Ing° Félix Morales Bueno

AUDITORIA INFORMATICA
CURSO BASICO

Barquisimeto

AUDITORIA INFORMATICA

INTRODUCCIÓN

Cuando se habla de Auditoria Informática la mayoría de las personas tiende a establecer un parangón con la **Auditoría Contable o Financiera.** Sin embargo en lo único que se parecen es en el hecho de que es comparar lo normado con lo ejecutado. Pero dentro de la Auditoria Informática se producen una serie de actividades y funciones que devienen de las labores de sistemas, las cuales difieren bastante de las funciones y actividades contables y financieras.

¿ Podríamos hablar de una Auditoria **ex ante** y de una **ex post?** Definitivamente estoy convencido que sí. Se consideraría (en función del llamado Control de Calidad Total) , que antes de iniciar cada una de las fases de un Sistema, sería necesario realizar una Auditoría ex ante con la finalidad de verificar si se han contemplado todos los elementos necesarios, - detectar y prevenir los posibles errores, etc. **¿ Quién realizaría esta auditoría** ‘ Es aquí donde cobra importancia la llamada **Técnica de los Grupos de Inspección.** Un Grupo de Inspección con una lista de chequeo, realizaría la **auditoría ex ante:** es indudable que en ese grupo debe participar personal de Auditoria Informática. La Auditoría ex post, es de la que se ha venido tratando anteriormente, la que se realiza después de implantado el sistema.

¿PERFIL DE FUNCIONES DE UN AUDITOR INFORMATICO?

“ Un Auditor Informático debe tener los conocimientos técnicos para comprender el tema que vaya a examinar “.[1]

Esto implica que un Auditor Informático debe:

a) Conocer de Hardware, Software y sistemas que utilice la organización en la cual se va a efectuar la auditoría.
b) Estar familiarizado con los estándares vigentes en la misma.
c) Utilizar paquetes de auditoría para examinar los datos almacenados en soportes magnéticos.
d) Ser capaz de codificar consultas en, al menos, un lenguaje de programación o un paquete, de acuerdo al sistema del cual se trate.
e) Tener conocimientos de lenguajes de control de tareas, sistemas operativos, análisis y programación de sistemas.

[1] L.Thomas., a.J y Douglas, I.J Auditoría Informática. Edit. Paraninfo. Madrid, 1988.p.

En función de estos conocimientos el Auditor Informático se encarga de revisar:[2]

a) Los controles en las aplicaciones instaladas, con el fin de determinar si producen información exacta, oportuna y significativa.

b) La integridad de los datos.

c) El ciclo de desarrollo de nuevos sistemas. Debe participar en los **Walkthrough** presentaciones- para dar su aporte en lo que podría considerarse una auditoría **ex ante** y participar en los grupos de inspección.

d) Auditoria de datos reales y resultados de los sistemas que ya estén implantados.

e) Procedimientos de operación.

f) Seguridad.

g) Mantenimiento de sistemas.

h) Procedimientos de adquisición de hardware y software.

i) Prácticas gerenciales del departamento de sistemas o informática

Debe además colaborar con los auditores financieros con el fin de que puedan utilizar los recursos de computación de la empresa en el desarrollo de sus procesos de revisión.

En algunos casos en relación a temas técnicos, los Auditores pueden necesitar ayuda del equipo del departamento de informática sobre equipos, ejecución de paquetes, temas de programación o interpretación de la documentación existente.

En realidad la Auditoria Informática se divide en varios tipos de Auditoría: de **Programas, de Procesos, de Procedimientos, de Sistemas de Hardware y de Seguridad.** Es posible entonces que dentro de las labores de Auditoría Informática participe **más de un Auditor** si no se encuentra una persona que pueda cubrir todos los tipos de Auditoría.

FUNCIÓN DE CALIDAD EN SISTEMAS DE INFORMACIÓN

Para ser consecuentes con la corriente actual **de calidad total** es necesario que en el análisis y diseño de sistemas se supervisen estrechamente los atributos o elementos que califican la calidad de un sistema. De acuerdo con algunos autores estos atributos se relacionan con:

[2] Fabregas, J.Lloréns. Sistemas de Información. Tomo II. (Calidad de Sistemas). Edit Reverte Venezolana S.A. Caracas. 1988.p.

a) Satisfacción de las necesidades (requerimientos) de los diferentes usuarios.

b) Satisfacción de las exigencias y necesidades del departamento de informática y de la organización en general.

c) Ser consistente con las exigencias del Medio General y Específico.

d) Ser controlable y auditable.

e) Ser implantado conforme a los procedimientos, política, estándares y lineamientos de la organización y del departamento.

f) Ser efectivo y eficiente.

COMPATIBILIDAD DE LA AUDITORIA CON LA FUNCIÓN DE CALIDAD

Aun cuando pareciese que existen repeticiones o conflictos de competencia entre ambas funciones no es así, la unidad o las personas que ejercen y desarrollan las funciones de calidad del sistema colaboran con la gerencia de Sistemas, Informática o Procesamiento Electrónico de Datos, para identificar: los métodos, normas, procedimientos, herramientas y fijar los estándares que contribuirían a desarrollar sistemas con una calidad acorde con los parámetros de la organización. También ayudan o auxilian al líder, analistas y programadores, de cada proyecto para que puedan aplicar los elementos mencionados.

La Auditoria se encarga de verificar que los procedimientos, estándares, métodos, normas, etc. Sean aplicados en forma conveniente y consistente. Elaborará los informes de auditoría y reportará a la autoridad correspondiente,

Auditoría revisa y evalúa los **detalles actuales.** Calidad lo hace **con visión de futuro,** para incorporar mejoras técnicas, tecnologías o productos nuevos que aparezcan el mercado.

Es evidente entonces que la Auditoría Informática no se opone ni compite con la Calidad de Sistemas, son actividades que se complementan para tratar de lograr sistemas **de alta calidad** tanto en el momento de **la implantación** como durante **su vida útil.**

Para que la Auditoría Informática y Calidad de Sistemas, puedan llevar adelante sus funciones en una forma eficiente, es necesario que los profesionales encargados del análisis, diseño, programación, implantación, administración y gerencia de los mismos, internalicen la necesidad de documentar adecuadamente los sistemas en cada una de las fases, ya que a la hora de auditar (en especial la Auditoría Externa), debe hacerse sobre algo tangible, examinable, establecido en forma normativa o procedimental. **Sin la documentación adecuada se hace casi imposible ejecutar una auditoría.** De igual forma, el control de la calidad de la calidad de cada una de las fases del sistema debe hacerse con el apoyo de una documentación adecuada.

Pero es también evidente que por las características del perfil que se esbozó al principio de la intervención, al profesional de Auditoría Informática **hay que formarlo,** pues **no es un Contador con ligeros conocimientos de computación,** ni un Computista, ni un Ingeniero de Sistemas, ni un Ingeniero en Informática, **es un profesional con un perfil bien definido,** que no se está formando en nuestras casas de estudio.

