso eficaz y eficiente de los recursos.

Los recursos del computador, como cualquier otro activo de la empresa, deben usarse de manera tal que brinde beneficios a toda la organización. Esto incluye la previsión de información cuándo y dónde sea necesaria, con un costo identificable y auditable. Los recursos del computador incluyen, hadware, software, telecomunicaciones y datos.

5.3 PROCEDIMIENTOS DE ADMINISTRACIÓN DE PROBLEMAS.

Algunos ejemplos de los posibles errores que pueden aparecer en ese registro son:

- Errores de programas
- Errores de sistemas
- Errores de operadores
- Errores de telecomunicaciones
- Errores de hardware

Algunos ejemplos de los datos que pueden contener los registros son:

- Fecha del error
- Descripción de la solución dada al error
- Código de error
- Descripción del error
- Fuente del error
- Iniciales del responsable del registro de errores
- Iniciales del responsable de cerrar la entrada en el registro de errores
- Departamento/centro responsable de la solución al error
- Código de estatus de la solución dada, por ejemplo, problema pendiente, problema cerrado hasta determinada fecha, o problema sin solución en el actual ambiente.

- Narrativa del estado de resolución del error
- Comunicación de problemas y su solución al personal correspondiente del sistema, programación, operaciones y usuario.

La solución de problemas debe comunicarse al personal correspondiente de sistemas, programación, operaciones y usuario a fin de garantizar de que los problemas se resuelvan en la forma más oportuna.

La verificación de la documentación de los centros responsables de la solución de problemas deben ser parte de la función gerencial. Esa documentación debe ser llevada apropiadamente para ser de utilidad.

Informe de la terminación anormal de trabajos

Este informe automatizado identifica todos los trabajos de aplicaciones que han terminado antes de haberse completado en forma correcta y por lo general incluye una explicación o indicación de las condiciones de terminación anormal asociada.

Las terminaciones anormales en exceso pueden ser indicadoras de:

- Pobre diseño, desarrollo y prueba de aplicaciones
- Instrucciones de operación inadecuadas
- Inadecuado apoyo de operaciones
- Inadecuada capacitación o rendimiento de los operadores

Informe de problemas del operador

Es un informe manual que llevan los operadores para registrar los problemas de operaciones del computador y sus soluciones. Las respuestas del operador fueron adecuadas o se les debe dar entrenamiento adicional.

Informe de distribución del output

Este informe identifica todos los informes generados por las aplicaciones y los lugares a los que se distribuyen. Puede ser manual o automatizado y puede resultar de utilidad para rastrear informes perdidos, demorados o distribuidos en forma equivocada.

Registro (Log) de consola

Este informe automatizado identifica a la mayoría de las actividades realizadas en el computador. Por su tamaño y complejidad es de difícil utilización a efectos de monitoreo de la actividad del computador. En general, la gerencia de sistemas utiliza uno de los informes sobre funciones específicas anteriormente nombrados.

Cronogramas de trabajos del operador

En general la gerencia de sistemas llevan estos cronogramas en forma manual como ayuda para la planificación de los recursos humanos. Al proveer personal adecuado a cargo del soporte de operaciones, la gerencia de sistemas se asegura que se satisfagan los requerimientos de los usuarios finales. Esto es especialmente importante durante los periodos críticos o de alta carga de trabajo. Los cronogramas deben ser flexibles como para que permitan un adecuado entrenamiento y cubrir requerimientos de puestos de emergencia.

Cronogramas de trabajos

Estos cronogramas permiten una utilización eficiente de los recursos del computador. Pueden llevarse en forma manual o automatizada. Debe darse a los trabajos con alta prioridad una disponibilidad óptima de recursos en tanto que las tareas de mantenimiento tales como respaldos de información (back up) y reorganización de sistema deben ser realizadas en momentos que no sean picos de utilización crítica. Los cronogramas de trabajo constituyen un medio de mantener las demandas de los usuarios en un nivel manejable y a la vez permitir que se procesen trabajos inesperados o a medida sin demoras innecesarias.

5.4 CONTROLES DE CAMBIOS A PROGRAMAS.

La Gerencia de sistemas establece procedimientos de Controles de Cambios a programas para controlar el movimiento de las aplicaciones, desde el ambiente de prueba, donde se realiza el desarrollo, hasta el ambiente intermedio, donde se realizan pruebas exhaustivas, y luego al ambiente de producción. Se denomina "procedimientos formales de entrega de trabajos" a aquella parte de la mecánica de los controles de cambios de programas que trata las acciones que el personal de operaciones del CENTRO DE PROCESO DE LA INFORMACIÓN han de realizar una vez que un programa o trabajo a superado la prueba de aceptación por parte de los usuarios y ha de pasárselo del ambiente intermedio al ambiente de producción.

Los procedimientos relacionados con éste proceso incluyen asegurarse de que:

- La documentación de sistemas, operaciones y programas estén completas, actualizadas y cumplen las normas establecidas.
- Se ha establecido la preparación, asignación de trabajos e instrucciones de operación.
- Los resultados de las pruebas de sistemas y programas han sido revisados y aprobadas por los usuarios y dirección de proyectos.
- La conversión de archivos de datos, se han realizado con exactitud y en forma completa según la evidencia de la revisión y aprobación de la gerencia usuaria.
- La conversión del sistema se ha realizado con exactitud y en forma completa según la evidencia, la revisión y aprobación de la gerencia usuaria.
- Todos los aspectos de los trabajos entregados han sido probados, revisados y aprobados por el personal de Control/ Operaciones.

5.5 OBSERVACIONES Y PRUEBA DE DIVERSAS FUNCIONES DE OPERACIONES.

Operación del computador

Los controles de operación del computador se refieren a la operación diaria del hardware y software dentro de la organización del CENTRO DE PROCESO DE LA INFORMACIÓN,

responsabilidad respecto del procesamiento de los computadores, incluyendo el montaje de los archivos guardados en medios magnéticos de almacenamiento secundario, cambio de formularios en impresoras, y puesta fuera de servicio de los dispositivos que requieran mantenimiento. Entre los controles de operación del compurador podemos mencionar:

Restricción de la capacidad de acceso del operador

Los operadores deben tener acceso restringido respecto de los archivos y las bibliotecas de documentación.

Las responsabilidades del operador deben limitarse a hacer procesar al computador y el equipamiento periférico relacionado. Debe impedirse a los operadores la corrección de programas y datos.

Restricción de acceso a utilitarios que permiten modificar software y/o datos.
Los operadores deben tener un acceso limitado al código fuente de programas en producción y a las bibliotecas de datos, incluyendo procedimientos de corrida.

Proceso de asignación de trabajos

Registro de trabajos a procesar y los correspondientes archivos de datos
Planificación de trabajos a procesar sobre una base predeterminada. Esta planificación puede realizarse usando métodos manuales o un software de asignación automática de trabajos.

Procedimiento de procesamiento de excepciones

- Obtención de aprobación por escrito de los propietarios de las aplicaciones de la ejecución de procesos o programas en una secuencia diferente a la normal.
- Obtención de aprobación por escrito de los propietarios de las aplicaciones al planificar trabajos a ser ejecutados únicamente por pedido.
- Registro de todas las solicitudes de procesamiento de excepciones.

- Revisión del registro de solicitudes de procesamiento de excepciones para determinar la corrección de los procedimientos ejecutados.

Manejo de reprocesos

- Todo reproceso debe estar correctamente autorizado y registrada para su revisión por la gerencia de sistemas.
- Deben establecerse procedimientos para reprocesos y deben ser realizados de acuerdo con esos procedimientos.

El procedimiento de auditoría para Operaciones del computador debe incluir una revisión de los manuales de operador para determinar si las instrucciones son adecuadas respecto de la operación del computador y su equipo periférico, procedimientos de encendido y apagado, acciones que han de cumplirse en caso de falla de máquina/software, registros que deben conservarse, tareas de trabajos rutinarios y actividades restringidas. En suma, el auditor de sistemas debe realizar pruebas para determinar si los procedimientos coinciden con la intención y autorización de la gerencia.

Capacidad de acceso del bibliotecario

- Debe restringirse el acceso del encargado de biblioteca al hardware.
- El acceso al computador del encargado de biblioteca debe limitarse sólo al sistema de administración de cintas.
- El acceso a las instalaciones de la biblioteca debe circunscribirse a sólo el personal autorizado.
- La eliminación de datos debe estar restringida a la planificación de producción.
- Debe llevarse un adecuado registro de ingreso y de salida de datos.

Contenido y ubicación de los archivos fuera de línea.

- Los medios de almacenamiento de archivos fuera de línea conteniendo programas y datos del sistema en producción deben tener claramente marcado su contenido.

- Las instalaciones de la biblioteca fuera de linea deben estar localizadas en un lugar físico independiente a la sala del computador. El procedimiento de auditoría debe incluir una revisión de las políticas y procedimientos para:
  - Administración de la biblioteca fuera de linea
  - Chequeo del ingreso/egreso de cintas incluyendo las autorizaciones firmadas
  - Identificación, etiquetando, entrega y recupero de archivos back-up de otras sedes
  - Sistemas de inventario para las cintas en esa sede y otras incluyendo ubicaciones especificas de almacenamiento para cada cinta
  - Eliminación y borrados de archivos de cintas, incluyendo autorizaciones firmadas.

Procedimientos de manejo de archivos

Deben establecerse procedimientos para controlar la recepción y liberación de archivos/medios magnéticos de almacenamiento secundario de otras sedes. Los procedimientos de auditoría deben incluir una revisión de esos procedimientos para determinar si son adecuados y coinciden con la intención y autorización de la gerencia. Asimismo, el auditor de sistemas debe realizar pruebas para determinar si estos procedimientos han sido seguidos.

Control de ingreso de datos

- Autorización de documentos de input
- Conciliación de totales de lotes
- Segregación de funciones entre quien ingresa los datos y quien revisa los datos ingresados en cuanto exactitud y errores.

Los procedimientos de auditoría para el ingreso de datos incluye una revisión de los controles y los procedimientos para determinar si:

- Existen controles adecuados
- El personal del CENTRO DE PROCESO DE LA INFORMACIÓN cumple las políticas establecidas

- Adecuada segregación de funciones
- Se producen, llevan y revisan informes de control
- Los informes de control son exactos y completos
- Los formularios de autorización son completos y contienen las firmas correspondientes.

Recorrida del Centro de Procesamiento de Información Centro de Proceso de la Información

Dado que los diversos ambientes de procesamiento varían entre las diferentes instalaciones, una recorrida del Centro de Proceso de Información en general dará una mejor comprensión al auditor de sistemas de las tareas, procedimientos y ambiente de control de operaciones.

Informe de administración de problemas

Cuando se realiza una auditoria de esta área, el Auditor de sistemas debe asegurarse de que se han desarrollado procedimientos adecuadamente documentados para guiar al personal de operaciones del sistema en cuanto a documentación, análisis y resolución de problemas en forma oportuna de acuerdo con la intención y autorización de la gerencia.

El auditor de sistemas debe realizar procedimientos para asegurarse de que se mantiene adecuadamente el mecanismo de administración de problemas y que los errores pendientes de resolución se tratan adecuadamente y son resueltos. Estos procedimientos incluyen:

- Entrevistas al personal de operaciones del sistema
- Revisión de los procedimientos utilizados en el sistema para registrar, evaluar y resolver cualquier problema operativo o de procesamiento para determinar si son adecuados para el análisis de servicios
- Una revisión de los registros de funcionamiento para determinar si existen problemas durante el procesamiento

- Una revisión de las razones de las demoras en el procesamiento de programas de aplicación para determinar si son válidas
- Una revisión de los procedimientos utilizados en el sistema para recopilar estadísticas respecto del rendimiento del procesamiento en linea para determinar si el análisis es exacto y completo
- Determinar si el sistema ha establecido procedimientos para manejar problemas de procesamiento de datos
- Determinar si todos los problemas identificados a/por Operaciones del Centro de proceso de la información se registran para su verificación y solución
- Determinar si se han identificado problemas significativos y recurrentes y se han tomado acciones para evitar su repetición
- Determinar si los problemas de procesamiento s resolvieron en forma oportuna y la solución fue completa y razonable
- Revisión de los informes de administración de sistemas generados por el sistema de administración de problemas para asegurarse de obtener evidencia de una adecuada revisión gerencial
- Revisión de la entrada al registro histórico (log) de errores pendientes de solución que describen problemas a ser resueltos para obtener una adecuada documentación y asegurarse de que son tratados en forma oportuna
- Revisión de la documentación de operaciones para asegurarse de que se han desarrollado procedimientos para la elevación de los problemas no resueltos a una instancia superior de la gerencia

5.6 EJEMPLO DE REVISIÓN

1. Existencia de rutinas y procedimientos establecidos para la programación y establecimiento del proceso de cómputo
2. Existencia de controles para asegurar que:
   - Definida la secuencia de los programas, éstos se ejecuten en orden correcto y en el tiempo adecuado.
   - Las funciones se corren oportunamente
   - Las funciones se corren usando las versiones correctas de los programas

- Las funciones se corren usando las versiones correctas de los archivos

Riesgos:

- Si no se cuenta con dichos controles puede ocurrir una pérdida de tiempo al no programarse adecuadamente las funciones, confusión en el área con respecto a los procesos que ya se han realizado y a los que deben realizarse.
- No se tienen parámetros para determinar la eficiencia del personal del área en la realización de sus funciones y la efectividad y oportunidad de los procesos.
- Si no se procesan todos los trabajos o las transacciones, los resultados del procesamiento pueden ser no confiables.

Control:

Por esto es recomendable diseñar políticas y procedimientos que incluyan la planeación, programación y verificación de los procesos del centro de cómputo. El diseño de tales políticas y procedimientos debe llevarse a cabo en conjunto con las áreas usuarias de la empresa.

3. ¿Hay rutinas y procedimientos establecidos para verificar la exactitud e integridad del proceso por computadora?

   Si los hay, describa los controles diseñados para asegurar que:

   - Los lotes, los totales de valores absolutos y los totales de corrida a corrida se concilian
   - Se verifican los códigos de fin de trabajo y otros mensajes del sistema
   - Se produce toda la información esperada
   - Se detectan y corrigen oportunamente todos los errores de procesamiento
   - Todos los problemas de procesamiento se registran en un informe de problemas o incidentes,
   - Se notifica al personal apropiado de sistemas y usuarios sobre los problemas de procesamiento

Riesgo:

Si el procesamiento es incompleto o inexacto, los resultados de dicho procesamiento no serán confiables.

Controles:

Estos controles son controles de aplicación, por lo que el cliente deberá tener un enfoque consistente para implantar tales controles a través de todas las aplicaciones.

3. ¿Tiene el área de operaciones, la responsabilidad del control y distribución de la información impresa (informes, cheques, formas especiales, etc.)?
   Si es así, describa los controles diseñados para asegurar que:
   - La entrega de la información está bajo control y es oportuna
   - Las formas especiales están bajo control y registradas antes y después de imprimirse

Riesgo:

Si no se tiene un control sobre la información impresa que se genera. Los reportes se imprimen y se entregan sin registrar su generación, la fecha en que se solicitó, la persona que lo solicitó y la persona que lo recogió.

Control:

Podría tener como consecuencia confusión entre los usuarios y el departamento de sistemas en casos como: si la información entregada es la solicitada, si la información llega a manos de la persona que le solicitó, si la generación de información es oportuna o si la información ya previamente se generó, por lo que es recomendable diseñar un procedimiento de solicitud, generación y entrega de reportes para que se tenga un control adecuado de fecha de solicitud, fecha de entrega, información a reportar, quién la solicitó y a quién fue entregada.

3. ¿Requiere la política de retención de registros que se mantengan éstos por lo menos el tiempo necesario para satisfacer los requisitos operacionales y legales?

Control:

De acuerdo al artículo 30 del Código Fiscal de la Federación, la contabilidad deberá conservarse durante un plazo de 10 años contando a partir de la fecha en que se presentaron o debieron haberse presentado las declaraciones con ella relacionadas

Riesgo:

De no cumplir con las obligaciones establecidas en ley, la autoridad quedará facultada para aplicar los procedimientos administrativos de ley a fin de poder auditar, y sancionar esta omisión.

4. ¿Hay rutinas y procedimientos establecidos para rastrear y reportar problemas de procesamiento?