AUDITORIAS E INGENIERIAS

Existe una gran diferencia entre las Ingenierías tradicionales (Civil, Electrónica, Química, etc.) y las nuevas ingenierías, tales como: Ingeniería de Software, Ingeniería de Sistemas, Ingeniería Informática. Para el desarrollo de los proyectos en cualquiera de las Ingeniería tradicionales existe un conjunto de **reglas, especificaciones, normas,** etc., las cuales permiten que los ingenieros, diseñadores, calculistas, inspectores, residentes, etc. puedan ejercer sus funciones. Los **Ingenieros Inspectores ejercen funciones equivalentes a las de los Auditores dentro de los proyectos desarrollados en el campo de sus respectivas especialidades.** Sin embargo dentro del campo de las nuevas ingenierías, las normas, especificaciones, etc. deben ser escritas para cada proyectos, n**o existen especificaciones oficiales, ni normativa, ni nada similar,** por lo tanto el parecido entre la Auditoría contable y la Auditoria de Sistemas o informática es solo una utopía. Se homologaron las funciones pero dentro de marcos de referencia diferentes. Es de esperar que las **Asociaciones de Profesionales de la Informática,** la de **Auditores Informáticos,** el **Colegio de Ingenieros** y el Gobierno a través de quien le competa, subsanen en un plazo más breve que largo, esta deficiencia. De esta forma se facilitaría el trabajo de los Auditores, las relaciones con los clientes y usuarios, se aclararían muchos problemas legales que se presentan por carencia de una normativa y los cuales se hacen evidentes dentro de las labores de Auditoría.

NECESIDAD DE LA AUDITORIA INFORMÁTICA

El uso de los computadores trae consigo la obligación de pensar. Y de pensar en futuro. Sin genialidad, pero con mucha racionalidad.

Y junto con los computistas e informáticos **generan** los **grandes proyectos** de sistemas de información. Proyectos utópicos, que nunca se terminan. Proyectos que nunca dejan de ser proyectos, por más que cambien la generación de los computadores y las metodologías de diseño.

-¿Qué ha pasado?.

Algo en este binomio “computadores – informáticos”, no ha funcionado bien, y los sistemas de información de nuestras empresas dejan mucho que desear. La rentabilidad de los centros de computación esta cuestionada y todos saben que el costo de la información producida es demasiado elevado.

Para empeorar las cosas, ahora aparece en el escenario la figura del “delito informático”. Figura que aumenta de proporción peligrosamente, de acuerdo a lo divulgado por las agencias internacionales de noticias y los informes presentados en las jornadas anuales del Colegio de Contadores de Venezuela. Las pérdidas anunciadas son de miles de millones de dólares y en nuestro modesto universo, cientos de millones de bolívares. Y sigue en ascenso. De seguir su expansión, dentro de poco, las pérdidas causadas por esa figura tan indeseable, igualarán las pérdidas ocasionadas por la improductividad de la mayoría de los centros de computación. **Se dice que se roban más de dentro de las organizaciones bancarias con los computadores, que los asaltantes desde afuera.**

¿Y aquí, qué sabemos sobre ese tipo de delito?.

Si nos guiamos por las noticias divulgadas, ese virus nos ha contagiado hasta ahora en pequeñas proporciones. Cuando atacará de nuevo, no se sabe. Lo que sí se sabe, es que la mayoría de **nuestras instalaciones están indefensas y muy poco o casi nada se ha hecho en materia de prevención.**
Los informes presentados en las últimas reuniones realizadas hace poco en Caracas, sobre medidas de seguridad y de contingencias, así lo demuestran.

¿Qué precauciones tomar?.

Daniel Seligmanh, en un artículo publicado por Fortune e intitulado “Macnamara´s Managment Revolution”, dijo “La base de la revolución ´Macnamaristá no es su apoyo en los computadores, sino la insistencia por **ser racional y sistemático”.**

Bajo esa premisa surgen la NASA y los proyectos espaciales.

Según Seligman, en la administración MacNamara, nada era aceptado por un simple acto de buena fe. **Las normas tradicionales no eran aceptadas sin ser verificadas y comprobadas.** Todas las interrogantes eran definidas rigurosamente y todas las posibles soluciones eran analizadas a la luz de sus consecuencias. Los datos debían ser exactos, debían ser precisos, y debían estar a tiempo. El cumplimiento de esos principios era vigilado permanentemente. **Además, en forma sistemática y recurrente, se sometía a una auditoría periódica, cada uno de los componentes del sistema de información, con el fin de determinar su confiabilidad como soporte de las funciones operacionales.** De esa forma había una evaluación permanente de todos los aspectos que envolvían esa administración.

ESTO ERA “SER RACIONAL Y SISTEMÁTICO

Estos principios son válidos para el éxito de cualquier administración. Pero es difícil aplicarlos en una sociedad que tiene una marcada tendencia por las decisiones intuitivas.

Con observar las permanentes correrías de nuestros ejecutivos resolviendo problemas “urgentes” e “imprevistos”, es suficiente para comprender lo difícil de la aplicación de estos principios en nuestras empresas.

Donde la improvisación sustituye con frecuencia a la planificación, es muy difícil ser racional y sistemático. Sin embargo, debemos insistir en la necesidad de serlo. Principalmente en lo referente a la auditoría y /o evaluación de nuestros sistemas de información.

Diferentes autores han expresado las siguientes opiniones acerca de la Auditoria Informática:

“Toda empresa debería hacer periódicamente una “auditoria administrativa”. Al referirse a “auditorias administrativa”. “Una evaluación completa de la empresa. Principalmente de su sistema de información. Ya que de su confiabilidad dependía el éxito de las decisiones gerenciales”.

“Auditoría : La técnica más amplia y poderosa para resolver los problemas empresariales, porque permite descubrir y corregir los errores administrativos”.

Además de permitir “descubrir y corregir los errores administrativos”, la Auditoría permanente de los sistemas de información, es el mejor sistema que se conoce como prevención al delito informático. Sin embargo, la mayoría de nuestras empresas no lo ven así.

En nuestro medio, las altas esferas directivas no parecen estar de acuerdo con los conceptos expresados anteriormente. O no hay un buen entendimiento de los mismos, o hay discordancia en relación a esos principios.

Las autoridades externas normalmente se dedican a la función tradicional de revisar **las cuentas financieras de la empresa y determinar si ellas reflejan de forma razonable su condición financiera.** Por supuesto que, “a la luz de principios contables de aceptación universal”.

Algunos auditores externos están acostumbrados a redactar una “carta de recomendaciones” después de cada auditoría. Es costumbre analizar en ellas algunos componentes del sistema de información de la empresa. El análisis es superficial y normalmente no esta sujeto a un seguimiento sistemático. Sin embargo, son muchos los administradores que dan inmenso valor a esas cartas, porque señalan errores administrativos que deben ser corregidos.

Las auditorías internas por otro lado, se ocupan mayormente de la revisión de las operaciones contables. Normalmente lo hacen con miras a facilitar la labor de los auditores externos. Los que están familiarizados con ese tipo de trabajo, saben que la mayoría de nuestras observaciones hacen todo lo posible para evitar las observaciones negativas, en las certificaciones de los estados financieros.

Las labores realizadas por ambas auditorías, distintas de las mencionadas anteriormente, son labores de excepción. Por este motivo, la mayoría de los componentes de un sistema de información de la empresa no son auditados con la periodicidad requerida. Algunos inclusive, nunca son auditados.

La información es un recurso valioso para toda organización. La mayor parte de las empresas no podrían sobrevivir sí careciera de información formal. En muchas de ellas se observa una tendencia cada vez mayor a ampliar la efectividad y la utilización de la información más allá de la simple vigilancia de los aspectos legales y de la solución rutinaria de problemas. Para hacer frente a estas necesidades cada vez mayores se necesitan fuertes inversiones. La cuestión es : ¿Justificará la inversión los beneficios recibidos?.

La elaboración de información formal cuesta dinero. ¿Cuánto debe gastar una empresa para obtener información?.

EL COSTO DE LA INFORMACIÓN

En algunas empresas, el procesamiento de datos para hacer frente a las operaciones legales y rutinarias y para obtener también información de alto nivel, representa entre 5 y 15% del costo total de operación de la empresa. En ciertas organizaciones financieras, el costo puede elevarse hasta 50%. Los costos de operación del sistema de información se identifican del modo siguiente:

1.- **Costo del equipo.** Dentro de ciertos limites, en general este es un costo fijo o perdido, que aumentará con los altos niveles de mecanización.

2.- **Análisis de sistemas, diseño e implantación.** Es un costo perdido que aumentará normalmente con los altos niveles de mecanización. Esta función incluye la formulación de una metodología para los procesamientos generales de datos. Si se usa la computadora, será necesario incluir también la preparación de programas.

3.- **Costo del espacio y del control de factores ambientales.** Este es un costo semivariable. Como ejemplos podemos mencionar el del espacio, el de los sistemas de acondicionamiento del aire, el de las unidades de control de energía, el de las medidas de seguridad, etc. Normalmente, estos costos aumentan con los altos niveles de mecanización.

4.- **Costo de conversión.** Es un costo perdido o amortizable que incluye toda clase de cambios, por ejemplo, del método electromecánico a la computadora.

**** Los llamados costos perdidos pudiesen ser considerados (como en cualquier proyecto), costos de inversión inicial y por lo tanto no serian perdidos, serian amortizables.**

5.- **Costo de operación.** Básicamente es un costo variable y comprende las diversas clases de personal, la instalación y mantenimiento de sistemas, los suministros, los servicios y su conservación.

" El computador como una panacea, es una abstracción. Como instrumento puede ser muy útil. Y como instrumento, el adquiere valor en función del uso que el hombre haga de el: El hombre, por el uso que haga del instrumento.

Ninguna máquina ha producido más leyendas utópicas que el computador. Son mayoría los que piensan que el computador lo hace todo. Que es fácil de usar y que todo está preprogramado. Muchos dirigentes empresariales piensan que basta con instalar un computador en su empresa, para dotarla de un sistema de gestión automatizada. ¡Qué lejos están de la realidad¡.

El computador lejos de simplificar la técnica y los negocios, ha aumentado su complejidad e impuesto a los investigadores y a los directivos de empresas, una serie de servidumbres constante-mente cambiantes."[3]

Y así mismo como el advenimiento del computador ha hecho más compleja la administración empresarial, ha dificultado la labor de auditoría, que ya de por sí es compleja.

Sin embargo, el computador como instrumento, puede ser muy útil. Y como instrumento el adquiere valor en función del uso que el hombre haga de él. Así el computador pasa a ser un instrumento para enfrentarse a lo complejo. Pasa a ser una herramienta para la auditoría.

PROGRAMAS PARA AUDITORIA

Existen tres tipos de programas de computador que sirven como herramienta para la verificación de controles:

1.- **Generadores de Datos de Prueba.**

Este tipo de programas emplea diversas técnicas para generar datos de prueba variables, tales como valores al azar, valores constantes, valores dentro de rangos específicos que han de colocarse en los campos dentro de los registros, o datos que se encuentran en condición de error.

[3] LAGO, Danton, "EL COMPUTADOR Y LA VENTA DE ILUSIONES", El Carabobeño, 21-11-86, c-9.

2.- **Programas de computador "hechos a la medida".**

Son programas diseñados internamente por personal de programación, para efectos específicos de Auditoría.

Ventajas: Puede utilizarse en vez de los programas de operación de Auditoría en aquellos computadores en los que se usan estructuras no estándar para los archivos de datos.

Desventajas:

1.- Costo de Desarrollo relativamente alto.

2.- Necesidad de que el auditor posea un conocimiento técnico específico sobre el lenguaje de programación empleado.

3.- Los programas (a menos que sean preparados por el auditor) deben verificados para asegurar que efectúan los procesos que se pretenden.

4.- Alto grado de obsolescencia de un año a otro para algunos, conforme cambian las estructuras de los archivos y de los registros.

5.- Mantenimiento continuo con la ayuda técnica y costo correspondiente.

3.- **Programas de Operaciones de Auditoría de Propósito General.**

Principal herramienta para el auditor. Se han introducido varios sistemas de programas de operación. Aunque poseen características individuales y únicas, tienden a ser similares en cuanto a concepto y propósito. Básicamente, dichos programas de operación presentan un métodos por el que las instrucciones escritas que cubren actividades de Auditoría, pueden ser convertidas a programas de computador.

Los paquetes de programas de operación de Auditoría, son lenguajes de programación especializados diseñados para cubrir las necesidades del auditor.

Un usuario de programas de operación de Auditoría de propósito general especificará más procesamiento con menos codificación que los programas "hechos a la medida". Por lo tanto esta herramienta es mucho más productiva en la utilización del tiempo de programación.

Dentro de estos programas se encuentran los programas monitores internos, los cuales permiten medir el número de compilaciones efectuadas en el desarrollo de un programa determinado y el número de horas empleados en el mismo. La eficiencia del programador se determina comparando con los estándares de la organización.

Así como cualquier proyecto con objetivos y áreas orientadas, por ejemplo, un proyecto de desarrollo de sistemas, la Auditoría de un sistema computarizado de empresas debería ser

estructurada de arriba hacia abajo. También debería contener un número de fases lógicas y pasos dentro de dichas fases. Además debería ser acompañada por puntos apropiados donde la revisión gerencial y la aprobación de trabajo adicional sean requeridos, basados en resultados documentados de pasos previos. También deberá ser un proceso controlable, sujeto a los mismos tipos de gerencia de proyectos y técnicas de control que son usualmente aplicadas en proyectos de desarrollo de sistemas. En resumen, deben ser desarrollados aplicando las técnicas y método de sistemas.

Si el auditor de sistemas de información espera tener éxito, un proyecto de Auditoría deberá ser comenzado con:

(1) Un nivel apropiado de entendimiento de la metodología a ser usada y
(2) Un sumario del campo de conocimiento que un auditor debe tener para realizar sus decisiones, sobre todo el alcance a que puede llegar la Auditoría.

Los pasos a dar en la metodología pueden ser sumarizados como sigue:

1.- Establecer objetivos iniciales sobre toda la Auditoría.

2.- Obtener un entendimiento inicial de los negocios y sus sistemas, en términos de sus operaciones, la industria a y así sucesivamente, a través de la recopilación de información básica.

3.- Desarrollar una forma de representación que muestre el entendimiento de los objetivos de la empresa.

4.- Expandir dicha comprensión para abarcar los riesgos del material inherente (o exponerse) a la organización si aquellos objetivos no son cumplidos.