   Si los hay, describa los controles diseñados para asegurar que:

   - Todos los problemas en el procesamiento se registran en un informe de problemas o incidentes
   - Se notifica al personal adecuado responsable del procesamiento de información y al usuario, de los problemas en el procesamiento
   - El gerente de sistemas monitorea el estado de las actividades para la solución de problemas

Riesgo:

- Si el área de operaciones no cuenta con una bitácora de procesamiento en la cuál se registren los procesos realizados, el resultado de su funcionamiento y la ocurrencia de errores, no existirían parámetros para determinar las causas de una falla significativa en el sistema y dar seguimiento a su corrección.
- Dependencia de personal para la solución de errores.
- Los errores pueden presentares en forma recurrente y causar pérdidas de tiempo en la corrección.
- Si no se da seguimiento ni se informa de los problemas de procesamiento, pudieran no resolverse oportunamente. Asimismo, los problemas de procesamiento posteriores

pudieran no resolverse oportunamente. Asimismo, los problemas de procesamiento posteriores pudieran haberse causado por los problemas anteriores, si los problemas anteriores no fueron informados y no se les dio seguimiento, esta relación no podrá ser identificada y pudieran introducirse errores adicionales en el sistema.

Control:

Por lo que es recomendable diseñar una política y procedimiento que determine registrar detalladamente los problemas que se han presentado así como las soluciones aplicadas en una bitácora.

3. El riesgo de pérdida de información obliga a tener respaldada toda la información de la Compañía por lo que es indispensable definir una política en la que se especifique con que frecuencia se realizarán los respaldos y que es lo que se va a respaldar. No existe una regla fija para definir la frecuencia, aunque lógicamente entre menor sea el tiempo, mejor.

Los respaldos no sólo deben considerar las diferentes bibliotecas sino también todas los programas de aplicación, utilerías y el Sistema Operativo.

Resulta importante mencionar que estos respaldos, deben ser guardados en algún lugar custodiado dentro y fuera de las instalaciones. El acceso a los mismos debe estar restringido a las personas que para ello se designaron.

4. Si han habido interrupciones significativas de procesamiento durante el año, ¿hay rutinas y procedimientos establecidos para respaldos y recuperación de información?. Si no han habido interrupciones significativas, no es necesario describir las actividades de procesamiento de respaldo y recuperación.

   Si los hay, describa los procedimientos diseñados para asegurar que:

   - Se hacen regularmente respaldos de la biblioteca de programas y de la información

- Se hacen los respaldos de los sistemas después de cada cambio significativo en el software
- Se mantiene un registro de respaldos
- Los archivos de respaldo se guardan en un lugar seguro y en un lugar diferente
- Se mantiene un inventario de cintas y el lugar actual de tales cintas
- Las cintas se encuentran en condiciones ambientales apropiadas (calor, polvo, agua)
- Se restringe el acceso de las cintas a los usuarios.
- Se cuenta con un software de administración de cintas.
- Se cuenta con procedimientos de reinicio y recuperación para ayudar a los operadores en la resolución de las interrupciones del procesamiento.
- Los respaldos de efectúan regularmente
- Los respaldos se realizan antes y después de cambios importantes del software del sistema.
- Se mantiene un registro de los respaldos
- Se cuenta con copia de respaldos y esta se mantiene fuera de las instalaciones.

Los planes de recuperación se prueban regularmente.

Riesgos:

- Riesgo de pérdida definitiva de información en caso de alguna falla de los discos duros de los servidores y debido a la no-disponibilidad de respaldos para recuperar la información el procesamiento pudiera no ser terminado oportunamente y el costo para restaurarlo pudiera ser importante.
- Si los procedimientos para administrar los medios de almacenamiento de datos son inadecuados, los trabajos o transacciones pudieran ser procesados usando programas o archivos de datos equivocados, o las copias de respaldos de los programas y archivos de datos pudieran perderse o destruirse.

Control:

Es conveniente crear una política de respaldos que incluya tanto un programa de respaldos como la definición del registro histórico a retener y los lugares de almacenamiento de las cintas. Los procedimientos adecuados de respaldos ayudan a asegurar la disponibilidad de los recursos de información.

6. SOPORTE TÉCNICO A LOS SISTEMAS DE INFORMACIÓN

La responsabilidad de la función de soporte técnico es brindar supervisión y soporte a los sistemas en producción e identificar y ayudar a la solución de problemas en los sistemas. Asimismo, es responsabilidad del soporte técnico el evaluar la administración de las tecnologías actuales que pueden beneficiar las operaciones globales.

Si el cliente tiene un sistema de base de datos, utiliza redes de comunicación o tiene una configuración compleja de su sistema operativo podría ser importante que revisemos estos controles dentro de estas funciones al hacer nuestra evaluación sobre la confiabilidad de los sistemas. Los controles y procedimientos que normalmente encontramos en estas funciones de soporte, generalmente son de naturaleza muy técnica y requerirán de la participación de un especialista en auditorias por computadora o con experiencia similar.

Procedimientos escritos

Los procedimientos que tratan las tareas a ser realizadas por el personal de Soporte técnico o soporte a usuarios debe establecerse de acuerdo con las estrategias y políticas globales.

Las funciones de soporte incluyen:[19]

- Determinar la fuente de los problemas del computador y tomar las acciones correctivas apropiadas
- Iniciar los informes de problemas que sean necesarios y garantizar que los problemas se resuelvan en forma oportuna.
- Obtener un conocimiento detallado del sistema operativo y otro software de sistemas
- Dar respuesta a las indagaciones sobre sistemas especificos
- Controlar la instalación de los cambios al software de sistemas para mejorar su eficiencia y adaptar el sistema a las exigencias de la organización y la configuración del computador.

[19] *IS Audit and Control Journal*, Vol. 4, 1995, Págs. 28-35 y 42-47

- Proveer soporte técnico para el procesamiento computarizado de las telecomunicaciones
- Llevar la documentación del software comprado incluyendo emisión de nuevas versiones y arreglos de problemas, así como documentación de sistemas y utilitarios "de desarrollo interno".

6.1 EJEMPLO DE REVISION.

1. ¿Tiene el cliente un sistema de base de datos que mantiene la información utilizada en el proceso contable?

   Si así es, describa los controles diseñados para asegurar que:

   - Los cambios a la base de datos del software se revisan y se prueban antes de instalarse
   - Las peticiones para añadir, modificar o borrar datos se revisan con el personal de procesamiento de datos y los usuarios utilizan la información en un sistema de aplicación.
   - Los reportes de las estadísticas de la base de datos, tales como tiempo de respuesta, disponibilidad, errores y otra información, los revisa el administrador de la base de datos.
   - Los parámetros disponibles del software del sistema que se evalúen y se implementen aquellos que son apropiados.

1. ¿Cuenta el cliente con un grupo de apoyo técnico que mantenga el sistema operativo y otros programas del sistema? Si así es, describa los controles diseñados para asegurar que:

   - Los cambios a los programas del sistema se revisan y prueban antes de instalarse
   - Los cambios se instalan en periodos de muy poca o nula actividad del sistema, para minimizar el potencial de errores en los sistemas de producción
   - Las bibliotecas de los programas del sistema sólo las pueden modificar un número limitado de personal técnico autorizado
   - La documentación de los programas del sistema se mantiene actualizada y se guarda en un lugar seguro

2. ¿Utiliza el cliente medios de comunicación de información que involucran lugares lejanos y el uso de líneas públicas?

   Si asi es, describa los controles diseñados para asegurar que:

- La red de comunicaciones está adecuadamente soportada por personal con experiencia para configurar y mantener el software de comunicaciones y los equipos físicos como módem y controladores
- Todos los intentos de acceso remoto se validan a través del uso de claves de acceso, confirmación de acceso o técnicas similares
- Los cambios al hardware de comunicaciones y software se autorizan y prueban antes de ser instalados
- El equipo de comunicación y la documentación de la red, están físicamente seguros y el acceso está restringido al personal técnico de apoyo

Riesgos:

Si las funciones de la base de datos, el sistema operativo y de comunicaciones no se controlan debidamente, la información y los programas se pueden perder o alterar, los controles lógicos de seguridad se pueden desviar, es más probable que haya fallas del sistema y en general, los sistemas podrían no procesar información confiable. En ambientes de procesamiento sencillos, muchas de estas funciones las realizan los vendedores y los cambios a estos sistemas son mínimos. En ambientes más complejos, el control de estas funciones puede ser aún más importante.

Si las actualizaciones al software del sistema no se controlan adecuadamente, los datos y programas pudieran perderse o alterarse, los controles de seguridad lógica pudieran evadirse, las fallas del sistema pudieran ocurrir con mayor frecuencia y en general el sistema pudiera no procesar confiablemente.

Las modificaciones internas al software del sistema pudieran tener impactos imprevistos en el software de otra aplicación o del sistema, por lo cual deben controlarse muy estrechamente. Si tales modificaciones no se controlan adecuadamente, los datos y

programas pudieran perderse o alterarse, los controles de seguridad lógica pudieran evadirse, las fallas del sistema pudieran ocurrir con mayor frecuencia y, en general, el sistema pudiera no procesar confiablemente.

7. SEGURIDAD DE LA INFORMACIÓN.

La seguridad está definida en el diccionario como el conjunto de medidas tomadas para protegerse contra robos, ataques, crímenes y espionajes o sabotajes. La seguridad implica la cualidad o estado de estar seguro, es decir, la evicción de exposiciones a situaciones de peligro y la actuación para quedar cubierto frente a contingencias adversas.

El uso creciente y la confianza en los computadores en todo el mundo ha hecho seguir una preocupación legitima con respecto a la seguridad informática. El uso de los computadores se ha extendido en ambientes comerciales, gubernamentales, militares e incluso en los hogares. Grandes cantidades de datos vitales sensibles se están confiando y almacenando cada vez más en computadores. Entre ellos se incluyen registros sobre:

- Individuos (médicos, financieros, bancarios),
- Negocios (activos, inventarios, contabilidades, nóminas personal, datos de fabricación)
- Diferentes registros públicos y secretos gubernamentales y militares.
- Grandes transacciones monetarias tienen lugar diariamente en forma de transferencias electrónicas de fondos.
- Más recientemente, informaciones tales como notificaciones de propiedad intelectual y datos comerciales estratégicos son también almacenados, procesados y diseminados mediante computadores. Entre ellos se incluyen diseños de nuevos productos, planes y estrategias comerciales, listas de clientes y datos de ventas, contratos legales y muchos otros.

El acceso, revelación o destrucción no autorizada de datos puede violar la privacidad individual. La corrupción de datos comerciales puede provocar pérdidas significativas y potencialmente catastróficas a las empresas. Merece la pena recordar, sin embargo, que las amenazas a la seguridad no son exclusivas de los computadores. Están inevitablemente presentes en cualquier forma la salvaguarda de activos valiosos. El problema potencial con los computadores es que el creciente recurso a ello para almacenan datos valiosos no suele venir acompañado de las medidas de gestión

necesarias para prevenir los potenciales peligros de la exposición a perder la información almacenada. Por tanto, el uso de prácticas y políticas de seguridad adecuadas con frecuencia suele adoptarse después y no antes de confiar datos y activos a los computadores. Esto tiende a crear ventanas de vulnerabilidad de las cuales pueden tomar provecho los salteadores. Además, algunos de los muchos beneficios de la computación (como por ejemplo el gran número de usuarios, la conectividad, el acceso remoto y la compartición de programas y datos) pueden representar importantes debilidades de seguridad y posibles puntos de penetración en los sistemas inadecuadamente diseñados.

Los sistemas informáticos y los diseños de software deberian preocuparse de los temas de seguridad e incorporar salvaguardias y mecanismos adecuados para reforzar las políticas de seguridad. Por otra parte, el uso de extensas medidas de seguridad puede aumentar el coste y restringir la utilidad, facilidad de uso y rendimiento de los sistemas informáticos. El reto para los diseñadores de sistemas es lograr un buen equilibrio haciendo que los computadores sean efectivos sin comprometer a la seguridad.

El computador es sólo una parte de los sistemas de seguridad total. Por tanto, la definición de las políticas de seguridad adecuadas es mejor dejarla a los propietarios de los datos y a los creadores de las aplicaciones. El computador, y especialmente el sistema operativo, debería concentrarse en proporcionar un conjunto flexible y funcionalmente completo de mecanismos de seguridad de modo que las políticas de seguridad elegidas puedan ser efectivamente llevadas a la práctica.

7.1 POLITICAS DE SEGURIDAD[20]

Deben establecerse con claridad el marco y propósito de la seguridad y ello debe comunicarse a todas las partes involucradas para que esa seguridad se implemente y se mantenga con éxito. Un elemento clave para lograrlo son políticas de seguridad por escrito que sirvan para aumentar la concientización sobre la seguridad en toda la organización. [2]

[20] Milan Milenkovic, Sistemas Operativos, E .U. A. 2ª Edición 1980, p. 376

1. Como se pueden introducir y sacar información del sistema.
2. Quién esta autorizado a acceder a qué información y bajo qué condiciones.
3. Cuáles son los flujos permisibles de información dentro del sistema.

7.1.1 Principios

Las politicas de seguridad suelen estar guiadas por los antiguos principios de:

- **Minimo de privilegio:**

Cada sujeto debería tener permitido acceso únicamente a la información esencial necesaria para completar las tareas que el sujeto está autorizado a realizar.

- **Separación de deberes:**

Si hay un conjunto de operaciones que puede poner en riesgo una organización, debería exigirse que dos o más personas con intereses contrapuestos estuviesen implicadas en ellas. Es decir, deberían ser necesarias dos personas con dos llaves diferentes para abrir la caja de caudales.

- **Rotación en roles:**

Las operaciones delicadas no deberían ser confiadas permanentemente al mismo personal; una cierta rotación en las responsabilidades es más probable que descubra incorrecciones.

- **Control de acceso discrecional**:

Estas políticas son generalmente definidas por el propietario de los datos, quien puede transferir derechos de acceso a otros usuarios. Generalmente, el creador de un archivo puede especificar los derechos de acceso de los usuarios. Esta forma de control de acceso es habitual en sistemas de archivos. El ser vulnerable al ataque de caballos de Troya, en donde los intrusos se hacen pasar por usuarios legítimos.

- **Control de acceso obligatorio:**

Las restricciones de acceso obligatorio no están sujetas a la discreción del usuario y por tanto limitan el daño que un caballo de Troya puede causar. En este esquema, los

usuarios se clasifican en clase de seguridad especifica. Por ejemplo los administradores universitarios no pueden transferir a los estudiantes el derecho de acceder a los registros de notas.

7.1.2 Componentes claves de las politicas de seguridad

- **Apoyo e involucración de la gerencia**

La gerencia demuestra su compromiso aprobando y respaldando claramente la concientización en la seguridad y capacitación formales.

- **Filosofía respecto del acceso**

El acceso a la información computadorizada debe realizarse exclusivamente en una necesidad de saber, necesidad de hacer.

- **Autorización de acceso**

Un gerente responsable del acceso correcto y generación de información debe extender una autorización por escrito para que los usuarios accedan a información computarizada. Dichas autorización debe pasar directamente al administrador de seguridad de manera que no ocurra una manipulación o alteración de la autorización.

- **Revisión de la autorización de acceso**

Como con cualquier otro control, los controles de acceso deben ser evaluados en forma regular para asegurar que siguen siendo eficaces. Los cambios de personal y en los departamentos, intentos maliciosos, el puro descuido pueden producir un impacto sobre la eficacia de los controles de acceso. "Por esa razón, el Administrador de seguridad, asistido por los gerentes que dan autorización de acceso, deben hacer un examen de los controles de acceso por lo menos una vez por año. Debe actualizarse cualquier acceso que exceda la filosofía de "necesidad-de-saber. Necesidad-de-hacer".

- **Percepción de la seguridad**

Todos los empleados, incluyendo la gerencia, deben ser recordados de la importancia de la seguridad por medio de:

- Una política de seguridad por escrito
- Entrenamiento
- Declaración de no-divulgación firmada por el empleado
- Boletines internos de la empresa
- Vigencia ostensible de las normas de seguridad
- Auditorías periódicas

- Las responsabilidades de los empleados incluyen las siguientes:

  - Mantener en secreto el código de ID y las contraseñas
  - Informar de cualquier sospecha de violación de la seguridad al Administrador de seguridad
  - Leer la política de Seguridad
  - Mantener una buena seguridad física al conservar con llave las puertas, salvaguardando las claves de acceso, no divulgando las combinaciones de las cerraduras de acceso de las puertas, e interrogando a las personas desconocidas.

Los terceros que no son empleados de la compañía y que tienen acceso a los sistemas de la empresa también deben conocer las políticas y consiguientes responsabilidades de seguridad.

- **Papel del administrador de seguridad**

El administrador de seguridad, por lo general un miembro del departamento de Sistemas de Información, tiene a su cargo la responsabilidad de implementar, monitorear, y hacer cumplir las normas de seguridad establecidas ya autorizadas por la gerencia. Para lograr una apropiada segregación de funciones, no debe estar a cargo de actualizar los datos de las aplicaciones ni ser un usuario final, programador de aplicaciones, operador del computador o empleado de carga de datos. En las organizaciones más grandes, es una función de tiempo completo; en otras más pequeñas puede ser realizada por alguien que también tenga otras responsabilidades que no estén en conflicto.