5.- Cuantificar la materialidad y dar prioridad a las exposiciones, en relación a los propósitos particulares de la Auditoría, bien sea financieros, de control u operacional.

6.- Obtener información adicional a través de recopilaciones detalladas de información, para entender los procesos y actividades por medio de las cuales la empresa espera lograr sus objetivos, y la estructura de control que esta utiliza para asegurar la obtención de los mismos.

7.- Determinar como los aspectos del ambiente afectan el sistema, y si los controles de dicho ambiente son confiables.

8.- Determinar las causas de los errores que puedan ocurrir con el sistema y las transacción dentro del sistema, las cuales pudieran causar dichos errores.

9.- Obtener suficiente información para identificar y evaluar los puntos fuertes y débiles de los controles, así como la efectividad y eficiencia en la prevención o detección y corrección de estos errores.

10.- Determinar los controles claves, los cuáles previenen o detectan y corrigen errores que deberían ser confiables en base a su relativa efectividad y eficiencia.

11.- Diseñar pruebas apropiadas para los controles claves.

12.- Examinar el menor número práctico de controles primarios y secundarios seleccionados para asegurarse que trabajen apropiadamente y hacer prevención o detección y corrección de las causas de errores.

13.- Evaluar los resultados de todos los controles de identificación, evaluación y procesos de prueba, y reportar los resultados de la Auditoría, incluyendo debilidades determinadas y su relativa materialidad en términos de exposiciones totales para la organización.

Este proceso puede tomar considerable tiempo y esfuerzo, envolviendo muchos pasos individuales, la recopilación de muchos tipos de información y documentación, y el entendimiento de muchos sistemas y transacciones. También incluye el desarrollar un método que habilite la estructuración de los esfuerzos resultantes, evaluaciones y documentación de Auditoría, en un conjunto racional de papeles de Auditoría.

VALOR DE LA INFORMACIÓN

El valor de la información está basado en diez características, que se enumeran a continuación:

1.- **Accesibilidad.** Esta característica se refiere a la facilidad y rapidez con que se puede obtener la información resultante. Por ejemplo, la rapidez de acceso puede medirse en términos de un minuto contra veinticuatro horas. Pero, ¿qué valor tiene esa información para el usuario?. ¿Valdrá, por ejemplo, Bs. 10.00 más por acceso con respecto al viejo método?.

2.- **Comprensibilidad.** Se refiere a la integridad del contenido de la información. No se refiere necesariamente al volumen sino que el resultado sea completo. Esta característica es sumamente intangible y, por tanto difícil de cuantificar.

3.- **Precisión.** Se refiere a que no haya errores en la información obtenida. Cuando se trata de un gran volumen de datos, en general se producen dos clases de errores: de transcripción y de cálculo. Muchos aspectos de esta característica pueden ser cuantificados. Por ejemplo, ¿cuál es la proporción de errores por cada mil facturas elaboradas por métodos manuales y por computadoras? ¿Qué valor representa reducir el número de errores?. Por ejemplo, ¿aumentarán las ventas 0.5% si el número de errores de facturación se reduce a 10%?.

4.- **Propiedad.** Se refiere a que también se relaciona la información con lo solicitado por usuario. El contenido de la información debe ser apropiado para el asunto de que se trate, todo lo demás será superfluo y a la vez costoso en su elaboración. Esta característica es difícil de medir y al igual que ocurre con los demás, ojalá éste implica en la eficacia del diseño de los sistemas.

5.- **Oportunidad.** Esta característica se relaciona con una menor duración del ciclo de acceso: entrada, procesamiento y entrega al usuario. Por lo común, para que la información sea oportuna, es preciso reducir la duración de este ciclo. La oportunidad puede medirse en algunos casos. Por ejemplo, ¿en que proporción se podrán aumentar las ventas si se informa inmediatamente al cliente sobre la disponibilidad de artículos de inventarios?.

6.- **Claridad.** Esta característica se refiere al grado en que la información está exenta de expresiones ambiguas. La revisión de un informe puede resultar costosa. ¿Cuánto cuesta revisar este informe? (A la claridad puede asignarsele un valor muy preciso en dinero).

7.- **Flexibilidad.** Concierne a la adaptabilidad de la información, no sólo a más de una información, sino a más de un responsable de la toma de decisiones. Esta característica es muy difícil de medir; pero puede asignarse un valor cuantificado dentro de un margen muy amplio.

8.- **Verificabilidad.** Se refiere a la posibilidad de que varios usuarios examinen la información y lleguen a la misma conclusión.

9.- **Imparcialidad.** Se refiere a que no exista un intento de alterar o modificar la información con el fin de hacer llegar a una conclusión preconcebida.

10.- **Cuantificable.** Se refiere a la naturaleza de la información producida por un sistema formal de información. Aunque a veces los rumores, conjeturas, etc. Se consideran como información, están fuera de nuestro ámbito.

EL VALOR DE LA INFORMACIÓN PERFECTA.

Los resultados de las decisiones gerenciales están influenciados no sólo por las manipulaciones de factores sobre los cuales un gerente tiene control, sino además, por una gran variedad de factores incontrolables y muchas veces desconocidos. Fuerzas naturales, gubernamentales, competitivas y consumidoras ofrecen pequeñas oportunidades para su manipulación. También, el éxito de las decisiones es influenciado por estos factores.

Información Imperfecta.

Obviamente es poca la información perfecta. En contados casos somos precisos en nuestras predicciones, o en nuestro entendimiento de cómo son las cosas. Podríamos asumir que el valor de la información se incrementará con aumentos en la precisión de la información.

Usando el valor de la información perfecta, (el máximo beneficio obtenible a través de un entendimiento perfecto es tener claro como son las cosas y si así seguirán), como medidor, podemos entonces determinar el valor de la información imperfecta, al estimar que tan cerca está dicha información de ser perfecta.

El análisis Bayesiano genera evaluaciones subjetivas de las probabilidades de que la información será correcta, y provee también la información que será descontada en caso de no ser perfecta. El próximo paso es usar la evaluación descontada para determinar el valor de la información propuesta, de acuerdo con su desviación estimada de la información perfecta (el valor el cual podemos estimar).

El foco del análisis Bayesiano es valorizar la información anticipada en términos del valor esperado de la información perfecta. El valor de la información es determinado por los resultados esperados. Esto es por supuesto, un acceso válido y lógico. Raramente podemos justificar la colección de información por amor a la información (fuera de universidades y bibliotecas). La información es reunida y procesada para producir un resultado. Para el gerente de mercadeo, dicho resultado aparece en la forma de estrategias, las cuales dirigen las actividades hacia un resultado provechoso.

GENERALIDADES ACERCA DE LA UTILIDAD DE LA INFORMACIÓN.

A pesar de las diferencias en la percepción de los usuarios de la información, es posible hacer algunas generalidades concernientes al valor de la información.

Nosotros si podemos observar que el valor de la información aumenta si:

(1) el formato, el lenguaje y el grado de detalle accede a los deseos del usuario;

(2) los accesos físicos y organizacionales se vuelven más fáciles; y

(3) el tiempo de adquisición es cercano al tiempo de uso(con tal y no ocurra después de la decisión).

Podemos recíprocamente generalizar que la información y su valor disminuirá tan pronto como:

(1) el formato y el lenguaje sean menos entendible;

(2) el volumen de los detalles incremente;

(3) los accesos físicos y organizaciones a la información se vuelvan más difíciles;

(4) el tiempo de adquisición es distante del tiempo de uso (y sin importancia después de la decisión).

USO DEL CHECK LIST.

Una lista de chequeo también puede ser usada para examinar el valor utilitario de la información disponible. Esto se aplica igualmente a la información de mercadeo, la generada para otros usos en la firma y la información inesperada o no solicitada.

Una lista básica de chequeo pudiera ser la siguiente:

1.- ¿Es el formato, el lenguaje y la presentación de la información legible para el usuario?.

2.- ¿Es toda información externa removida? ¿la sumarización de este maximizada?.

3.- ¿Está el tiempo de entrega de la información cerca del tiempo de necesidad?.

4.- ¿Existe fácil acceso y retiro de la información necesitada?.

5.- ¿Existen barreras innecesarias de organización para el acceso y uso de la información?.

La información es un recurso costoso. Y es costoso no solo en su adquisición y manejo, sino también en su descuido. Procesar la información, incluyendo su adquisición, almacenamiento, transmisión y entrega a los que toman decisiones, requiere gastos de tiempo, recursos humanos y facilidades. La selección de información pertinente, proveniente de las masas de datos disponibles, son actividades de tiempo adicional y de absorción de recursos. Los equipos para el procesamiento de datos, el software necesario que le acompañe y el staff de procesamiento de información son grandes inversiones.

Información errada o inadecuada puede resultar en decisiones inapropiadas, con gastos y costos potencialmente desastrosos, pérdida de tiempo y pérdidas excesivas de costos y oportunidades.

Es aparente que un balance debe ser alcanzado entre los costos de la información descuidada (valor de la información) y los costos de la adquisición y proceso de la información. La gerencia prudente de los recursos de la información demanda una teoría y técnica para determinar el valor de la información, la cual permitirá comparaciones con costos asociados.

La gerencia está interesada en la información, no sólo por su propio interés, sino más bien por los beneficios que puede generar. El valor es asignado a la información de acuerdo los resultados esperados de decisiones basadas sobre dicha información, cuando se compara con los resultados recibidos sin la información.

Un gerente debe determinar si adquiere o no la información. El debe también decidir que hacer con la información disponible. Las decisiones son hechas tomando en cuenta que datos hay que eliminar, cuales van a ser adquiridos o cambiados, o de alguna manera procesados. Un criterio explícito para determinar el valor de un dato de información es esencial.

Una variedad de métodos pueden ser usados al determinar el valor de la información:

> El Método Simple de: Ahorro. Está basado sobre los costos estimados de los errores de decisión, los cuales serían evitados si la información en cuestión ha sido adquirida y usada.
>
> El Método de Retorno de Inversión.(TIR)provee un cálculo después de la prueba de los retornos(a través de mejores decisiones) resultado de inversiones alternadas de información.

El Método del Valor Actual. Emplea un cálculo de los retornos estimados en inversiones alternadas de información, descontados por el costo marginal del capital. Este considera el valor actual de beneficios futuros resultantes de la información.

El Método Bayesiano. Incorpora los conceptos esenciales del valor del ahorro y el retorno de inversiones, encontrados en los demás métodos. El análisis Bayesiano considera resultados de actividades alternativas, con estimados de sus pagos asociados y probabilidades de ocurrencia. Este acceso es especialmente útil cuando la naturaleza de la información por recibir puede ser anticipada antes de adquirirse. El análisis Bayesiano puede ser aplicado, por ejemplo, en determinar si hacer o no una investigación de mercadeo.

Las utilidades proveen un vehículo adicional para evaluar el valor de la información. Las utilidades tienen características que explican el valor de un producto (o servicio).

La información, como los productos, posee forma, tiempo y lugar y utilidades de posesión. Estas características pueden ser usadas en explicar el valor de bits individuales de información y en identificar inhibidores del uso de la información.

CONTROL Y CONTROLES.

Palabras usadas con demasiada frecuencia en informática, sin importar mucho el verdadero significado de ambas.

Con el computador se han multiplicado los controles. Analistas y programadores han sido pródigos en su creación. Controles de todo tipo han aparecido. Necesarios e innecesarios. Hay que crear controles, pareciera ser la consigna. Sin embargo, no son muchas las mejorías proporcionadas por nuestros softwares en las funciones de control.

En todos los centros de computación existen muestras palpables de la facilidad con que analistas y programadores han confundido el significado de ambas palabras. “Control de Producción”. “Control de Cuentas por Pagar”. etc. Son los títulos de las aplicaciones más comunes en todas las instalaciones. Todas registrando el pasado, creando historia, creando controles. Pero con muy poco control.

¿Cuánto control ejercen nuestros gerentes a través del computador?.

¿Y cuánto sobre el computador y sus procesos?.

Según Drucker, para que un gerente pueda ejercer el control, los controles deben satisfacer siete condiciones fundamentales:

- Deben ser económicos:
- Deben tener significado:
- Deben ser apropiados:
- Deben ser congruentes:
- Deben estar a tiempo:
- Deben ser simples: y
- Deben ser operativos.

¿Cuántos controles en nuestras instalaciones podrían satisfacer parte de esas condiciones?.

El computador ha representado en nuestras instalaciones un cambio significante en materia de control. Su avanzada tecnología y la rapidez de sus procesos han creado condiciones inmejorables para la creación y mantenimiento de los controles necesarios al ejercicio del control. Usado con eficacia, el computador debería ser la columna vertebral de nuestras empresas en esa materia. El problema está en la filosofía usada por analistas y programadores en el desarrollo del software destinado a apoyar estas gestiones.

¿Cuándo no se sabe controlar, para que crear controles?.

La mayoría de los estudiosos de la ciencia de la administración están de acuerdo con lo dicho por Henry Fayol, hace cincuenta años, a respecto del control de las empresas.
Fayol reconoció claramente que: “en una empresa, el control consiste en verificar si todo ocurre en conformidad con el plan adoptado, con las instrucciones emitidas y con los principios establecidos. Tiene como fin señalar nuestras debilidades y errores a fin de rectificarlos e impedir que se produzcan nuevamente. Actúa sobre todo: cosas, personas y acciones”.

El control implica la existencia de metas y planes. Ningún ejecutivo puede controlar sin ellos. Y cuanto más claros, más completos y más coordinado sean estos planes, más completo puede ser el control.

¿Y nuestros analistas y programadores, conocen las metas y planes de nuestras empresas?,
¿Los entiende?.
¿Están preparados para entenderlos?.
¿Tienen en conocimiento necesario?.
La respuesta más frecuente es NO.

¿Cómo se puede desarrollar un software para controlar metas y planes que no se conocen?.

El desarrollo de un software adecuado, es una labor difícil. Requiere de un personal de muy alta calidad. Entrenado y actualizado.