7.2 ASPECTOS DE SEGURIDAD

Los controles de acceso y ambientales brindan elementos de confidencialidad, integridad, protección y disponibilidad administrada de las instalaciones y sistemas computadorizados. Tales controles reducen el riesgo de condiciones adversas al negocio debidas mal funcionamiento del computador, fallas en los datos o el software, o abuso de responsabilidades, en tanto se continúa proveyendo información y servicios computarizados para quienes lo necesiten.

Hay dos aspectos de la seguridad de la información. Estos son:

- **La seguridad fisica** - Control sobre el acceso físico al hardware, incluyendo el CPU, las cintas y unidades de disco, terminales de la computadora y los medios para el almacenamiento de información como son cintas y discos.
- **Seguridad Lógica** - Control sobre el acceso a los recursos del sistema, incluyendo la capacidad para accesar la información o ejecutar programas y transacciones.

La seguridad podría ser especialmente importante en los casos de clientes con sistemas complejos que contienen numerosos controles programados o que ejecutan rutinas automatizadas de autorización y aprobación para las transacciones contables, tales como aprobación para el pago o uso de Intercambio Electrónico de Datos (IED) para compras y control de inventario. El acceso a los sistemas de la computadora puede permitir que personal no autorizado afecte estos procesos, dando como resultado errores o pérdida de activos. Cuando una de las siguientes situaciones surge, debemos completar este perfil:

- El cliente tiene rutinas automatizadas de aprobación y autorización, que pueden causar el movimiento de grandes cantidades de activos, incluyendo efectivo, inversiones o inventario.

- Un número importante de procedimientos de control programados, dependen de la existencia de restricciones adecuadas de acceso.

Si ninguna de las condiciones se cumple y no hemos identificado controles de seguridad que atenúen un riesgo identificado de error, podemos concluir que la confiabilidad de los

sistemas no depende de los controles de seguridad de la información y por lo tanto no necesitamos responder las preguntas relacionadas con la seguridad.

7.2.1 SEGURIDAD FÍSICA Y EL AMBIENTE

El departamento de sistemas debe contar con los elementos de seguridad física suficientes para proteger tanto software como hardware de posibles contingencias.

La exposición a riesgos físicos y ambientales puede producir pérdidas financieras, repercusiones legales, pérdida de credibilidad o pérdida de competitiva. Tiene causas de origen natural o humanos y puede exponer el negocio al riesgo de acceso no autorizado. Desde un punto de viste de sistemas, las funciones que deben protegerse son las siguientes:

Documentar y evaluar la seguridad física y los controles ambientales del lugar en donde se encuentra el equipo de computación y medios de almacenamiento para determinar la adecuación de los controles al examinar el lugar.

Probar los controles sobre la seguridad física y protección del ambiente para determinar su funcionamiento y eficacia mediante la aplicación de técnicas de auditoria apropiadas.

Evaluar el ambiente de seguridad física para determinar que se cumplen los objetivos de control al analizar el resultado de pruebas y otras evidencia de auditoría.

7.2.1.1 EXPOSICIONES DE RIESGOS FISICOS

Para ejercer esta seguridad es recomendable considerar lo siguiente:

a) Debe evaluarse lar rutas de ingreso físico para comprobar una seguridad adecuada:

- Todas las puertas de acceso

- Ventanas y divisores de vidrio
- Divisores de habitaciones y cubículos modulares móviles
- Sobrepisos
- Sistemas de ventilación

b) Las exposiciones a riesgos debidas a violaciones accidentales o intencionales incluyen:

- Ingreso no autorizado
- Daño a equipamiento y propiedad
- Vandalismo sobre equipamiento, propiedad y documentos
- Hurto de equipo, propiedad o documentos
- Copiado o visualización de información delicada
- Alteración en equipamiento o información de naturaleza sensible
- Divulgación de información sensible
- Abuso de confianza de los recursos de procesamiento
- Extorsión
- Defraudación

La mayor exposición a riesgos la producen quienes no están informados, lo hacen accidentalmente o sin saberlo, aunque la seguridad se refiere a todos los posibles causantes de una violación.

c) Controles físicos:

Los controles físicos están diseñados para proteger a la organización ante accesos no autorizados. Los controles físicos deben circunscribir el acceso a solamente el personal autorizado por la gerencia. Esta autorización puede ser explícita, como una puerta con cerradura, para la cual la gerencia ha dado la llave o bien implícito, como un perfil de tareas que implica acceso a informes y documentos sensitivos.

- Puertas con cerrojo
- Cerradoras con combinaciones
- Cerraduras electrónicas
- Cerraduras biométricas de puertas
- Entrada en un registro histórico
- Manual

  Debe exigirse que todos los visitantes firmen un registro que indique su nombre y apellido, empresa a la que representa, razón de la visita y persona con la que se entrevistan. Generalmente se hace en el escritorio de recepción y entrada a la sala del computador. Antes de tener acceso, se debe exigir a los visitantes que presenten un medio de verificación de la identidad.
- Electrónico
- Cámaras de video
- Guardias de seguridad
- Persona de mantenimiento
- Cerrojos en terminales del computador
- Sistema de alarma

7.2.1.2 EXPOSICIONES DE RIESGOS AMBIENTALES

Las exposiciones ambientales a riesgos básicamente se producen por fenómenos naturales. Sin embargo, con controles adecuados, puede reducirse la exposición de tales elementos.

Los controles ambientales reducen el riesgo de interrupción de la actividad del negocio debido a un entorno afectado en forma adversa. Este entorno incluye la calidad del aire, corriente eléctrica y condiciones de terreno y atmosféricas.
Las exposiciones riesgos básicamene se producen por fenómenos naturales. Sin embargo, con controles adecuados, pueden reducirse.

- Incendio
- Desastres naturales

- Terremotos, volcanes, huracanes, tornados, etc.
- Inundación
- Falla del suministro eléctrico
- Picos de tensión
- Falla del sistema de aire acondicionado
- Cortoscircuitos
- Fallas de equipos
- Daños por humedad
- Amenazas o ataque de bombas.
- Detectores de agua,

  Debe colocarse detectores de agua en la sala de computador debajo del piso sobre-elevado y cerca de los drenajes del piso. Todo centro de almacenamiento de equipo que no tenga personal permanente también debe tener detectores de agua. Cuando se activan los detectores deben producir una señal que pueda ser escuchada por el personal de seguridad y de control.
- Extinguidores portátiles,

  Los extinguidos portátiles deben estar ubicados en posiciones estratégicas en todo el centro. Debe tener una etiqueta de inspección y debe ser revisado en forma anual. Deben indicar que sirven para incendios de clase A, B, o C.
- Alarmas de incendio manuales,

  Deben existir alarmas de accionamiento manual en ubicaciones estratégicas en todo el centro.
- Detectores de humo,

  Debe existir detectores de humo por debajo y por encima de los panales del cielo raso en todo el centro, y por debajo del piso sobre-elevado de la sala del computador. Los detectores deben producir una señal que se pueda escuchar cuando sean activados.
- Sistemas de supresión de incendios,

  Los sistemas de supresión de incendios están diseñados para que se activen en forma automática luego de que detecten una fuente de gran calor con las que se produce un incendio. Como los detectores de humo que deben producir una señal audible cuando sean activados. El sistema debe ser revisado y comprobado en forma anual. El sistema debe accionar automáticamente otros mecanismos para delimitar el incendio.

Ello incluye cierre de puertas, aviso al departamento de bomberos, cierre de conductos de ventilación y apagado de equipo eléctrico no esencial.

Existen varios medios para la supresión de incendios:

- Agua,

  Son rociadores, son eficaces pero no son muy populares pues dañan los equipos y otros bienes.
- Halón 1301,

  Los sistemas a base de Halón liberan gas a alta presión para quitar el oxigeno del aire, con lo que se impide la combustión. El Halón es bastante popular que no daña el equipo como el agua. Debe existir una señal de alarma audible y una breve demora antes de que se inunde con este gas para que el personal pueda evacuar el área y discontinuar el procesamiento y desconectar los equipos. Debido a sus efectos perjudiciales sobre la capa de ozono, se están realizando investigaciones para reemplazarlo por otros sistemas.
- Ubicación estratégica de la sala del computador,
  - Para reducir los riesgos de inundaciones, la sala del computador no debe estar en los subsuelos o sótanos del edificio. En un sistema de varios pisos, los estudios indican que la mejor ubicación que reduce los riesgos de fuego, humo y daño por agua para la sala del computador son los pisos 3, 4, 5 o 6.
  - Inspección periódica por parte de expertos del departamento de bomberos.
  - Para asegurar que todos los sistemas de detección de incendios cumplen con códigos de edificación, el departamento de bomberos debe inspeccionar el sistema y las instalaciones en forma anual. Asimismo, debe notificarse la ubicación de la sala del computador al Departamento de Bomberos a fin de que, en caso de incendio, apresten el equipo adecuado para incendios de material eléctrico.
  - Paredes, pisos y cielos rasos incombustibles alrededor de la sala del computador.
  - Las paredes que rodean la instalación de procesamiento de información deben acotar o bloquear la expansión del incendio. Las paredes que rodean la instalación deben tener una capacidad probada de resistir el fuego por lo menos dos horas.

- Protectores de pico de tensión,

  Son aparatos que reducen el riesgo de daños al equipo por picos de tensión. Utilizan reguladores de voltaje que miden la corriente que llega y bien aumentan o disminuyen la carga para mantener una corriente constante. Por lo general están incorporados en los sistemas de fuentes eléctricas ininterruptibles (UPS).

- Suministros ininterruptibles de energía (UPS- Uninterrulacionptible Power Supply)

  Un sistema de UPS incluye un generador, a bateria o combustible, que hace interfase entre las lineas eléctricas que entran a la instalación y la conexión que da energia al computador. El sistema generalmente "limpia" la energía a fin de que la potencia de la corriente al computador sea uniforme. En caso de que se interrumpa la energía, el UPS continúa suministrando al computador corriente desde el generador durante cierto lapso. Según el grado de sofisticación de la UPS el suministro puede durar días o tan solo unos minutos par poder hacer una desconexión ordenada del equipo. El sistema de UPS puede estar integrado en el computador o puede ser un equipo externo al mismo.

- Cableado ubicado en paneles y cañerías para electricidad

  Los incendios por electricidad siempre constituyen un riesgo. Para reducir el riesgo de que ocurra un incendio de ese tipo y se extienda, el cableado eléctrico debe estar oculto y en cañerías a prueba de fuego. Estas cañerias generalmente incluyen un poso sobre-elevado a prueba de incendio en la sala del computador.

- Prohibición de comer, beber y fumar dentro de la instalación de procesamiento de información,

  Los alimentos, bebidas y el tabaco pueden provocar incendios, acumulación de contaminantes o dañar el equipo de naturaleza sensible (especialmente los líquidos). Deben ser desterrados de la instalación de procesamiento de la información. Esta prohibición debe ser expresa.
- Planes de evacuación de emergencia documentados y probados

  Los planes de evacuación deben hacer hincapié en la seguridad de las personas.

- Acceso restringido sólo a personal del departamento de sistemas al cuarto del computador (SITE), mediante tarjetas electromagnéticas o llaves que se otorguen a los autorizados para ello.
- Existencia de un "palomar" o ventanilla a través de los cuales se entregarán los reportes a los usuarios y así evitar su acceso al "site".
- No almacenar papelería dentro del "site" ya que es susceptible de incendiarse fácilmente.
- Instalar un equipo de "No break" que permitiera no estar a expensas de fallas en el suministro de energía eléctrica.
- Contar con un piso falso en el cual se coloque el cableado de la máquina con el fin de evitar un posible corto circuito dentro del "site".
- Instalar un equipo de aire acondicionado confiable para mantener la temperatura del computador adecuada.

7.2.1.3 EJEMPLO DE REVISIÓN.

1. ¿Hay seguridad física para el hardware y los datos electrónicos adecuada para el uso de las computadoras del cliente?

   Describa los controles diseñados para asegurar que:

   - El acceso al procesador de la computadora, al disco y a los dispositivos para almacenamiento de información en cinta, al equipo de comunicaciones y a la consola de control está restringido a personal autorizado.
   - El acceso a los sistemas de las microcomputadoras que procesan las transacciones que son importantes en conjunto está restringido a personal autorizado.
   - La información se almacena físicamente en un lugar seguro.
   - Cuando el acceso lógico está restringido a las terminales en vez de a usuarios individuales, el acceso físico a tales terminales esté restringido a personal autorizado.
   - Copias impresas, informes y otras salidas, así como archivos en cintas o discos se distribuyen o se recogen por las personas asignadas.

Riesgos:

Robo, modificación, pérdida parcial o total de información y equipo básico para la operación de la empresa.

Controles:

Implantar un dispositivo adecuado de control de acceso garantice la seguridad de equipo e información localizada dentro del SITE.

1. ¿Incluyen los controles de equipo?
   - Mantenimiento preventivo periódico.
   - Ambiente físico adecuado (temperatura, humedad, energía eléctrica suficiente etc.)
   - Protección adecuada contra incendios (dispositivos de prevención, detección y extinción de incendios).

Riesgos:

En caso de siniestro puede ocurrir una pérdida parcial o total del equipo así como de la información que se guarda en dichos equipos, lo cual puede provocar pérdidas que afecten la operación.
Daños en equipo e información por falta de temperatura adecuada.

Control:

Implementar dispositivos adecuados de regulación y monitoreo de temperatura, prevención y extinción de incendios que garanticen la salvaguarda de equipo e información que se encuentra dentro del SITE.

MÉTODOS Y PROCEDIMIENTOS

- ¿Existe una política corporativa en cuanto a la propiedad de los datos y a la protección de los datos confidenciales?
- ¿Existen políticas y controles adecuados para la restricción de acceso a las bibliotecas de operación por parte de los programadores, de tal forma que se impidan cambios no autorizados?

Riesgo:

Si las medidas físicas de seguridad no son adecuadas, el acceso físico no autorizado a la computadora podrá dar como resultado la pérdida o sustitución de información, programas y salidas o daños intencionales a las instalaciones de la computadora y al equipo.

7.2.2 SEGURIDAD LÓGICA

Se refiere a la evaluación de los controles existentes en el departamento de sistemas con el objeto de asegurar la integridad de la entrada, proceso y salida de datos, la restricción de acceso a procesos y la identificación de usuarios autorizados, verificando entre otros aspectos el adecuado uso de claves de acceso, menús mandatarios y su congruencia con él puesto que se esta desarrollando. Se evalúa también la compatibilidad del sistema con el usuario, verificando el adecuado aprovechamiento que se tiene de éste, la frecuencia de fallas o trabajos complementarios manuales.

En muchas ocasiones, la seguridad puede ser administrada por el gerente de sistemas y deberá requerir una pequeña parte de sus actividades diarias a asegurarse que las medidas establecidas se estén llevando a cabo. Otra práctica común en organizaciones medianas o pequeñas, es delegar responsabilidades de seguridad en diferentes líneas. Por ejemplo, el gerente de operación puede encargarse de la seguridad física y acceso al "site", y la persona encargada del software de sistema puede mantener al dia los controles de acceso.

En organizaciones más complejas, se está incrementando el reconocimiento de la importancia de coordinar todos los aspectos que se relacionan con la seguridad del computador a través de asignar a una persona o un grupo reducido de personas con la función de **administrador de la seguridad**. Estas personas pueden no tener una relación directa dentro del departamento de sistemas (por ejemplo, auditoría interna).

La seguridad lógica evita que personas no autorizadas puedan entrar al sistema y obtengan información que no requieren conocer.

7.2.2.1 CONTRASEÑAS

En sistemas basados en contraseña, cada usuario tiene una contraseña, que puede ser inicialmente asignada por el sistema o por un administrador. Muchos sistemas permiten a los usuarios cambiar posteriormente sus contraseñas. El sistema almacena todas las contraseñas de usuario y las utiliza para validarlos. Cuando un usuario inicia una sesión, el sistema solicita y el usuario suministra una contraseña presumiblemente secreta y especifica.[21]

Las contraseñas son populares ya que no requieren un hardware especial y son relativamente fáciles de implementar. En el lado negativo, las contraseñas ofrecen protección limitada, ya que pueden ser relativamente fáciles de obtener o adivinar.

Las contraseñas elegidas por los usuarios son frecuentemente palabras de diccionario o nombres propios. Esto hace que sean fáciles de recordar pero también fáciles de adivinar. Por ejemplo, los ID, nombres o apellidos de usuarios, deletreados hacia atrás o hacia adelante, contabilizan típicamente un significativo porcentaje de las contraseñas usadas. Los ataques a las contraseñas suelen intentar primero estas posibilidades y seguir luego quizá con una lista personalizada de contraseñas comunes y conocidas. Si éstas fallan, el alcance puede proceder por prueba y error con palabras contenidas en el diccionarios en línea. Si las contraseñas son palabras de un diccionario facilitan la ruptura de la clave de cifrado mediante prueba y error exhaustiva con ayuda de un computador.

[21] Milan Milenkovic, Sistemas Operativos, E .U. A. 2ª Edición 1980, p. 379

Las contraseñas elegidas por el sistema, por otro lado, son generalmente combinaciones aleatorias de letras y números que son difíciles de adivinar pero también difíciles de recordar. Como resultado, los usuarios tienden a anotarlas y almacenarlas en algún lugar a mano cerca del terminal. En vez de la exposición a la adivinación nos encontramos con la exposición a la revelación del secreto.

Se ha propuesto varias técnicas auxiliares para reforzar el nivel de protección posibilitado por el mecanismo de contraseña. Desgraciadamente, la mayoría de ellas tienen desventajas que reducen su efectividad o su aceptación por el usuario. Por ejemplo, los esquemas de contraseña adicionales a petición del sistema a intervalos aleatorios durante el uso del computador. Esto tiende a fastidiar a los usuarios legítimos.

Otro grupo de técnicas pretenden desanimar a los usuarios no autorizados que intentan iniciar sesiones probando una serie de contraseñas diferentes. Un modo de tratar el problema es limitar el número de intentos consecutivos de aperturas de sesión desde un destino dado y proceder a la consiguiente desconexión en línea.

7.2.2.1 CARACTERISTICAS DE LAS CONTRASEÑAS

Las contraseñas deben ser fáciles de recordar para el usuario, pero difíciles de adivinar para quien intente adivinarla.

La primera asignación de contraseña debe ser hecha por el administrador de seguridad. Cuando el usuario hace una conexión por primera vez, el sistema debe obligarlo a cambiarla para mejorar su confidencialidad.

Si se ingresa una contraseña errónea una cantidad determinada de veces, por lo general tres, debe ser desactivada automáticamente por un lapso apreciable.

Si un código de ID ha quedado desactivado por el olvido de la contraseña, el usuario debe notificar al administrador de seguridad. Entonces este último debe reactivar el código de ID sólo tras verificar la identificación de los usuarios, tal como lo hace un banco

con la identificación de un cuentahabiente antes de dar información por teléfono, por ejemplo: apellido de soltera de la madre.

Las contraseñas deben estar encriptadas internamente. La encriptación es un medio de codificar la contraseña almacenada. Con ello se reduce el riesgo de que un individuo tenga acceso a las contraseñas de otras personas; si no puede entender, tampoco la puede utilizar.

Las contraseñas no deben exhibirse de ninguna manera, ni en la pantalla del computador cuando se ingresa, ni en los informes computarizados, o escritas sobre un papel adherido al escritorio de una persona.

Debe cambiarse periódicamente. En forma regular, por ejemplo cada 30 días, el usuario debe cambiar su contraseña. El mejor método es que el sistema computarizado obligue a cambiarla.

Reglas de sintaxis de la contraseña.

- Debe tener por lo menos cuatro caracteres de longitud. Más corta es fácil de adivinar.
- Debe permitir la combinación de caracteres alfabéticos y numéricos.
- No debe poder asociarse en especial con el usuario, como sucede con el primer nombre, nombre del cónyuge, de una mascota etc.
- Cuando se cambia el sistema no debe permitir que se vuelvan a utilizar las mismas contraseñas.

Los códigos de ID que no sean utilizados tras un lapso de tiempo, deben ser desactivados para evitar que sean mal utilizados. Lo puede hacer el sistema de forma automática o que lo haga manualmente el administrador de seguridad.

7.2.2.2 RUTAS DE ACCESO LOGICO

El acceso lógico al computador puede hacerse por distintas vías:

- **Consola del operador**

Estas terminales privilegiadas controlan la mayoria de las operaciones y funciones del computador. Para brindar seguridad, estas terminales deben estar ubicadas en la sala del computador o en instalaciones adecuadamente controladas de manera que el acceso físico al computador sólo pueda ser hecho por los operadores del comptutador y el personal de soporte.

- **Terminales en línea**

Este acceso lógico es el más popular entre los usuarios. Generalmente requiere un código de ID y una contraseña para tener acceso al computador. El acceso en línea permite el procesamiento de los datos en forma inmediata. El acceso en línea sirve para la carga de transacciones, consultas a archivos y actualización de los archivos. Dado que el acceso es inmediato, también lo es iniciar la seguridad lógica respecto de este acceso. Este control se satisface con el uso de software de control de acceso.

- **Procesamiento diferido**

Esta modalidad de acceso es indirecta ya que se realiza el acceso por medio del procesamiento de transacciones. Generalmente cosiste en acumular las transacciones de entrada y procesarlas luego de determinado lapso o luego de que se haya acumulado cierta cantidad de transacciones. La seguridad se realiza limitando a quienes pueden acumular transacciones.

- **Puertas de telediscado**

La utilización de puertas de conexión de discado telefónico consiste en contactar una terminal remota a una línea telefónica y así tener acceso al computador al discar el

número de una línea telefónica especial. A menudo debe utilizarse un módem como interfase entre la terminal remota y la línea telefónica a fin de codificar y descodificar las transmisiones. La seguridad se realiza al dar un medio identificado con el usuario remoto para determinar la autorización de acceso que posee. Ello puede ser por medio de línea de llamado invertido, utilización de un código de ID y software de control de acceso, o haciendo participar a un operador del computador para que verifique la identidad de quien hace la llamada y luego realiza la conexión al computador.

- **Redes de telecomunicaciones**

Las redes de telecomunicaciones enlazan una cantidad de terminales de computador con un computador por medio de líneas. Las líneas pueden ser privadas, es decir dedicadas a solo un usuario, o públicas, como las de los sistemas nacionales de teléfonos. La seguridad debe realizarse de la misma manera que en las terminales en línea.

7.2.2.3 RIESGOS DE ACCESO LOGICO

Los controles de acceso lógico inadecuados incrementan el riesgo de que la organización incurra en pérdidas a causa de exposiciones a riesgos técnicos y del negocio. Tales exposiciones pueden provocar inconvenientes menores a la detección completa de las funciones computadorizadas.

- **Causantes de violación de acceso lógico**

A menudo quienes violan el acceso lógico son las mismas personas que pueden aprovecharse de las exposiciones a riesgos físicos, aunque las destrezas que se requieran para aprovecharse de las exposiciones a riesgos lógicos son de índole más técnica y compleja.

- **Piratas informáticos**

Los piratas informáticos por lo general intentan poner a prueba los límites de las restricciones de acceso para demostrar su capacidad para superar los obstáculos. A

menudo no ingresan con el propósito de destrucción, aunque a menudo ese es resultado final.

- **Empleados autorizados y no autorizados.**

Son quienes tienen el acceso a la información computadorizada más fácil debido a que custodian la información. A demás de los controles de acceso lógico, la buena segregación de funciones y supervisión ayudan a controlarlos.

- **Usuarios finales**

En particular hay que tener cuidado con los ex-empleados que han dejado la organización en condiciones desfavorables.

- **Terceros interesados o capacitados**

  - Competencia
  - Potencias extranjeras
  - Crimen organizado
  - Piratas informáticos contratados por un tercero

- **Personal de tiempo parcial o temporario**
- **Proveedores y consultores externos**

7.2.2.4 EXPOSICIONES A RIESGOS DE ACCESO LÓGICO.

Las exposiciones a riesgos que existen debido al aprovechamiento de las debilidades de control de acceso lógico accidental o intencional incluyen:

- **Exposición de carácter técnico**

Alteración, uso o destrucción de programas de producción y archivos de datos no autorizados. Estas exposiciones incluyen código de programa oculto y la modificación

directa o indirecta de datos y programas. Existen muchos términos para estos tipos de exposición entre los que se encuentran:

1. **Manipulación de datos**

Consiste en la alteración de datos antes o a medida que se ingresa al computador. Este es el abuso más generalizado dado que se requiere poco conocimiento técnico y se realiza antes de que la seguridad del computador pueda proteger los datos.

2. **Caballos de Troya**

Consiste en ocultar código con fines maliciosos dentro de un programa autorizado. Tal código oculto se ejecutará cuando se ejecute el programa autorizado.

3. **Redondeo por defecto**

Consiste en retirar pequeñas sumas de dinero de una transacción o cuenta computarizada y enviar la cantidad a la cuenta del autor de la violación.

4. **Técnica del salame o tajada**

Consiste en tomar una pequeña tajada de la sumas de las transacciones o cuentas computarizadas.

5. **Virus informáticos**

Los virus informáticos son programas dolosos que pueden auto-duplicarse y transmitir de un computador a otro, sea al compartir disquetes o por la transmisión de la lógica por medio de líneas de telecomunicaciones o contacto directo con el código máquina infectada.

Un virus puede simplemente mostrar un mensaje gracioso en las terminales, o borrar peligrosamente o alterar los archivos, o llenar la memoria del computador con basura hasta el punto que el computador ya no funciona. El peligro adicional es que un virus permanezca "hibernando" o en un estado aletargado hasta que determinando acontecimiento lo pone en actividad, como una fecha (el 1 de enero - Feliz año Nuevo) o que se copie una cantidad de veces.

6. **Gusanos**

   Son programas destructivos que borran datos o utilizan grandes cantidades de recursos del computador peno no se duplican.

7. **Bomba lógica**

   Las bombas son similares a los virus pero no se duplican.

8. **Puertas traseras.**

   Las puertas traseras son salidas o puertas abiertas hacia fuera de un programa que permiten que se inserte lógica especial dentro en un programa autorizado, tal como interruptores del programa para poder revisar los datos en el medio de procesamiento. Estos "agujeros" también permiten que se inserte lógica no autorizada.

9. **Ataque asincrónico**

   En un ambiente de multiprocesamiento, los datos viajan a través de lineas de telecomunicaciones asincrónicas (en una sola dirección). Por ello, muchas transacciones deben "esperar" que la línea esté libre y fluya en la dirección adecuada antes de que se las trasmita. Los datos que están en espera son susceptibles a acceso no autorizado denominado ataques asincrónicos. Este es una exposición muy compleja, para evaluarla el auditor de SI necesitará la ayuda del administrador de red y del analista de software.

10. **Fugas de datos**

    La fuga de datos consiste en la extracción de la información del computador. Puede realizarse impidiendo archivos en listados, o simplemente robarse informes computarizados o cintas.

11. **Intercepción de lineas**

    Esta técnica consiste en captar la información que se está transmitiendo por medio de líneas de telecomunicaciones.

12. **Apagado del computador**

Puede iniciarse el apagado del computador por conexiones directas (en línea) con terminales o microcomputadores, o indirectas (líneas de telediscado) de terminales. A menudo para ello se requiere tener acceso a un código ID de alto nivel. No resulta tan difícil si los controles de acceso correctos no están implementados alrededor de los códigos de ID y las conexiones de telecomunicaciones con el computador.

13. **Interrupción de servicio**

Las líneas de telecomunicaciones son vulnerables a que alguien se entrometa con ellas o que sean contadas de manera accidental.

7.2.2.5 EXPOSICION DE DELITOS INFORMATICOS.

Los delincuentes pueden utilizar los sistemas informáticos para robar dinero, bienes, software o información de la empresa. También constituye un delito cuando se manipula el proceso de aplicación o datos para que se acepte información falsa o transacciones no autorizadas.

Los delitos informáticos con el fin de aprovechar el computador y la información que contiene pueden ser perjudiciales para la reputación, la moral y la mismísima existencia de una organización. El saldo puede consistir en la pérdida de clientes, una situación embarazosa para la gerencia y el inicio de acciones legales contra la organización.

7.2.2.6 CONTROLES DE ACCESO LOGICO

Pueden protegerse los archivos computarizados de acceso innecesario o no autorizados por medio de controles que reduzcan el riesgo de utilización inadecuada, robo, alteración o destrucción intencional o no. En un ambiente de procesamiento por lotes, este control puede preverse limitando o monitoreado las actividades del operador del computador. En un sistema en línea, las rutas de acceso son más complejas y directas, y el nivel de control debe ser consecuentemente más complejo. Estos controles de acceso no necesitan ser aplicados solamente a los operadores del computador, si no también a los

usuarios finales, programadores, administradores de seguridad, gerencia y a toda persona que pueda utilizar el computador.

- **Códigos de ID y contraseñas para limitar el acceso.**

Puede utilizarse esta identificación del usuario en dos etapas en el cual el sistema computarizado primero verifica que el usuario tiene un código de ID válido y luego obliga al usuario a substanciar su validez personal por medio de una contraseña.

Las reglas de acceso detallan quién puede tener acceso a qué. Tal acceso debe hacerse sobre la base de la necesidad de saber, la necesidad de hacer y los tipos de acceso disponibles.

Tener acceso al computador no siempre implica que se tenía acceso sin restricciones. Puede fijarse el acceso al computador en diferentes niveles. Al limitar el acceso a un nivel adecuado, puede brindarse una capa de seguridad. Cuando el Auditor de SI hace una revisión del acceso a un computador, desea saber qué puede hacer con ese acceso. Entre estos tipos de restricciones se incluyen:

- De sólo leer
- De sólo consultar
- Leer - escribir
- Crear
- Actualizar
- Borrar
- Ejecutar
- Copiar

El tipo de acceso menos peligroso es el de sólo consulta, en tanto que la información a la que se accede no sea sensible o confidencial. Ello es así puesto que el usuario no puede utilizar el archivo computadorizado más que para hacer una vista o visualizarlo.

Al hacer una revisión el auditor de Sistemas de Información debe buscar:
"Patrones o tendencias que indican el abuso a los privilegios de acceso o concentrarse en una aplicación sensible, y violaciones tales como intentos de acceso a archivos computarizados que no están autorizados y la utilización de contraseñas erróneas".

El auditor debe tratar la violación con el administrador de seguridad para su investigación.

El administrador de seguridad y la gerencia responsable deben colaborar para investigar y determinar la severidad de la violación. Generalmente la mayoria de las violaciones son accidentales.

Si el intento de violación es serio, debe notificarse a la gerencia ejecutiva, no a autoridades legales. Le corresponde a la gerencia hacer la denuncia a las autoridades.

Debe existir directivas escritas para actuar ante violaciones de acceso que identifiquen los diversos tipos y niveles de violación, y cómo debe responderse ante ellos. Con ello se logran definir criterios para juzgar la seriedad de la violación.

7. 2 .2. 7 PROCEDIMIENTOS DE AUDITORIA

El auditor de sistemas debe analizar y evaluar las políticas, estructuras organizativas, procedimientos operativos y controles de acceso utilizados para proteger el software y archivos de datos ante una divulgación, manipulación o destrucción no autorizadas.

El auditor debe de tener en cuenta las siguientes tareas para evaluar los controles de acceso lógicos:

- Obtener una comprensión general del ambiente de procesamiento de información para evaluar las necesidades de seguridad por medio de una revisión de la documentación pertinente, indagación y observación.
- Documentar y evaluar los controles sobre las potenciales vías de acceso al sistema para asegurarse de su adecuación, eficiencia y eficacia mediante una

revisión apropiada de las correspondientes funciones de seguridad de hardware y software e identificar cualquier deficiencia o redundancia.

- Probar los controles acerca de rutas de acceso para determinar su funcionamiento y eficacia al aplicar técnicas de auditoría apropiada.
- Evaluar el ambiente de control de acceso para determinar que se satisfacen los objetivos de control al analizar resultados de pruebas y otra evidencia de auditoría.
- Evaluar el ambiente de seguridad para asegurarse de su adecuación al revisar las políticas por escrito, observar las prácticas y procedimientos y compararlos con las normas correspondientes de seguridad.

7. 2. 2. 8 EJEMPLO DE REVISION

1. ¿Hay políticas de seguridad establecidas que provean lo necesario para la dirección e implantación general de la seguridad?

   Si así es, describa los controles diseñados para asegurar que:

   - La política se comunica efectivamente a los usuarios y al personal de procesamiento de datos
   - El cumplimiento de la política lo monitorea efectivamente el personal encargado de seguridad
   - La política se revisa periódicamente para asegurar que sigue siendo adecuada aún con los cambios en la tecnología o en el negocio del cliente

1. ¿Hay rutinas o procedimientos establecidos para la asignación o modificación de la capacidad de acceso?

   Si así es, describa los controles diseñados para asegurar que:

   - La gerencia, a un nivel adecuado, es responsable de autorizar el acceso a la información y a los sistemas, y que se considera una adecuada segregación de funciones para conceder la autorización
   - Hasta donde sea posible, se asigna una identificación única a usuarios individuales
   - Los usuarios son responsables de rendir cuentas sobre la actividad realizada en el sistema con el uso de su identificación de usuario

- Se avisa al encargado de seguridad (o a otro administrador) cuando el personal se retira de la compañia, o cambia de puesto, con el fin de trasladar o cambiar oportunamente sus capacidad de acceso
- Se da a conocer al gerente correspondiente el nombre de sus subordinados que tienen acceso a su información, y los niveles de acceso que tienen autorizado
- El acceso a los programas de utilería que pueden sumar, cambiar o borrar información o programas está restringido a un número mínimo de personas de procesamiento de datos

1. ¿Hay control de acceso al software en uso o está limitado el acceso de alguna otra manera, hasta donde sea posible, a través del sistema operativo, para restringir el acceso de los usuarios solo a los recursos de la computadora (información, programas, transacciones, etc.) que son necesarios para la realización de sus funciones?