El anuncio hecho por la IBM en las últimas semanas al lanzar su nuevo PC, dejó muy en claro lo que casi todos saben y muy pocos lo dicen. El desarrollo del hardware avanza a una velocidad muy distinta a la del software. El software no acompaña el hardware. Uno va adelante y el otro va atrás, siempre retrasado y esto no es raro. Los usuarios de micros del modelo AT, hasta hoy los están usando a media máquina. El software tan esperado todavía no está disponible. El de los nuevos PCs, posiblemente lo esté a finales de 1988, si no hay retrasos. Y eso que la IBM dispone de dinero, de personal calificado y además entrenándose permanentemente. Invierte todos los recursos requeridos en el logro de un objetivo. Y aún así, lanza al mercado un producto incompleto.

¿Y nuestras empresas, como pueden avanzar en el desarrollo de software?.

Según Fayol, una de las finalidades del control, “es señalar nuestras debilidades y errores para rectificarlos”.

¿QUÉ DEBE SABER UN AUDITOR INFORMATICO?.

¿El conocimiento requerido para los auditores de sistemas de información varia, dependiendo del ambiente de los sistemas, pero debería incluir la consideración de algunos o todos los aspectos siguientes:

1.- **Estructura del Sistema de Aplicación.**

Esto incluye un repaso del hardware (terminales, unidades de almacenamiento y procesadores); un repaso del desarrollo de sistemas y técnicas de mantenimiento; un repaso sobre programación y uso de tablas de decisión y matrices; un análisis de la documentación computarizada, incluyendo tipos estilos y standards; y repasar las técnicas de control gerenciales de los proyectos de sistemas. Al completar este entrenamiento, el auditor tendría una apreciación de cómo un sistema de aplicaciones es desarrollado (o comprado), operado y mantenido.

2.- **Controles y Procedimientos del Sistema de Aplicaciones.**

Esto incluye el objetivo de los controles de aplicación, el método de aplicar dichos controles y las técnicas para análisis del control interno. Las actividades en la

aplicación del proceso de datos, comunicación de datos y otras áreas pertinentes al procesamiento de aplicaciones serian incluidas, tales como el uso de la base de datos y diccionario de datos. También incluye identificación de los terminales y verificación para los sistemas en línea, y a la vez, los procesos de autorización sobre los usuarios y terminales y transacciones procesables de los usuarios. Las técnicas de computación que podrían ser usadas para asistir en el control de acceso a los datos y los programas también son incluidas.

3.- Gerencia de Datos.

Esto abarca el almacenamiento de datos en cinta y discos; el uso de sellos internos y externos; la preparación de boletines de acceso; definición de registro y archivo; generación de archivo, acceso, y control; y la extracción de datos de las bases centrales de datos. Clave en este aspecto de entrenamiento es la habilidad para definir y comunicar el archivo PED (*) de datos y otros problemas en un lenguaje que pueda ser fácilmente entendible por el personal de procesamiento de datos.

4.- Controles de Instalación.

Esto incluye controles de entrada (input) y salida (output), inventario de producción, controles de instalación, manejo en los errores de los controles de producción, distribución de reportes, control sobre las cintas y otras bibliotecas de almacenamiento, respaldo (back-up) y recuperación, y almacenamiento fuera de sitio (off-site) y retención de archivos. También incluye el propósito y uso de lenguajes de control, sistemas de operación, software del sistema y programas de utilidad. Además, incluye el familiarizar al auditor con las responsabilidades, papel que desempeñará y separación de obligaciones y aspectos de las operaciones computarizadas, funciones de biblioteca, sistema y programación, servicios técnicos, manejo de archivos y, el origen y autorización de las transacciones. Por último, donde los centros de servicio u otros centros remotos de procesamiento son usados, esto incluye arreglos contractuales, propiedad de datos y programas, repasos y accesos de Auditoría.

5.-**Desarrollo de Sistemas y Controles sobre los Procesos de Mantenimiento.**

Esto incluye controles sobre el desarrollo y manteniendo de los procesos y la aplicación de estos durante los proyectos descritos. También debería incluir exposición para el diseño e implementación de los standars de sistemas y técnicas gerenciales de proyectos. Los controles específicos a ser implementados en nuevos sistemas por ejemplo controles sobre entrada (input), procesamiento, salida (output), corrección de errores, cambios de sistema, pista de Auditoría, recuperación de desastres, retención de (*) OED: Procesamiento Electrónico de Datos. Archivos y procedimiento, deberían ser cubiertos. En instalaciones más sofisticadas, se debería incluir exposición de los conceptos tanto de la programación modular como del uso de técnicas de programación interactiva.

6.- Controles de Sistemas En-Línea y Software.

Cuando los termínales, equipos de entrada remota, sistemas de transferencia electrónica de fondos y similares están en uso, el auditor necesita tanto del entrenamiento adicional en los fundamentos de un sistema en línea como de los controles que pueden ser usados con ellos.

7.- Controles sobre el Sistema Manejador de Base de Datos y Software.

Cuando un sistema manejador de base de datos (ODBMS) está en uso, el auditor necesita entrenamiento adicional desde un punto de vista conceptual en su diseño total y uso en el diccionario de datos. Sumado a esto, el auditor necesita poseer conocimientos en los atributos específicos del DBMS en uso en la instalaciones así como en los controles sobre su uso. El entrenamiento sobre el rol y las responsabilidades del administrador de la base de datos o la función del servicio técnico responsable del DBMS, es esencial.

8.- Minicomputadoras y Procesamiento Distribuido.

El auditor necesita información básica sobre los aspectos del control del hardware y software en uso, donde las minicomputadoras son usadas en un ambiente único para especificas aplicaciones. Donde las minicomputadoras (o terminales inteligentes, los cuales son frecuentemente efectivos como microcomputadoras) están en uso, el auditor también requiere entrenamiento sobre conceptos de procesamiento distribuido y las consideraciones relativas al control de procesamiento distribuido.

9.- Aspectos Específicos de las Instalaciones y Sistemas bajo Auditoría.

Por cada una de las aplicaciones del hardware y software que la organización usa (software de sistemas, manejador de cinta), el también requiere entrenamiento adicional en el uso de los aspectos o funciones y en el control de consideraciones relacionadas a aquel aspecto o función.

La clave para este entrenamiento es primero, identificar los aspectos del PED y su organización, que pudieran tener implicaciones potenciales de control o que pudieran ser usadas para los propósitos de técnicas de control requerido y luego determinar que nivel mínimo de conocimiento es requerido para el auditor del sistema tenga la posibilidad de conversar razonablemente sobre el tema del procesamiento de los datos del usuario, y del personal de gerencia. La razón del entrenamiento no es habilitar a la persona para trabajar en una base diaria con daca uno de estos conocimientos y funciones del profesional PED, pero si entenderlo de manera que tenga la habilidad de identificar sus implicaciones de control.

Los aspectos de este control son sustanciales. El auditor de sistemas, en una empresa de tamaño mediano o una gran organización, requerirá entre dos día y una semana, o más entrenamiento en cada tópico, o posiblemente 200 o más horas de entrenamiento en un

período de dos años antes de ser capacitado razonablemente para identificar las implicaciones de sus controles. Esto no es un costo de Auditoria, pero sí un costo de mantenerse al día en la forma en la cual la compañía hace sus negocios.