Si así es, describa los controles diseñados para asegurar que:

- El sistema lo administra y lo monitorea personal competente autorizado
- El sistema se instaló correctamente
- Los cambios al software los hace personal técnico de soporte y que están sujetos a los procedimientos administrativos de cambios en el sistema operativo
- Los usuarios guardan en secreto sus claves de acceso
- Las claves de acceso están sujetas a un mínimo de posiciones, a cambios periódicos y a acuerdos apropiados
- Se utiliza efectivamente la capacidad de emisión de reportes del sistema, y se toman medidas correctivas y disciplinarias, si es necesario

Riesgos:

Si no están disponibles los controles de acceso lógico, o no son efectivos, es difícil restringir el uso no autorizado del sistema. Esto podrá ocasionar la pérdida de información, de programas, de activos u otros recursos. Además, los controles de acceso lógico pueden ser muy efectivos para reducir los errores de procesamiento, restringiendo el acceso a los usuarios autorizados y conocedores y a los programas de producción.

Carencia de control con respecto a las cuentas activas que en realidad son usadas.

Desperdicio de volumen en disco.

Sin políticas de seguridad establecidas, el acceso a los recursos de información no puede estar restringido de manera apropiada. Como resultado, los datos o los programas pueden ser modificados sin autorización. Una política de seguridad es importante, ya que es un medio para coordinar el nivel de seguridad sobre diversos recursos de información.

Si los usuarios no tienen asignados claves únicas, puede no ser posible hacerlos responsables de sus actividades cuando accesan al sistema. Si no se mantiene la confidencialidad de tales contraseñas, se facilita para los usuarios no autorizados acertar la clave y contraseña de un usuario autorizado y accesar al sistema.

Si a los usuarios se les otorga el acceso más allá del nivel mínimo necesario para realizar sus funciones, puede comprometerse la segregación de funciones. Esto daría por resultado la entrada de transacciones no autorizadas o inválidas, o la pérdida de datos, activos u otros recursos.

Controles:

Revisión de las cuentas de usuarios que no se usan desde seis meses atrás y cancelarlas.
Borrar las librerías de producción que no se utilizan.
Diseñar junto con el área de Recursos Humanos una política para el manejo y registro de cuentas de personal que deja de laborar en la compañía.

7.2.3 PLAN DE CONTINGENCIAS

Las operaciones clave de los negocios pueden verse afectadas en caso de que ocurra alguna contingencia que interrumpa el proceso normal de operación. Un control para reducir este riesgo consiste en desarrollar un plan que permita proteger de una manera adecuada la información y equipos con que se cuenta.

El plan de contingencias, es el proceso de definir, desarrollar, documentar y mantener planes de emergencia con el propósito de enfrentar cualquier tipo de desastre que de manera significativa afecte el desarrollo de procesamiento de información. Este tipo de desastres pueden incluir temblores, incendios, huelgas, fallas eléctricas, daño intencional a los respaldos o instalaciones, robo del equipo, etc.

En estos días, sólo existen pocas situaciones donde es posible volver a procesos manuales. Cuando esto es posible, el costo incurrido en pérdida de tiempo y confusión puede ser muy alto. Por lo tanto, las compañías deben proteger sus sistemas de sistemas de posibles destrucciones o interrupciones, desarrollando planes que puedan permitir seguir operando el negocio.

El propósito subyacente de la planificación de contingencias es poder reanudar la operación del negocio, es esencial que se considere la organización total, no solamente los servicios de procesamiento cuando se desarrolla el plan. Cuando no existe un plan unificado para la reanudación del negocio, el plan para el procesamiento de datos debe extenderse para incluir la planificación para todas las unidades que dependan de las funciones de procesamiento de datos.

7.2.3.1 PROPOSITOS

Los propósitos de un plan de contingencias van a estar definidos de la siguiente manera:

- **Acción de emergencia**

Los procedimientos para reaccionar a las crisis, desde los procedimientos de activación de gas Halón hasta evacuaciones de emergencia

- **Notificación**

Los procedimientos para notificar a los gerentes pertinentes en caso de que se produzca un desastre. Por lo general se incluye una lista de números de teléfonos particulares de emergencia.

- **Declaración de desastre**

Los procedimientos relacionados con la evacuación del daño que sigue al desastre. Los procedimientos para declarar un desastre e invocar el plan pertinente.

- **Recuperación de sistemas**

Los procedimientos que han de seguirse para restaurar los sistemas criticos y vitales a nivel de servicio de emergencia dentro de una macro de tiempo determinado de acuerdo con la estrategia de recuperación de sistemas definido en el plan.

- **Recuperación de la red**

Los procedimientos para reactivar las comunicaciones de voz y datos a niveles de emergencia dentro de un tiempo determinado de acuerdo con la estrategia de la recuperación de la red definida en el plan.

- **Recuperación de usuarios**

Los procedimientos para recuperar funciones de usuarios críticas y vitales dentro de un marco de tiempo, de acuerdo con la estrategia planificada. Ello incluye la documentación de las instrucciones tiempo, de acuerdo con la estrategia planificada. Ello incluye la documentación de las instrucciones para procesar manualmente los datos que antes podían procesarse por medio de un sistema automatizado. Inclusive si el procedimiento en una época fue manual, no debe darse por sentado su conocimiento. Esto es especialmente cierto puesto que muchos empleados con antigüedad como para haber realizado la tarea en forma manual pueden haber dejado la empresa.

- **Operaciones de Salvamento**

Los procedimientos para salvar las instalaciones, los registros y el hardware, a menudo incluyendo el reclamo de la póliza de seguro y la determinación de la viabilidad de volver a ocupar el sitio de desastre.

- **Reubicación**

Los procedimientos para reubicar las operaciones de emergencia a una instalación original o una instalación nueva y la restauración a los niveles de servicio normales.

7.2.3.2 DIFERENTES NIVELES DE DESASTRES

No todas las interrupciones del servicio se clasifican como desastre. Por ende, debe estar vigente un buen sistema de clasificación a fin de hacer una determinación para poder iniciar los esfuerzos destinados a recuperarse del desastre.

a) **No desastres**

La interrupción en el servicio que surge de un mal funcionamiento del sistema u toros fallas. Exige una acción para recuperar a un status operativo a fin de reanudar el servicio. Puede requerir restituir el hardware, software o archivos de datos.

b) **Desastres**

Interrupciones que provocan que toda la instalación se ponga en situación no operativa por un largo periodo de tiempo, generalmente más de un dia. Exige actuar para recuperar a un satus operativo, generalmente por medio de una instalación de procesamiento alternativa. Puede requerir restituir el software y los archivos de datos a partir de copias externas. Es necesario que la instalación alternativa esté disponible hasta que la instalación de procesamiento de datos original quede restaurada.

c) **Catástrofe**

Interrupciones mayores que son el producto de la destrucción de la instalación de procesamiento. Se requiere pasar a una instalación en stand-by al corto o largo plazo. Se necesita una instalación de procesamiento alternativo para satisfacer las necesidades operativas inmediatas, como en el caso de un desastre. Asimismo, debe identificarse y equiparse una instalación nueva, permanente para brindar una continuidad de los servicios de procesamiento de datos en forma periódica.

Deben proveerse todos los insumos necesarios para el esfuerzo de recuperación para que pueda continuarse con las actividades normales de negocios. Ello incluye procedimientos detallados actualizados impresos en papel que puedan ser seguidos con facilidad por el personal contratado que no está familiarizado con las operaciones estándares.

7.2.3.2 ORGANIZACION

A fin de implementar las estrategias que se han desarrollado para la recuperación del negocio, debe identificarse al personal clave en toma de decisiones. Esas personas generalmente están a cargo de equipos que se crean como respuesta a funciones o tareas críticas definidas en un plan. Según el tamaño de la operación del negocio.

Se debe contar con:

- Equipo de acción ante una emergencia: puestos de vigilancia de incendios. Ellos se encargarán de la evacuación ordenada del personal.
- Equipo de evaluación de daños: Evaluar la extensión del daño después del desastre.
- Equipo de la administración de la emergencia: Coordina los equipos de recuperación y toma decisiones claves.
- Equipo de sede alternativa de almacenamiento: Transporte y envío de medios magnéticos y los registros a la instalación de recuperación así como establecer y supervisar el almacenamiento.
- Equipo software: restaurar los paquetes de sistemas, carga y prueba de software de sistema operativo y resolver problemas a nivel de sistema.
- Equipo de aplicaciones: restaurar en los sistemas back-up.
- Equipo de seguridad: monitorea en forma continua la seguridad del sistema y los enlaces de comunicaciones, también resuelve los conflictos de seguridad que impiden la recuperación rápida del sistema. Se asegura de la instalación correcta y el funcionamiento del paquete de software de seguridad.
- Equipo de Operaciones de Emergencia: Constituido por los operadores de turno y los supervisores de turno que actuarán en la sede de recuperación de sistemas y administran la operación de sistema durante los proyectos de desastre y recuperación.
- Equipo de recuperación de red: Responsable de redireccionar el tráfico de las comunicaciones de voz y el tráfico de las comunicaciones de datos y restablecer el control de la red y acceso a la sede de recuperación. Da soporte continuo para las comunicaciones de datos y supervisa la integridad de la comunicaciones.
- Equipo de comunicaciones: Viaja a la sede de recuperación de los usuarios donde trabaja junto con el equipo de recuperación de red remota. También solicita la instalación y trabajar con los operadores de centrales telefónicas.

- Equipo de hardware para usuarios.
- Equipo de preparación de datos y registros.
- Equipo de soporte administrativo: Controla las funciones de contabilidad y nómina.
- Equipo de insumos.
- Equipo de salvamento: Provee la información necesaria para presentar los reclamos de seguros.

Un desastre es cualquier suceso que tiene un componente de azar o incertidumbre, que cuando ocurre tiene potencial como para interrumpir el procesamiento normal del negocio. Tales interrupciones a menudo se asocian con desastres naturales tales como terremotos, inundaciones, tornados, huracanes, incendio, etc. Sin embargo, los hechos desastrosos pueden ocurrir cuando a la empresa no se le brindan los servicios esperados, como una falta de energia, pérdida de capacidad de comunicaciones, pérdida de la provisión de gas, pérdida de servicio de transporte. Etc. Aunque la pérdida de tales servicios puede deberse a un desastre natural, también puede deberse a un hecho aislado. Un buen plan de contingencias deberá tener en cuenta todos los tipos de hechos desastrosos.

7.2.3.4 SEGUROS

La póliza de seguros de procesamiento de datos es por lo general una póliza multi-riesgo diseñada para brindar diversos tipos de cobertura de SI. Debe ser de constitución modular de manera tal que pueda adaptarse al ambiente particular de SI del asegurado.

7.2.3.5 LAPSO CRITICO DE RECUPERACION

Es el lapso de tiempo en el que debe reanudarse el procesamiento del negocio antes de arriesgarse a incurrir en pérdidas. Los lapsos de tiempo asociados en los que pueda considerarse un desastre o no-desastre siempre depende de la naturaleza del negocio que se interrumpe.

También la época del año o el día de la semana puede afectar el lapso de tiempo para la recuperación.

7.2.3.5.6 APLICACIONES QUE DEBEN SER RECUPERADAS

Aplicaciones que deben ser recuperadas dentro de un lapso crítico de recuperación son aquellas aplicaciones, software base y archivos de datos que han sido identificados y documentados como críticos deben ser enumerados en primer término. Debe realizarse un análisis del carácter crítico del tiempo, al identificar las aplicaciones criticas, el software de sistemas o los archivos de datos a recuperar.

7.2.3.5.7 RESPALDO DE MEDIOS MAGNETICOS Y DOCUMENTACION EN SEDE.

Un elemento crucial de un plan de contingencia en la sede original o alternativa es la disponibilidad de datos adecuados. La duplicación de datos importantes y de la documentación es un pre-requisito de cualquier tipo de recuperación incluyendo almacenamiento fuera d la sede de los datos de back-up y documentación.

- **Procedimientos periódicos de respaldos**

Los archivos de datos y el software deben ser resguardados en respaldos en forma periódica. El periodo en el que se programa el respaldo debe de ser según el programa de aplicación o sistema. Por ejemplo, ciertos sistemas de aplicación que corren en forma mensual, en los que se actualizan archivos o de transacciones requerirán que se programe un respaldo luego de la corrida mensual en producción. Sin embargo, el software de sistema o de aplicación que se actualiza frecuentemente puede requerir respaldos semanales. A menudo los sistemas en linea en tiempo real que procesan un gran volumen de transacciones exigen respaldos cada noche o de inmediato de las actualizaciones de archivos maestros en una instalación de procesamiento separada.

La programación periódica de los respaldos puede hacerse por medio de un sistema de administración automatizada de cintas y software de trabajo esquemático automatizado. La automatización del procedimiento de respaldo evitará ciclos erróneos u omitidos debido a errores del operador.

- **Frecuencia de rotación**

El respaldo de datos y software debe dar margen a la presencia continua de cambios. Con propósitos de back-up se conserva una copia del archivo o registro a determindado momento. También deben conservarse todos los cambios o transacciones que se presentan durante el intervalo entre la copia y la fecha actual.

- Puntos a tener en cuenta para establecer el cronograma de respaldos de archivos:
  - Debe determinarse la frecuencia del ciclo de respaldos y periodo de rotación para cada archivo de datos.
  - La estrategia de respaldo debe anticipar fallas en cualquier paso de ciclo de procesamiento
  - Los archivos maestros deben ser "back-upeados" en momentos convenientes, como al finalizar un procedimiento de actualización.
  - Los archivos de transacciones deben conservarse conciliados con los archivos maestros, de manera que pueda actualizar una generación previa de un archivo maestro para recrear el archivo maestro actual.
  - Los archivos en tiempo real requieren técnicas de respaldos especiales, tal como el registro de transacciones en un bitácora, la utilización de imágenes previas y/o posteriores a la actualización de registros maestros, identificación de las transacciones con la hora, simulación de comunicación, etc.
  - Los sistemas de Administración de Base de datos requiren un respaldo especializado.
  - Deben conservarse descripciones de los archivos de los cuales se hace respaldos; para los sistemas de bases de datos, estas descripciones pueden ser reemplazadas por una versión de los diccionarios de datos.
  - Puede ser necesario asegurarse de la licencia para utilizar ciertos en una sede alterna, y los arreglos deben hacerse con anticipación.
  - Respaldos del software debe incluir tanto las bibliotecas de código objeto y código fuente, y debe incluir un mecanismo para guardar los parches a los programas en forma actualizada en todas las sedes de respaldo.

De la misma manera, debe mantenerse toda la documentación que se necesite para una operación continua y exitosa del negocio en la instalación de respaldos en la sede

alternativa. Ello incluye los documentos fuente que se necesitan para la restauración de la base de datos de producción. De la misma manera que con los archivos de datos, las copias en las sedes alternas deben mantenerse actualizadas para asegurarse de que sean útiles.

- Entre la documentación de la que debe hacerse respaldos y almacenarse en la sede remota se incluye:

  - Procedimientos operativos
  - Documentación de sistema y programas
  - Procedimientos especiales
  - Documentos fuente de INPUT
  - Documentos Output
  - Una copia del Plan de Continuidad del Negocio Vigente

- Puesta a prueba del plan de continuidad del negocio.

La mayoría de las pruebas de contingencias son de escala menor que una prueba total de todas las porciones operativas de la empresa. Ello no debe incidir para no realizar una prueba exhaustiva total o parcial ya que el propósito de la prueba de recuperación de desastres es determinar hasta que punto funciona el plan o que partes han de mejorarse.

- La prueba debe tratar de realizar las siguientes tareas:

  - Verificación de que la información del plan de contingencia es compleja y exacta
  - Evaluación del rendimiento y percepción por parte de los miembros que no pertenezcan a la contingencia
  - Evaluación de la coordinación entre el equipo de contingencia y los proveedores y vendedores externos
  - Medición de la habilidad y capacidad de la sede de respaldos para realizar el procesamiento prescrito
  - Evaluación de la capacidad de recuperación de registros

- Evaluación del estado y cantidad del equipo e insumos que se han reubicado en la sede de recuperación
- Medición del rendimiento general de las actividades de operaciones y procesamiento de datos relacionados con mantener la capacidad del negocio

Durante cada fase de prueba, debe llevarse la documentación detallada de las observaciones, problemas y las soluciones. A menudo esta documentación actúa como información histórica importante que puede facilitar la recuperación real en caso de un desastre. Asimismo, la documentación contribuye a realizar un análisis detallado de fortalezas y debilidades del plan.