La trayectoria de carrera, la posición y materia de compensación debe recibir gran atención con esta inversión de entrenamiento, porque la compañía necesita retener al auditor PED por lo menos de tres a cuatro años. Muchos proyectos futuros de sistemas pueden requerir un tiempo de desarrollo quizás excediendo un año, y usualmente alcanza de dos o tres años. Por lo tanto es crítico para la Auditoria que los auditores PED sean retenidos durante el desarrollo de proyectos, donde sea práctico.

La falla de esto, es que existe una implicación pesada sobre la calidad de la documentación de la Auditoria de desarrollo de sistemas, de forma tal que el auditor que llega al proyecto "hecho a medias" tenga la habilidad de seguir lo que ya está hecho y determinar lo que aun se necesita hacer.

CINCO GRANDES PELIGROS.

Los cinco grandes daños para un complejo de computación son el fuego, el agua, el robo, el fraude y el sabotaje. De éstos, el fuego es probablemente el más serio.

LOS INCENDIOS.

Son un problema critico en un centro de computación por varias razones. Primero que todo, las oficinas de computación típicamente contienen materiales inflamables como el papel, cajas, tarjetas, diskettes, cintas, y mucho plástico, etc. El hardware, cables y otros también pueden ser fuente de serios incendios. Aún más, una vez que un pequeño incendio comienza en un equipo de computación, casi siempre es difícil de combatirlo porque los cables, cintas y algunos componentes del hardware emiten humos densos y tóxicos, los cuales inmediatamente fuerzan a que el incendio sea pequeño y pueda ser extinguido rápidamente o que los empleados estén equipados con máscaras anti-gas, el humo los sacará del sitio y aún, pequeños incendios crecerán al no ser chequeados.

Desafortunadamente, los sistemas contra incendio dejan mucho que desear. Los sistemas de irrigación constituyen un problema de tanto daño como el fuego causaría, ya que ellos constituyen un peligro especial a la biblioteca de cintas. Sistemas de dióxido de carbono, la alternativa a la irrigación por agua, son peores que el agua, para los empleados que quedan atrapados en el cuarto de computadoras.

La mayoría de los centros de computación están atestados con equipos permanentes y un gran complemento de carritos y carretillas. Hay frecuentemente una o dos salidas, y casi siempre todas, excepto una, están cerradas. Este tipo de situación, a la par con el hecho de que la mayoría de los incendios repentinamente emiten humos fuertes y gases dentro de los cuartos (como ocurre cuando se abre la puerta de una bóveda o se hala un panel de piso), significa que el cuarto de computadoras constituye un serio peligro para el personal. Los operadores en estos grandes cuartos podrían no alcanzar la salida antes de los 20 o 30

segundos que permiten los irrigadores de dióxido de carbono (no aconsejables en centros de computación), de dejar salir a la gente de dejar caer la espuma.

El fuego es considerado la gran amenaza para las localidades de computadoras por el peligro de destrucción a los archivos de datos y programas. El equipo en sí, usualmente está cubierto por un seguro, y los fabricantes de equipos tienden a responder rápidamente, reemplazándolos o reparándolos, así que la restauración física constituye un problema menor. El reemplazo o reconstrucción de las cintas, discos y archivos de tarjetas es frecuentemente más difícil y algunas veces imposible. Los negocios que no hacen respaldo ("back – up") de sus archivos computarizados más importantes se arriesgan a la pérdida completa de todos sus registros, y ellos los arriesgan todos los días. Dicho "respaldo" fuera de sitio (off-site) es el más importante paso singular que una compañía puede hacer para protegerse a si mismo.

Sumado a la pérdida de registros o equipos, el incendio podría causar otras pérdidas las cuales podrían no estar cubiertas por el seguro. La más importante de estas sería "la pérdida del ímpetu del negocio" (o "momentum"). Un retraso de semanas o meses crea pérdida irreparables a cualquier organización, aún si es posible restaurar las oficinas y registros a su condición original. No solo una línea aérea con su sistema de reservaciones o un banco que posee cajeros automatizados, podrían ser dañados seriamente por un incendio en el cuarto de computadoras, sino también cualquier organización que realmente dependen de su procesamiento de computadoras.

LOS DAÑOS DEL AGUA.

En varios desastres en cuartos de computadoras, lo que el fuego no destruyó, el agua de los bomberos lo hizo. El agua puede entrar en una localidad de computadoras de varias formas. Computadoras en los sótanos o a nivel de tierra en áreas bajas son vulnerables a las inundaciones y varios centros de computación han sido inundados. Centros de PED también pueden ser inundados por el agua con la ruptura de tuberías, incluyendo las que están en pisos falsos y techos, o en las paredes.

En un caso, un cuarto de computadoras fue inundado con agua de una tubería que se rompió en el piso de arriba. Durante la construcción, el techo del cuarto no fue sellado, y cuando la tubería rompió, el agua penetró a través de agujeros, a través del cielo raso y sobre el cuarto de computadoras.

Las inundaciones también pueden ser resultados de combatir incendios sobre pisos de arriba del centro de computación. Esto sugiere una solución obvia: que todos los agujeros del techo sean tapados. Los agujeros son inevitables durante la construcción y a menos que procedimientos especiales sean tomados, los mismos no son tapados.

Los sistemas de irrigación plantean otro daño de agua. En un gran centro de computación se encontraron recientemente de 4 a 6 pulgadas de agua, después que la "cabeza" de un irrigador accidentalmente se rompió. Analizando la situación, se encontraron 4 violaciones de seguridad.

(1) Las tuberías estaban llenas y listas para regar en el instante que la “cabeza” se rompió. Una práctica mejor es el método de la “tubería seca” donde un retraso (30 segundos) está previsto, mientras las pipas de un reservorio, se llenan.

(2) No había una llave para cerrar la tubería en el cuarto. L a llave correcta estaba varios pisos abajo.

(3) No habían desagües debajo del piso falso. Desagües y contornos de nivel son mandatarios en una edificación bien diseñada.

(4) Ni siquiera habían sido provistos con forros e impermeables, los cuáles hubieran protegido fácilmente los equipos de computación. Como resultado, las computadoras fueron desmanteladas, sus partes secadas o cambiadas, probadas, reemsambladas y vueltas a probar.

Mientras que el agua en sí es una amenaza para los componentes computarizados y cables, la misma no constituye un peligro a cintas magnéticas. **Las pruebas han demostrado que las cintas que han sido sumergidas en agua por varias horas pueden ser leídas sin errores después que han sido secadas enteramente (por lo menos dos días) y rebobinadas.** La capa de óxido que cubre la cinta magnética tiene una base de agua y, sin embargo, si dichas cintas retienen humedad por un periodo extenso, lo más probable es que haya expansión de óxido y su eventual destrucción.

ROBOS.

Un sistema de computación es un recurso corporativo de valor y puede ser robado en el mismo sentido que los inventarios o dinero cuando el personal de computación usa el “tiempo” del computador de la compañía para correr trabajos o procesar programas para ajenos. El problema existe a escala pequeña en casi todas las instalaciones computarizadas. Probablemente no exista una corporación en este país que no haya tenido su sistema de computación apropiado para usos ajenos al negocio en un tiempo dado. El mismo problema ocurre con el mal uso de las fotocopiadoras, solo que a una escala más grande.