Deben hacerse revisiones y actualizarse los planes y estrategias de respaldos para desastres de acuerdo con un cronograma para reflejar un reconocimiento continuo de los requerimientos cambiantes. Ello se basa en que:

- Una estrategia que es adecuada en un momento puede no resultar adecuada a medida que cambian las necesidades de la organización.
- Pueden desarrollarse o adquirirse nuevas aplicaciones.
- Los cambios en la estrategia del negocio pueden alterar la importancia de las aplicaciones críticas o hacer que se consideren como críticas aplicaciones adicionales.
- Los cambios al ambiente de software o hardware pueden convertir en obsoletas I inapropiadas las previsiones actuales.

- Minimizar los efectos financieros y operativos cuando se presente el desastre.

Evitar la interrupción de las funciones críticas del negocio manejadas en el computador, tales como producción, que pudieran tener consecuencias muy graves.

Definir las posibles alternativas de proceso que puedan ser empleadas dependiendo de la situación que origine la interrupción.

Proporcionar eficientes medidas de recuperación en el proceso de funciones a través de un plan orientado a restablecer las funciones normales del departamento de sistemas a la mayor brevedad posible para volver al estado que se tenia antes de que ocurriesen las fallas. Por ejemplo, si la falla en un equipo destruye información contenida en una base de datos, deben existir planes para la obtención del último respaldo de dicha base de datos y determinar las transacciones necesarias para actualizar la misma.

La compañía debe asignar a un equipo la responsabilidad de desarrollar un plan de contingencias. Este deberá incluir a personas que conozcan perfectamente la actividad del negocio, asi como expertos técnicos del área de sistemas. Esto con el fin de identificar claramente como la contingencia afecta directamente a los usuarios y por ende las operaciones de la Compañía.

7.2.3.5.8 EJEMPLO DE LO QUE SE DEBE CONSIDERAR PARA DESARROLLAR UN PLAN DE CONTINGENCIAS.

1. Identificar las aplicaciones criticas que se verian más afectadas de acuerdo a diferentes variables (ej. la duración de la contingencia, periodo de presentación del siniestro, etc.)
2. Documentar los requerimientos mínimos de operación de dichas aplicaciones críticas. Estos deben incluir: recursos de hardware y versiones de software necesarios, tiempos de proceso, programas, archivos, espacio de almacenamiento y otros elementos como papeleria.
3. Pruebas periódicas del plan de contingencias (simulacros).
4. Definición de responsabilidades para mantener actualizado el plan.
5. Lista de teléfonos, direcciones y demás datos relativos al personal, proveedores y terceros relacionados con el plan.
6. Procedimientos del plan (actividades a realizar) y responsabilidades del personal implicado.
7. Puntos relativos a los "backups" o respaldos de información (ubicación, acceso y personas autorizadas).
8. Convenios formalizados sobre hardware de respaldo con el proveedor u otras empresas con configuraciones similares de equipo, plasmando los acuerdos tomados

en las cláusulas de dichos convenios. Aún cuando la Compañía sea miembro de alguna organización que pudiera facilitar la obtención de dicho respaldo, tal como la Asociación Mexicana de Usuarios de Sistemas Interactivos de Cómputo (AMUSIC), en la cual se tienen relaciones con otros propietarios con configuraciones de equipo similares, es conveniente formalizar un convenio al respecto.

9. Una vez que el plan ha sido desarrollado, diferentes personas serán asignadas a efectuar pruebas para determinar que tan efectivo es el plan. Es indispensable que este plan se tenga por escrito y conservar una copia del mismo fuera de las instalaciones.
10. Este plan debe estar organizado de tal manera que cada persona pueda obtener la información que necesite sin tener que consultarlo todo por completo. Los empleados de la Compañía deben conocer la existencia de dicho plan y su impacto en las actividades particulares.
11. Es importante llevar a cabo simulacros con el objeto de que cada uno de los responsables, sepa cual es su actividad en el caso de una emergencia.
12. El plan de contingencias debe ser revisado constantemente ya que cualquier cambio en el software, hardware o nuevas aplicaciones deben considerarse en el mismo.

8. ADQUISICIÓN, MANTENIMIENTO Y DESARROLLO

Los controles de desarrollo de sistemas son en general más importantes en los ambientes más grandes de procesamiento, en donde existe mayor actividad de desarrollo y mantenimiento, los sistemas son más complejos y existe menos confianza en el software comprado. El personal de desarrollo de sistemas se caracteriza por ser el responsable de la selección y/o diseño y programación de sistemas de aplicación, conjuntamente con los usuarios de los sistemas.

Estos controles permiten asegurar que los programas de aplicación nuevos y modificados funcionen como lo determina la herencia al controlar el proceso de desarrollo a través del diseño apropiado, especificación y prueba de sistemas nuevos o modificados. El proceso de desarrollo de sistemas se mejora si el cliente tiene auditores internos de sistemas de información que realicen repasos previos a la implantación de los sistemas nuevos o modificaciones significativas a los ya existentes.

Un proceso bien controlado de desarrollo de sistemas incluye:

- Controles de cambios de programa que afectan sistemas de aplicación
- Controles que aseguren que se realicen cambios autorizados en los programas existentes y que estos se desarrollen de manera planeada.

Los controles de cambios de programas nos permiten asegurar que los controles de seguridad y edición continúen siendo efectivos una vez que se realizaron modificaciones en los programas existentes.

La participación de los usuarios en el diseño de sistemas y su aceptación del mismo antes de ponerlo en funcionamiento, permite asegurar que los sistemas operen como se espera.

Una función de seguridad de la calidad, deberá operar de manera independiente del equipo de trabajo y es su responsabilidad asegurar que el trabajo se ha realizado de acuerdo con lo planteado.

Los usuarios y otros grupos tales como auditores internos de sistemas de información pueden evitar los cambios a los sistemas.

Los controles para implantar nuevos sistemas, aseguran que los programas nuevos de sistemas de aplicación realicen las rutinas correcta de edición utilizando archivos de datos correctos.

Las rutinas de verificación de fechas dentro de los programas de sistemas de aplicación permiten asegurar que se apliquen los controles correctos.

Los sistemas de aplicación son aquellos programas que manejan normalmente los usuarios, por ejemplo nómina, cuentas por cobrar, etc.

8.1 CONTROLES.[22]

La relación entre la administración y el control de operaciones con las razones para desarrollar sistemas de información básicamente en dos formas:

1) para mejorar la exactitud y la consistencia y
2) Aumentar la seguridad de los datos más importantes.

- **Prever mejor seguridad**:

Algunas veces el hecho de que los datos puedan ser guardados en una forma adecuada para su lectura por medio de una máquina, proporcionan una seguridad que es difícil de alcanzar en un medio ambiente donde no existen computadoras.

- **Control de la calidad de entrada.**[23]

Existen varias razones que explican por que un buen diseño debe controlar la cantidad de datos en la entrada. Primero, las operaciones de preparación y entrada dependen de las

[22] Análisis y diseño de sistemas de información, James A. Senn, Pag 64

personas. Dado que los de mano de obra son altos, los asociados con la preparación e ingresos de los datos también son altos, los asociados con la preparación e ingreso de datos también son altos. Disminuir los requerimientos de datos puede reducir los costos y ocurrir lo mismo con los costos de mano de obra. Segundo, la fase de entrada puede ser un proceso lento que toma mucho más tiempo que le que necesitan las computadoras para llevar a cabo sus tareas. De hecho, la computadora quizá permanezca sin hacer nada durante el tiempo que se preparan los datos y la entrada para su procesamiento. Al disminuir los requerimientos de la entrada para su procesamiento. Al disminuir los requerimientos de la entrada, el analista puede acelerar todo el proceso desde la captura de datos hasta que los resultados llegan a manos de los usuarios.

- **Evitar los retrasos.**

Un retraso en el procesamiento que es resultado de las operaciones de preparación o de entrada de datos, recibe el nombre de cuello de botella. Evitar los cuellos de botella debe ser siempre uno de los objetivos que l analista persiga al diseñar la entrada, tal como se discutió en el proyecto de la historia con que inicia este capitulo.

- **Evitar los errores de los datos.**

El tercer objetivo está relacionado con los errores. En cierto sentido la tasa de errores depende de la cantidad de datos, ya que entre más pequeña sea ésta menores serán las oportunidades para cometer errores. Es común encontrar en las operaciones de venta al por menor una tasa promedio del 3% de error en las operaciones de entrada de datos. Si el volumen de datos es de 10,000 transacciones por semana, entonces se presentarán aproximadamente 300 errores. A pesar de lo anterior, el analista puede reducir el número de errores al disminuir el volumen de datos que deben ingresarse por cada transacción.
El analista también puede modificar las tasas de error de una operación a través de diseño de la entrada, ya que la forma en que se deben ingresar los datos puede tener efectos sobre la incidencia de los errores.

[23] Análisis y diseño de sistemas de información, James A. Senn, Pag 478.

Otros aspectos del control de errores es la necesidad de detectarlos cuando éstos se presentan. Las verificaciones y balances en los programas para entradas de datos, denominadas técnicas de validación de entradas, también descubren errores en la entrada.

- **Evitar los pasos adicionales.**[24]

Algunas veces el volumen de transacciones y la cantidad de datos en preparación, o el trabajo de entrada de datos , es algo que no se puede controlar. Cuando no es posible reducir el volumen de transacciones, el analista debe asegurar que el proceso sea lo más eficiente posible. El analista experimentado también evitará diseños para la entrada que traigan como consecuencia una mayor cantidad de pasos a seguir. El efecto que trae consigo ya sea añadir o quitar un paso cuando se alimentan los cheques al proceso bancario, será multiplicado muchas veces en el transcurso de un día de trabajo.

- **Mantener la sencillez del proceso.**

Quizá el mejor consejo para los analistas es alcanzar todos los objetivos. Claro esta que al incluir tantos controles sobre los errores las personas puedan tener dificultades al emplear el sistema. En otras palabras, el control de los errores puede obstruir la tarea. El sistema mejor diseñado se ajusta a las personas que lo utilizarán y al mismo tiempo, proporcionarán métodos para el control de los errores. La simplicidad funciona y es aceptada por los usuarios. En contraste, cuesta trabajo que los usuarios acepten diseños para la entrada que sean complejos o confusos, y no existe ninguna garantía para el éxito al instalar un sistema complejo. En consecuencia, es aconsejable evitar la complejidad cuando hay opciones más sencillas.

[24] Análisis y diseño de sistemas de información, James A. Senn, Pag 479.

8.1.1 IDENTIFICACION DE CONTROLES.[25]

En situaciones donde se ejerce buen control ya sea por parte de la gerencia o por el seguimiento del proceso, quizá no sea problema determinar si una actividad se ha llevado a cabo en forma adecuada.

Aun así, los analistas deben examinar los métodos de control durante la etapa de análisis: Existen estándares específicos de desempeño?, Quién se encarga de comparar el desempeño contra los estándares? Cómo se detectan los errores? Cómo se corrigen los errores. Se cometen demasiados errores?. La falta o debilidad de los controles es un descubrimiento importantes en cualquier investigación de sistemas. Elaborar un diagrama de flujo de proceso total puesto que da mayor referencia de todo el sistema y de su operación.

8.1.2 VERIFICACION DE LOS DATOS DE TRANSACCION.

Aun las transacciones válidas pueden contener datos que no lo son. Por consiguiente, los analistas deben asegurarse de especificar métodos para validar los datos cuando desarrollan los procedimientos de entrada. Existen cuatro métodos para validar los datos.

- **Pruebas de existencia.**

Algunos de los campos de datos de las transacciones son diseñados para no dejarlos vacíos o en blanco. Las pruebas de existencia examinan los campos esenciales para determinar que éstos contengan datos. Por ejemplo, en los procesamientos de inventario, no es correcto aceptar pedidos que no especifiquen la cantidad solicitada de determinado artículo.

[25] Análisis y diseño de sistemas de información, James A. Senn, Pag 129.

- **Pruebas de límites y rangos**

Estas pruebas verifican la veracidad de los datos de una transacción. Las pruebas de límites sirven para validar la cantidad mínima o máxima aceptable para un dato. Las pruebas de rango validan tanto los valores mínimos como máximos.

- **Pruebas de combinación.** [26]

Las pruebas de combinación validan el hecho de que varios datos tengan al mismo tiempo valores aceptables; en otras palabras, el valor de un campo determina si son correctos los valores de los demás datos.

- **Procesamiento duplicado.**

En áreas especialmente impotentes, quizá sea necesario procesar los datos más de una vez, ya sea en un equipo deferente o en una forma distinta. Después de dicho procesamiento, los resultados se comparan para determinar su consistencia y exactitud. El proceso duplicado asegura la mayor exactitud.

- **Corrección automática.**[27]

Algunas veces los analistas especifican la realización de programas para corregir errores en los datos. Este método para validar los datos se emplea con el fin de reducir el número de pasos necesarios para corregir errores o rechazos de transacciones durante el procesamiento. Este método sólo requiere que el programa detecte un error y efectúe ña corrección en forma automática.

- **Dígitos de verificación**

Dos de los errores más comunes en el manejo de datos se presentan cuando los datos son capturados en forma incorrecta, estos errores de conocen como errores de

[26] Análisis y diseño de sistemas de información, James A. Senn, Pag 503.

transcripción. Otro tipo común de error de transposición, es el cambio deposición de dos o más dígitos, lo que trae como resultado que el dato sea incorrecto.

Dado que la posibilidad de que estos errores se presenten es muy alta, se ha diseñado un método especial para ayudar a detectarlos durante el procesamiento por computadora. Este método denominado dígito de verificación, añade un dígito más al dato que será utilizado con fines de identificación. El dígito de verificación se añade al número original antes que se haga uso de éste. En otras palabras para utilizar dígitos de verificación con los números de cliente, se calcula el dígito y se suma al número de cliente, con lo que se obtiene un número de cinco dígitos, antes que sea asignado a cualquier cliente. En realidad, es necesario advertir a los usuarios del número sobre la inclusión del dígito de verificación.

Están disponibles los siguientes perfiles de controles, para ayudar a obtener una mejor comprensión de los controles para la adquisición, desarrollo y mantenimiento de sistemas:

- Prueba de la factibilidad de un proyecto
- Modificación al sistema
- Involucración del usuario
- Prioridades
- Especificación del Diseño
- Programación
- Pruebas
- Documentación
- Implantación y evaluación
- Mantenimiento
- Liberación

[27] Análisis y diseño de sistemas de información, James A. Senn, Pag 504.

8. 2 SOLICITUD POR PARTE DEL USUARIO

Recibir una solicitud formal y por escrito de servicios del área de sistemas donde se indique:

- Nombre y autorización del solicitante.
- Relación con otras aplicaciones y procesamiento electrónico y/o manuales.
- Requerimientos del usuario, incluyendo aspectos de negocios, operaciones y de control.
- Evaluar la solicitud (tanto técnica como financieramente).
- Conocer cuales son las necesidades de información y como se cumple con ellas, definir el sistema, analizar sus características, encontrar las deficiencias y aportar sugerencias.
- Realizar entrevistas con el usuario solicitante para determinar los volúmenes de información que se manejarán con base en las necesidades y también para establecer prioridades.
- Elaborar un calendario de actividades tomando en cuenta el tipo de equipo con que se cuenta, el tiempo, el personal, los limites de responsabilidad, y cómo se trabajarán los procesos, así como establecer fechas tentativas de iniciación y terminación.

8.3 PRUEBA DE LA FACTIBILIDAD DE UN PROYECTO.[28]

Las investigaciones preliminares examinan la factibilidad del proyecto, la posibilidad de que el sistema sea de utilidad para la organización. Se estudian tres pruebas de factibilidad, todas ellas importantes: operacional, técnica y financiera.

- **Factibilidad operacional:**

  - Los proyectos propuestos únicamente tienen beneficios cuando logran ingresar al grupo de sistemas de información que satisfacen los requerimientos de la organización. En otras palabras ,esta prueba de factibilidad formula la siguiente pregunta:

[28] Análisis y diseño de sistemas de información, James A. Senn, Pag 89.

- Trabajará el sistema cuando esté terminado e instalado?
- Existen barreras importantes para la implantación?
- Existe apoyo suficiente para el proyecto por parte de la administración?
- Los métodos que actualmente se emplean en la empresa son aceptados por los usuarios
- Los usuarios han participado en la planeación y desarrollo del proyecto?
- El sistema propuesto causara prejuicios? Producirá resultados pobres en algún aspecto o área? Se perderá el control en alguna área? Se perderá la facilidad de acceso a la información.

- **Factibilidad Técnica.**[29]

- Entre los aspectos técnicos que es común que aparezcan durante la etapa de factibilidad de la investigación, se incluye los siguiente:
- Existe o puede adquirir la tecnologia necesaria para realizar lo que se pide?
- El equipo propuesto tiene la capacidad técnica para soportar todos los datos requeridos para usar el nuevo sistema
- El sistema propuesto ofrecerá respuestas adecuadas a las peticiones in importar el número y ubicación de los usuarios
- Si se desarrolla el sistema, puede crecer con facilidad
- Existen garantías técnicas de exactitud, confiabilidad , facilidad de acceso y seguridad de los datos.

- **Factibilidad financiera y económica.**[30]

Un sistema puede ser desarrollado desde un punto de vista técnico y que, además será utilizado se llega a instalar, debe ser una buena inversión para la organización. Los beneficios financieros deben igualar o exceder a los costos. Las cuestiones económicas y financieras formuladas por los analistas durante la investigación preliminar, tienen el propósito de estimar lo siguiente:

[29] Análisis y diseño de sistemas de información, James A. Senn, Pag 90.
[30] Análisis y diseño de sistemas de información, James A. Senn, Pag 90.

- El costo de llevar a cabo la investigación completa de sistemas.
- El costo del hardware y software para la aplicación que se está considerando.
- Beneficios en la forma de reducción de los costos o de menos errores costosos.
- El costo si nada sucede (es decir si el proyectos no se lleva a cabo.)

8.4 ESPECIFICACIÓN DEL DISEÑO.[31]

Los dos objetivos operacionales de diseño que siempre buscan las personas que los desarrollan son la confiabilidad y la factibilidad de mantenimiento de sistema. Esta sección centra su atención en la importancia de estos objetivos y los medios para alcanzarlos.

- **Diseño de sistemas confiables.**

Se dice que un sistema tiene confiabilidad si no produce fallas costosas o peligrosas al usarse de manera razonable, es decir, de tal forma que un usuario tipico espera que sea normal. Esta definición reconoce que los sistemas no siempre se utilizan en la manera en que los diseñadores lo esperan. Existen cambios en las formas en que los usuarios usan el sistema y también en las operaciones de la empresa. Sin embargo, hay ciertos pasos que los analistas deben dar para garantizar que el sistema sea confiable cuando se lo instala y que la confiabilidad se puede mantener después de la implantación.

- **Enfoques de la confiabilidad.**

Hay dos niveles de confiabilidad. El primero es en el que el sistema cumpla con los requerimientos correctos. Por ejemplo, se espera que un sistema tenga caracteristicas o controles específicos de seguridad, construidos dentro de él a petición de los usuarios. Pero si el diseño no los especifica y permite la pérdida de fondos o mercancia durante mucho tiempo antes de que alguien detecte el problema, el sistema no es confiable. La confiabilidad a nivel diseño es posible sólo si el analista lleva a cabo una determinación

[31] Análisis y diseño de sistemas de información, James A. Senn, Pag 765.

cabal y efectiva de los requerimientos de los sistemas. Se necesita un estudio cuidadoso y completo del sistema para satisfacer ese aspecto de confiabilidad.

El segundo nivel de confiabilidad del sistema tiene que ver con los resultados reales que le sistema entrega al usuario. En este nivel, la confiabilidad del sistema se entrelaza con la ingeniería del software y su desarrollo.

- **Prevención de errores.**[32]

Hay tres enfoques para la confiabilidad. Con la prevención de errores, los desarrollados y programadores hacen todos los intentos por evitar que los errores ocurran. El propósito de los métodos y técnicas estructurados es poner énfasis en la identificación temprana y cuidadosa de los requerimientos del usuario.
Los analistas deben considerar que es imposible alcanzar por completo este objetivo. Los errores pueden ocurrir no obstante los mejores esfuerzos de gente muy competente.

- **Detención y corrección de errores.**

Este método se usa características del diseño que detectan errores y hacen los cambios necesarios para corregir ya sea el error, mientras el programa éste en uso, o el efecto sobre el usuario, de tal forma que no ocurra una falla. La detección de los errores del usuario, tal como un mal deletreo de los términos importantes o la introducción de comandos inválidos.

- **Previsiones de auditoria y confiabilidad.**[33]

A menudo, los usuarios tienen una tendencia a confiar en los sistemas más de lo que debieran al extremo de que con frecuencia creen en los resultados producidos por un sistema de información basado en una computadora sin el escepticismo suficiente. Por lo tanto, la necesidad de asegurarse de incluir los controles adecuados en el sistema es un paso esencial en la selección de software. Los auditores deben tener la capacidad de

[32] Análisis y diseño de sistemas de información, James A. Senn, Pag 776.

validar los reportes y salidas y probar la autenticidad y precisión de los datos e información.

Entre los procedimientos de auditoría y control que son los intereses están los siguientes:

- Rastrear una transacción por cada paso del proceso y tener la capacidad de examinar los valores de datos intermedios producidos durante el procesamiento.
- Imprimir registros y transacciones seleccionados del sistema que cumplan ciertos criterios para validar la precisión y autenticidad tanto de las transacciones como de los resultados.
- Mantener un balance constante en el sistema cuando éste implique cuestiones financieras y reportar si el sistema está balanceado.
- Producir un diario detallado de todas las transacciones y el efecto de éstas en los saldos de las cuentas o en los registros del archivo maestro.
- Proporcionar los controles suficientes en la entrada, tales como controles y cuenta de los lotes y transacciones.

La confiabilidad de un sistema quiere decir que los datos son confiables, que son preciso y creíbles. También incluye el elemento de seguridad, el que evalúa el analista determinado el método y adecuación de protección del sistema contra el uso no autorizado. El hecho de que el sistema tenga contraseñas no es una protección suficiente del acceso. A menudo se requieren niveles múltiples de contraseñas para permitir a los distintos miembros del equipo de acceso a los archivos y bases de datos o funciones que necesiten. Puesto que no todas las personas requieren el mismo nivel de acceso, muchos sistemas de seguridad utilizan niveles múltiples de contraseñas que controlan el nivel de entrada en el sistema y permite a un individuo: preparar informes que la persona está autorizada a recibir, presentar datos de transacción para su procesamiento, cambiar saldos de cuenta o corregir datos de archivos, o bien cambiar los parámetros o contraseñas de seguridad actuales.

[11] Análisis y diseño de sistemas de información, James A. Senn, Pag 922.

Las características de seguridad técnica no son adecuadas se las contraseñas o los demás métodos de seguridad se muestran siempre que se usen.

En la actualidad, para muchas organizaciones, los sistemas de información basados en computadoras son el corazón de las actividades cotidianas y objeto de gran consideración en la toda de decisiones.

Las empresas consideran con mucho cuidado las capacidades de sus sistemas de información cuando deciden ingresar o no en nuevos mercados o cuando planean la respuesta que darán a la competencia. Sin ayuda automatizada, las dependencias gubernamentales tendrían que hacer un alto ante el volumen de trabajo que abrumaría a sus administraciones y empleados.

En éste hay que considerar lo siguiente:

- La organización del proyecto (quién lo hará, responsabilidades, plan de trabajo, asignación de trabajo etc.).
- Identificación de especificaciones personales y técnicas, conocer las necesidades detalladas a través de entrevistas, análisis de funciones del personal, etc.
- Conocimiento del sistema actual, analizando las funciones del personal, quienes tienen acceso a la información, procedimientos de seguridad, control de entradas y salidas, pantallas, formas y reportes, identificación de los puntos que requieren mayor control, análisis de la arquitectura técnica, etc.
- Elaborar diagramas de flujo y de bloque.

Comprende lo siguiente:

- El diseño detallado del sistema, que consiste en complementar el diseño técnico, identificar las unidades de programación, elaborar la narrativa del programa, realizar ciclos de programación o de prueba en áreas lógicas, y revisar en conjunto las partes del programa.
- Programación con base en los estándares fijados, codificación, compilación, prueba individual del programa y prueba global del sistema en áreas lógicas o

ambientes de prueba, conversión del sistema anterior al nuevo, identificando los datos que se manejarán.

- Instalar un sistema o varios a la vez a través de instalaciones piloto o sistemas paralelos.
- Echar a andar el sistema alimentándolo con datos reales y que el usuario los verifiqué contra los datos obtenidos manualmente para ver si funciona adecuadamente el sistema.
- Desarrollar material de consulta como manuales de operación, técnicos y del usuario
- Dar seguimiento al sistema para corregir cualquier posible error o implementar alguna corrección que lo mejore. Este tipo de actividades se deben llevar a cabo en áreas de memoria destinadas a pruebas, de manera que los programas "originales" no se vean afectados sino hasta que las modificaciones hechas han sido probadas suficientemente.

Este punto es sumamente importante en el proceso de correcciones a las bibliotecas de producción. Debe existir un procedimiento formal tanto para que toda corrección se haga un en ambiente de prueba como para que antes de liberar cualquier modificación o desarrollo se lleve a cabo una prueba en paralelo. Esto con el objeto de verificar el adecuado funcionamiento de los mismos y no provocar posibles problemas difíciles de resolver, pues la información real ya está en juego.

8.5 EJEMPLO DE REVISIÓN

8.5.1 Modificaciones de los sistemas o sistemas nuevos

1. ¿Hay rutinas y procedimientos establecidos para desarrollo de especificaciones para soportar el diseño de modificaciones de sistemas o sistemas nuevos?

   Si es así, describa los controles diseñados para asegurar que:

   - La información fuente (de entrada) y el medio de entrada de dicha información al sistema está identificado

- Las modificaciones se sujetan a normas de programación aplicables.
- Estén especificados el formato, medio y distribución de los informes.
- Estén identificados los pasos del procesamiento y la lógica
- Estén adecuadamente especificados los ambientes del hardware y el sistema de software
- Están adecuadamente dirigidos los requerimientos de seguridad de información
- Estén incorporados en el diseño del sistema los controles internos tanto programados como del usuario. Tales controles pueden incluir los totales por lote, la ediciones de entrada y las rutinas de verificación y los reportes clave de control.

Riesgos:

Si las especificaciones son inadecuadas, las transacciones procesadas por los sistemas adquiridos, desarrollados o modificados sin las especificaciones adecuadas, no procesaran información confiable.

Si las especificaciones se desarrollan sin la participación apropiada de varios representantes de procesamiento de datos, el sistema pudiera no haberse diseñado o programado de manera consistente con las actividades y procedimientos de cada uno de estos grupos y ciertas características deseadas del sistema pudieran no ser posibles ni prácticas de implantar.

Si las especificaciones son inadecuadas, las transacciones procesadas por el sistema pudieran no procesarse confiablemente.

Al no contar con una metodología de desarrollo es posible liberar sistemas nuevos o modificaciones que no cumplan con las necesidades y requerimientos del usuario, además en el caso de que personal de informática deje de laborar para la compañía se incurrirá en excesos de tiempo por el personal de nuevo ingreso para analizar y conocer el diseño y estructuras de los sistemas.

Incorrecto o inexacto proceso de datos, que sean detectados después de que se libere el sistema (por ejemplo: cálculos equivocados, errores de lógica, e inconsistencias internas), desbordamiento de campos, truncamientos de información, etc.

Falta de adecuados y suficientes reportes de validación, de cifras de control, los cuales proporcionarán al usuario suficientes datos para llevar a cabo una verificación de la exactitud del proceso, así como el que éste haya sido adecuado.

Reducción de la eficiencia de operación (tanto del computador como del personal usuario).

No adecuación del proyecto a la solicitud inicial del usuario.

Complicaciones para el futuro mantenimiento del sistema, lo cual implicaría que estos costos sean mayores.

Falta de consideración de elementos de seguridad y control adecuados.

Controles:

Con procedimientos de prueba suficientes que involucren a los usuarios, se pueden reducir el riesgo de error que se origina de la participación insuficiente de los usuarios en la especificación del diseño del sistema.

Establecer una metodología de desarrollo y modificación de sistemas que se apegue a las necesidades actuales de la empresa, incluyendo entre otros puntos la intervención del usuario en el proceso de definir en forma clara sus necesidades, la elaboración de la documentación de los sistemas que sirva como herramienta y apoyo en el funcionamiento del sistema y procedimientos de liberación de sistemas en donde participe el usuario y personal de sistemas.

Se deben de diseñar procedimientos de desarrollo y modificación de sistemas que proporcionen una estandarización de actividades a seguir.

8.5.2 Involucración del usuario

2. ¿Hay rutinas y procedimientos establecidos para la Involucración del usuario en la selección, diseño o modificación de los sistemas?

   Si así es, describa los controles diseñados para asegurar que:

   - Se les pide a los usuarios que describan las características o cambios que necesitan
   - Los usuarios o un Comité Directivo de sistemas que incluye representantes de los usuarios, revisan las especificaciones

   Riesgos:

   Si no, los sistemas no se podrían haber desarrollado de acuerdo con los requerimientos de los usuarios. En consecuencia, los sistemas podrían no funcionar adecuadamente. La participación del usuario en los procedimientos adecuados de prueba, puede reducir el riesgo de errores, debido a la participación inadecuada de los usuarios en la especificación del diseño del sistema.

8.5.3 Prioridades

3. ¿Hay rutinas y procedimientos establecidos para la asignación de prioridades para el desarrollo de sistemas y mantenimiento de proyectos?
   - Si así es, describa los controles diseñados para asegurar que:
   - Se da prioridad de manera consistente con la estrategia de los sistemas de información del cliente. A los cambios críticos se les da alta prioridad
   - Los cambios a los sistemas se hacen en orden correcto
   - Los cambios en las prioridades y en los programas se comunican a los usuarios

Riesgo:

Si no, el cliente podría no hacer los cambios necesarios a los sistemas en el orden correcto. Por ejemplo, los cambios a un sistema de facturación se tienen que hacer antes de cambiar el sistema de cuentas por cobrar para prevenir errores en los sistemas.

Retrasos en desarrollos y modificaciones importantes, pérdida de tiempo y oportunidad al usuario.

Controles:

Diseñar métodos y procedimientos que determinen la prioridad que debe de tener un desarrollo o una modificación en diversos casos.

8.5.4 Especificación de Diseño

4. ¿Hay rutinas y procedimientos establecidos para la revisión de las especificaciones de diseño, por parte del personal adecuado de procesamiento de datos independientemente del área de desarrollo y mantenimiento de sistemas (v.g., Operaciones, Seguridad y Apoyo a los Sistemas de Información)?
   ¿Existen estándares escritos de programación y desarrollo que estipulen la estructura de programas, la forma de constituir nombres significativos de variables, de archivos y de campos?

   Si así es, describa los controles diseñados para asegurar que el efecto de un sistema modificado o nuevo está considerado en las actividades de cada uno de estos grupos y que el diseño es adecuado.

Riesgo:

Si el desarrollo no se supervisa, los programas pudieran no satisfacer las especificaciones de diseño establecidas o pudieran hacerse modificaciones no autorizadas a los sistemas de aplicación.

8.5.5 Comité de Coordinación

5. En el desarrollo de nuevas aplicaciones o cambios substanciales en aplicaciones existentes, ¿se forman comités de coordinación integrados por el personal del departamento usuario y del departamento de sistemas, donde se revisan y aprueban los objetivos y el avance de los desarrollos?

8.5.6 Programación

6. ¿Elabora internamente el cliente sistemas de aplicación o modificaciones a los proyectos?

   Si así es, describa los controles diseñados para asegurar que:

   - Los programas se desarrollan de manera consistente de acuerdo con las normas de programación o otros lineamientos que el cliente aplica.
   - Los códigos nuevos o modificados son revisados por los supervisores de programación (v.g. Analistas, Líderes de Proyecto).
   - Los sistemas nuevos o modificados no se aplican antes de ser autorizados y probados para su implantación.
   - Si los controles sobre desarrollo interno no se dirigen hacia los puntos anteriores, podrían usarse programas no autorizados o inexactos o puede resultar difícil mantener los sistemas, obteniendo como resultado errores en el procesamiento e información incorrecta y engañosa.

Riesgo:

Si no se siguen las normas y guías de programación, el mantenimiento futuro del sistema pudiera ser más difícil.

Si no, el sistema podría no estar diseñado o programado de una manera consistente con las actividades y procedimientos de cada uno de estos otros grupos, y podrá no ser posible o práctico implantar ciertas características deseadas del sistema.

8.5.7 Pruebas

PRUEBAS DE LOS SISTEMAS .[34]

Durante la fase de prueba de sistemas, el sistema se emplea de manera experimental para asegurarse de que el software no tenga fallas, es decir que funciona de acuerdo con las especificaciones y en la forma en que los usuarios esperan que lo haga. Se alimentan como entradas conjunto de datos de prueba para su procesamiento y después se examinan los resultados. En ocasiones se permite que varios usuarios utilicen el sistema para que los analistas observen si tratan de emplearlo en formas no previstas. Es preferible descubrir cualquier sorpresa antes de que la organización implante el sistema y dependa de él.

En muchas organizaciones, las pruebas son conducidas por personas ajenas al grupo que escribió los programas originales; con esto se persigue asegurar, por una parte, que las pruebas sean completas e imparciales y , por otra, que el software sea más confiable.

7. ¿Hay rutinas y procedimientos establecidos para probar aplicaciones financieras nuevas o significativamente modificadas?
   Si así es, describa los controles diseñados para asegurar que:

[34] Análisis y diseño de sistemas de información, James A. Senn, Pag 37.

- Las pruebas incluyen algunos o todos los siguientes puntos, según cada caso:
- Se hacen pruebas de la lógica de los programas
- Se hacen pruebas de los procedimientos de entrada del usuario
- Se hacen pruebas de la conexiones con otros sistemas
- Si es adecuado, se hacen pruebas en paralelo con el sistema que se reemplaza.
- Se hacen pruebas de los controles y de los dispositivos de seguridad
- Las pruebas se realizan usando información de prueba en vez de información final.
- Se terminan y analizan las pruebas antes de usar sistemas nuevos o modificados.
- Los usuarios revisan los resultados de las pruebas y "aceptan" el sistema antes de Implantarlo

Riesgos:

Si no, se podrían implantar sistemas nuevos o modificados que contienen errores y causar resultados no confiables del procesamiento o la pérdida o alteración de la información.

Los sistemas nuevos o modificados que contienen errores pueden ser puestos en producción,, originando resultados de procesamiento no confiables a la pérdida o alteración de datos. Si no se prueba el software comprado su lógica de procesamiento y los métodos

8.5.8 Documentación

El departamento de sistemas es responsable de la elaboración de manuales técnicos o de operación y de usuario en el desarrollo de sistemas, con el objeto de que tanto usuarios como analistas y operadores puedan consultar las dudas que se les presenten.

El manual del usuario, es un documento que contiene los pasos a seguir en el manejo de un sistema, el significado de cada pantalla y reportes, ejemplos de mensajes, correcciones y controles del sistema, etc.

El manual técnico es para uso del personal de desarrollo y mantenimiento y de la gerencia del departamento. de sistemas y contiene flujogramas, la programación del sistema en el lenguaje utilizado, etc.

El manual de operación indica los pasos que el operador deberá seguir en la realización de cada una de sus funciones.

En general, se deben seguir los lineamientos de la metodología, estableciendo los controles y niveles de autorización necesarios para asegurar su cumplimiento, es indispensable en este proceso contar con las formas necesarias tanto para las solicitudes de usuarios, como para las transferencias de bibliotecas de producción a prueba. Estas formas deberán ser aprobadas por las personas responsables en cada área.

También se recomienda que existan formas para la liberación de los desarrollos o mantenimientos hechos, una vez que una prueba en paralelo se haya realizado.

8. ¿Mantiene el cliente documentación de todas las aplicaciones contables importantes, que cumple debidamente con las necesidades tanto del usuario como del personal de procesamiento de datos?

   Si así es, describa los controles diseñados para asegurar que:

   - La documentación es actual y refleja con exactitud el sistema tal como opera (manual de operador)
   - La documentación es lo suficientemente detallada para soportar cambios futuros al sistema (flujograma del sistema, formatos de registros e informes, código fuente, formulario para cambios del programa).
   - Las instrucciones del usuario y del operador son lo suficientemente detalladas para lograr el uso y operación adecuados del sistema (manual de usuario).
   - La documentación sensible se guarda fisicamente en un lugar seguro.
   - Incluye la documentación para cada aplicación lo siguiente:
     * Nombre de la aplicación.
     * Instrucciones para operadores y usuarios.

* Frecuencia de ejecución.
* Identificación de archivos de entrada y salida.
* Identificación de todos los informes de salida.

En la obtención de una mejor comprensión de la documentación de los controles antes mencionados, considere lo siguiente:

* Los tipos de usuario que necesitan documentación y la información relevante para ellos.
* Los pasos del procesamiento y la lógica
* Los puntos importantes de control.

Riesgos:

Si no existe documentación, es obsoleta o inadecuada, podrían ocurrir errores en la operación del sistema o en las futuras modificaciones al mismo.
La falta de documentación actualizada puede ocasionar errores de procedimiento por parte del usuario debido a la falta de conocimiento del sistema. En caso de que haya personal de nuevo ingreso en el departamento se incurrirían en excesos de tiempo para efectuar la capacitación de dicho personal.

Si la documentación no existe, es inadecuada o incompleta, los errores pueden ocurrir al operar o usar el sistema o al hacer modificaciones futuras del sistema.

Controles:

Diseñar manuales de usuario que contengan una descripción adecuada de diseño, desarrollo, y de los flujos de información de los procesos.

8.5.9 Implantación y evaluación.[35]

La implantación es el proceso de verificar e instalar nuevo equipo, entrenar a los usuarios, instalar la aplicación y construir todos los archivos de datos necesarios para utilizarla. Dependiendo del tamaño de la organización que empleará la aplicación y el riesgo asociado con su solo, puede elegirse comenzar la operación del sistema sólo en un área de la empresa (prueba piloto), por ejemplo en un departamento o con una persona o dos personas. Algunas veces se deja que los dos sistemas, el viejo y el nuevo, trabajen en forma paralela con la finalidad de comparar los resultados. En otras circunstancias, el viejo sistema deja de utilizarse determinado día para comenzar a emplear el nuevo día siguiente. Cada estrategia de implantación tiene sus méritos de acuerdo con la situación que se considere dentro de la empresa. Sin importar cuál sea la estrategia utilizada, los encargados de desarrollar el sistema procuran que el uso inicial del sistema se encuentre libre de problemas.

Una vez instaladas, las aplicaciones se emplean durante muchos años. Sin embargo las organizaciones y los usuarios cambian con el paso del tiempo, incluso el ambiente es diferente con el paso de las semanas y los meses. Por consiguiente, es indudable que debe darse mantenimiento a las aplicaciones; realizar cambios y modificaciones en el software.

8.5.9.1 Evaluación de un sistema.

La evaluación de un sistema se lleva a cabo para identificar puntos débiles y fuertes. La evaluación ocurre a lo largo de cualquiera de las siguientes dimensiones:

a) Evaluación operacional:

   Valoración de la forma en que funciona el sistema, incluyendo su facilidad de uso, tiempo de respuesta, lo adecuado de los formatos de información, confiabilidad global y nivel de utilización.

[35] Análisis y diseño de sistemas de información. James A. Senn, Pag 37.

b) Impacto organizacional:

Identificación y decisión de los beneficios para la organización en áreas tales como finanzas (costos, ingresos y ganancias), eficiencia operacional e impacto competitivo. También se incluye el impacto sobre el flujo de información interno y externo.

c) Opinión de los administradores

Evaluación de las actitudes de directivos y administradores dentro de la organización así como de los usuarios finales.

d) Desempeño del Desarrollo

La evaluación del proceso de desarrollo de acuerdo con criterios tales como tiempo y esfuerzo de desarrollo, concuerdan con presupuestos y estándares, y otros criterios de administración de proyectos. También incluye la valoración de los métodos y herramientas utilizados en el desarrollo.

Desafortunadamente la evaluación de los sistemas no siempre recibe la atención que merece. Sin embargo, cuando se conduce en forma adecuada proporciona mucha información que puede ayudar a mejorar la efectividad de los esfuerzo a de desarrollo de aplicaciones subsecuentes.

8.5.10 Mantenimiento

Este se refiere a cualquier modificación que se haga a los sistemas que ya se encuentran trabajando. Estas modificaciones pueden ser desde muy simples hasta cambios radicales en los sistemas. Para ello es indispensable seguir la misma metodología que ya hemos descrito para los desarrollos de sistemas.

Asimismo es importante señalar que debe existir una comunicación entre la gerencia de sistemas y el usuario en el desarrollo y mantenimiento de aplicaciones para conocer en forma más detallada sus necesidades de información.

El departamento de sistemas es responsable de desarrollar un entrenamiento con el usuario para darle confianza y enseñarlo a conocer y manejar el sistema, así como de la elaboración de manuales de consulta para resolver posibles dudas.

10. ¿Elabora el cliente internamente proyectos de mantenimiento para los sistemas de aplicación?

Si así es, describa los controles diseñados para asegurar que:

* Las peticiones para cambios a los programas se documenten y autoricen tanto por el usuario como por la gerencia de procesamiento de datos
* Los cambios a los programas de mantenimiento a los programas, estén sujetos en lo aplicable a las normas estándar de programación
* El mantenimiento lo lleve a cabo el personal adecuado (programadores vs. usuarios o analistas)
* Los usuarios revisen los resultados de las pruebas y "acepten" el sistema modificado antes de implantarlo.
* La documentación esté debidamente actualizada para reflejar el sistema revisado.

Riesgo:

Si las modificaciones a las aplicaciones existentes no se controlan adecuadamente, existe el riesgo de que tales aplicaciones no procesen en forma confiable. El riesgo de las modificaciones inexactas o inapropiadas aumenta con la antigüedad de la aplicación y la complejidad del cambio que se hizo.

8.5.11 Liberación

11. ¿Existen procedimientos para asegurar que los sistemas se desarrollen, prueben, aprueben e implementen en forma adecuada?

Riesgos:

Que se liberen modificaciones o nuevas aplicaciones que no cumplen con las expectativas del usuario o del departamento de sistemas.

Al momento de la liberación de no hacerlo una persona especificamente autorizada puede ocurrir alteración o pérdida de la información de producción.

Control:

Implementar políticas y procedimientos que garanticen la adecuada realización de los procesos de prueba y liberación.

Levantar una pequeña acta o minuta donde deberán firmar todos los involucrados "de conformidad" a fin de que todos compartan la responsabilidad en el diseño y uso de los sistemas.

También deberán firmar los documentos fuente y los informes y reportes de salida.

CONCLUSION

Día con día las organizaciones se hacen más dependientes de la información esto conlleva a que la administración de la información se convierta en una pieza clave de competitividad entre las empresas.

Dado el grado de los avances tecnológicos, dependencia de los sistemas de información, la complejidad de los procesos, volumen y almacenamiento de información, surge la necesidad de la creación de sistemas de información eficientes y eficaces. Esto implica un gran reto en las organizaciones ya que es necesario implementar controles, ya que el descuido sobre algún de ellos puede llegar a atentar contra la integridad de la operación de la empresa.

Ante esta situación surge la necesidad de auditar los sistemas de información y específicamente implementar los controles adecuados para poder contar con información confiable para la toma de decisiones.

La presente tesis muestra una opción para llevar a cabo la adecuada revisión de los controles generales.

Los puntos más importantes de cada control son:

Conocimiento del negocio

Con el propósito de comprender el grado de automatización de la compañía se necesitará la siguiente documentación:

Inventario de pc's y software,
Basándose en el inventario, verificar el lugar físico en donde se guardan las licencias y si se cuenta con un control de su custodia.

Organización

La efectividad de los procedimientos y controles del departamento de sistemas de información dependen en gran medida del grado en que la gerencia defina y supervise su organización y operaciones. Debido a la concentración de datos y funciones de procesamiento en este Departamento, se debe mantener una organización y definición de responsabilidades en la que se dé una adecuada segregación de funciones incompatibles.

Descripción de puestos,
Verificar aleatoriamente las descripciones de puestos en donde se verificará el nombre del ocupante, puesto, actividades, firma de conocimiento del documento por parte del usuario.

Operación

Se constituye por las tareas realizadas por los operadores del equipo, como ejecución de procesos especiales (como actualización de archivos), montaje de cintas, respuesta a mensajes de la consola, procedimientos de reinicio y recuperación después de alguna caída del sistema, impresión de reportes, liberación de aplicaciones, etc.

Bitácoras de Operación
Aleatoriamente escoger algunas bitácoras con el fin de verificar que estas se encuentren debidamente llenadas y verificadas, ver el orden consecutivo de la fecha, hora de operación, si las anotaciones están completas y legibles, si se cuenta con la revisión de estas.
Plan de contingencias y contratos de respaldo de hardware
Verificar si se han realizado pruebas al plan de contingencia y si se cuenta con documentación de estas, además verificar si el personal del área conoce los procedimientos a seguir en una contingencia.
Políticas de backup's
Verificar de forma aleatoria algunos respaldos con el fin de identificar su existencia y control de estos, así como probar su funcionamiento

Contratos de Mantenimiento

Verificar la existencia de contratos de mantenimiento de equipo, así como verificar en forma aleatoria los últimos mantenimientos realizados

Soporte Técnico

Comprende los puntos relativos a la adquisición, instalación y adaptación según se requiera del software del sistema (el software del sistema o sistema operativo son los programas desarrollados por el proveedor del equipo, que entre otras funciones se encargan de comunicar a la computadora las operaciones que mediante diferentes programas de aplicación realiza el usuario). El acceso al software del sistema debe ser restringido a cierto personal del Departamento de PED.

Documentación de los cambios y modificaciones al sistema operativo

Verificar que la documentación y pruebas realizadas al nuevo sistema operativo

Desarrollo

Los sistemas de aplicación son los programas que manejan los usuarios que se procesan en el computador. Su desarrollo se compone en general de las siguientes fases: diseño, elaboración del programa y su Implementación, así como los cambios de importancia que se requieran durante la vida de los sistemas ya existentes. Todas estas fases requieren de una metodología que permita su adecuado control, seguimiento y autorización.

Lista de las aplicaciones liberadas en el presente ejercicio

Proyectos de desarrollo y mantenimientos de importancia

Manuales sobre desarrollo y mantenimiento de aplicaciones

Mantenimiento

En esta sección se trata lo relativo a los procedimientos establecidos para llevar a cabo cambios cotidianos y modificaciones menores a los programas de aplicación existentes.

Los cambios pueden darse para corregir errores, por cambios en los sistemas o por incrementos en la productividad. Este tipo de actividades se deben llevar a cabo en áreas de disco destinadas a pruebas, de manera que los programas "originales" no se vean afectados sino hasta que las modificaciones hechas han sido probadas suficientemente

Relación de los mantenimientos de sistemas
Solicitud para el mantenimiento de sistemas

Seguridad

Se refiere a control sobre el acceso físico al hardware, incluyendo el CPU, las cintas y unidades de disco, terminales de la computadora y medios para almacenamiento de información como cintas y discos.

Seguridad Lógica la cual se refiere al control sobre el acceso a los recursos del sistema, incluyendo la capacidad para accesar la información o ejecutar programas y transacciones.

Altas y bajas de usuarios
Políticas de seguridad

De esta forma quedan definidos los principales controles que son necesarios para auditar los sistemas de información y obtener información confiable.

En nuestra experiencia hemos visto que en el mejor de los casos, la auditoría de los sistemas de información es muy pobre, por lo que se requiere dedicar mayor esfuerzo y recursos para fortalecer los controles internos de la información. Por lo tanto la presente tesis puede ser una guía básica para implementar el proceso de la auditoría de sistemas de información en las organizaciones.

Existe una inquietud real para que auditor tenga un mayor conocimiento de las computadoras permitiendo una nueva forma de hacer las cosas en beneficio de la organización

La finalidad común siempre será la de establecer una forma eficiente de hacer las cosas, reducir los riesgos y costos y garantizar que la integridad y oportunidad de la información sea la necesaria para la toma de decisiones.

BIBLIOGRAFIA

Análisis y Diseño de Sistemas de Información; James A. Senn, Mc. Graw Hill, Segunda Edición, México 1996.

Sistemas Operativos, Milan Milendovic, Mc. Graw Hill, Segunda Edición, España 1994.

Normas y Procedimientos de Auditoría, Edición 1998, Instituto Mexicano de Contadores Públicos, A.C.

Manual de Revisión CISA (Certified Information Systems Auditor), Information Systems Audit and Control Association, Buenos Aires Argentina 1997.

ASCA Estándar and Procedures Manual, IBM, J. Waldorn, Estados Unidos, 1995.

La Auditoría Bancaria Asistida por el Computador, Seminario Bancario, Abril 1998.

LACRO Computer Asurance Service Workshop "Lo Mejor Alrededor del Mundo", Galaz, Gómez Morfín, Chavero, Yamazaki 1994.

Material de Apoyo para la elaboración de una Auditoría, Galaz, Gómez Morfín, Chavero, Yamazaki. 1997.

Control Objectives, Controling Computer Enviroment; Objectives Guidelines & Audit Procedures, Melden Menkus CISA, CSP, Editor Zella G. Ruthberg, Information System Control Foudation, abril 1990.

Control y Auditoría del Computador, William C. (Mair, CPA, CDP), Donald R. (Wood, CPA), Deagle W. (Davis, CPA); Instituto Mexicano de Contadores Públicos y Touche Ross & Co, mayo de 1980.

EDP Auditing: Conceptual Foundations and Practice, 2nd Edition, 1998, Weber, Mc Graw Hill.

Accounting and Auditing Guidelines, AICPA.

Auditing & Systems Objectives Questions and Explanation, 1995, Gleim and Hillison, Gleim Publications.