Desafortunadamente, ha habido varios casos publicados donde este abuso alcanzó el punto, donde un operador de computadoras o varios de ellos manejaban un buro de servicios privados computarizados, usando el equipo del patrón. El potencial de ganancias puede ser deslumbrador; el patrón cubre todos los gastos inconscientemente (renta de los equipos, reparación y material) y en un caso, fue aún forzado a expandir su computadora para satisfacer el aumento de trabajo.

Datos o sensibles en forma legible de computadora fácilmente pueden ser robados. Muchas compañías invierten millones de dólares en archivos de datos y programas, y luego les proveen con la misma protección que le darían a una máquina de escribir o calculadora.

El Software de computadoras es otro recurso corporativo el cual es fácilmente robado. Las cintas magnéticas y discos son fácil y rápidamente copiados – sin rastros, muchas instalaciones usan los nuevosmini-reels (o mini-carretes), los cuales se introducen fácilmente en el bolsillo de una chaqueta o bolso. Los carretes tamaño standard pueden ser removidos en un portafolio o botados en la basura y luego ser recogidos. Luego de varias horas de impresos en los computadores también pueden ser escondidos en la basura.

FRAUDE.

Cada año, millones de dólares son desfalcados en corporaciones estadounidenses. En un número incrementados de casos, las computadoras han sido usadas para asistir en dichos fraudes. En efecto, el potencial de pérdidas por fraude y los problemas de prevención y descubrimiento de fraude se han incrementado considerablemente en sistemas basados en computadoras.

Muchos gerentes no tienen conocimientos de la enormidad del problema. El año pasado 69.000 personas fueron arrestadas en los Estados Unidos en casos de fraude y desfalco. Nadie conoce el número que no fue detectado. Muchos de aquellos que fueron detectados no resultaron en arresto. En muchos casos y por varias razones (tales como evitar la mala publicidad) la parte defraudada se resistió a demandar.

La observación más inquietante es que el ambiente del computador actualmente facilita algunas maquinaciones. Hay cuatro métodos básicos que el desfalcador puede usar:

1.- Manipular datos de entrada.

2.- Desarrollar programas o rutinas impropias.

3.- Alterar o crear archivos de daños ficticios.

4.- Transmitir ilegalmente, interceptar o desviar información teleprocesada.

Todos estos métodos han sido usados para defraudar corporaciones americanas y, sin duda, están siendo usadas ahora mismo.

La manipulación de datos de entrada. Usualmente es fácil de hacer porque el equipo de preparación de datos es fácilmente disponible y usable. Es muy difícil de detectar porque los datos falsos son indistinguibles de los datos legítimos y además los métodos típicos de control son frecuentemente simples y fácilmente conocidos a un gran número de personal de la organización. Así de no existir defectos, usualmente no es difícil introducir datos de entrada fraudulentos para capitalizar en esa debilidad.

“En una casa de corredores de bolsa en New York, un vice-presidente robo más de $250.000 sobre un periodo de 5 años manipulando los datos de entrada. Su esquema fue una variación compleja de lo que se conoce como “lapping”. Su rutina era ir a la oficina después del cierre o durante el fin de semana, y hacer nuevas tarjetas perforadas de datos. Como él estaba a cargo de la oficina principal de la compañía, le era íntimamente familiar

todas las operaciones y no despertaba sospecha al estar en la oficina durante las horas extras".

"En un complicado esquema de dos bancos y tres compañías, 4 hombres robaron $ 1.3 millones al alterar los datos de entrada – en este caso memorándums de depósitos antes de su procesamiento por las computadoras del banco".

El desarrollo de programas de computación fraudulentos. Es considerablemente más difícil que manipular datos de entrada, no porque la programación en si sea más difícil, sino porque la mayoría de las grandes compañías poseen procedimientos controlados de pruebas para nuevos programas y cambios de los mismos. Sin embargo, muchos problemas aún surgen.

"En una casa de corredores de bolsa, el gerente de procesamiento de datos robo $ 81.000 durante un periodo de 4 años con un plan basado principalmente sobre cambios no autorizados. El pudo emitir cheques sobre su compañía y enviarlos a cuentas falsas las cuales el había construido".

Alteración o creación de archivos de datos ficticios tales como aquellos mantenidos en cinta magnética o disco a menudo requieren manipulación de datos de entrada o el maltrato de programas para computadoras "limpios", fraudulentos o ambos.

"Durante un periodo de 5 años, el contador de una gran firma empacadora de frutas y vegetales de California, desfalco más de 1 millón de dólares al inflar cuidadosamente los recibos. Realizando toda la contabilidad de la compañía en un buro de servicios (el cual el poseía), el pudo mantener juegos múltiples de archivos; y esencialmente simulando los efectos de varias transacciones, el pudo robar cantidades, las cuales no distorsionaban los resultados reportados. Este robo envolvió la manipulación de datos de entrada y programas de computación, a la vez que los archivos principales".

La transmisión ilegal, intercepción o desvío de información teleprocesada se ha vuelto más importante en los últimos 2 años. Así como el volumen de transmisión continúa incrementándose y los negocios transmiten información crecientemente sensitiva – a menudo, a través de redes transmisoras comunes – las oportunidades para la interrupción, alteración o creación de mensajes ficticios han incrementado.

"En Marzo, en Oakland, la policía de California arrestó un empleado de un buro de servicios y se acuso con el robo de programas de un competidor; el ladrón aludido marcaba el número del computador de su competidor desde un terminal remoto, eludia el sistema de seguridad, copiaba la información deseada y luego la introducía en los archivos de su propia computadora".

En muchos de estos casos, la más enervante característica es la simplicidad del esquema.

Mientras que el fraude y el desfalco siempre han sido problemas potenciales para una compañía, el uso incrementado de sistemas de computación ha tenido a aumentar los riesgos en muchos casos. En este ambiente, las oportunidades para el fraude son ampliadas

y los problemas de prevención son incrementados porque sistemas basados en computadoras traen una nueva lista de complicaciones:

1.- Nuevos Tipos de Personas. Programadores, operadores, bibliotecarios, diseñadores de sistemas, aún gerentes de PED son en muchos casos una nueva "raza" de personas no familiarizadas con los convenios tradicionales de control. Las Auditorías y los procedimientos de control a menudo interfieren con el procesamiento eficiente de los datos y a menudo son consecuentemente despreciado por programadores y otros.

2.- Nuevas Formas de Datos. Los datos importantes (en tarjeta, cintas o discos) vírgenes. Anteriormente, reportes y libros mayores sensitivos y archivos tenía un carácter distintivo y podía ser identificados a la vista.

3.- Centralización de los Datos. Frecuentemente, todos los registros básicos y detalles de soporte, así como los datos de transacciones y aún los programas de procesamiento anteriormente pudieron ser difíciles porque los registros necesarios estaban localizados en diferentes oficinas, ahora es posible que todo el material esté en un solo cuarto. Desde que todos los datos de los sistemas de computación lucen casi igual, es difícil, decir cuando alguien está usándolos.

4.- Falta de Intervención Humana. Por su misma naturaleza, el proceso de programación reemplaza mucho el procesamiento manual y también mucho de la inspección manual, la cual no puede ser duplicada debido a la lógica del computador. Como resultado las transacciones inusuales las cuales nunca hubieran escapado a inspecciones manuales ahora saltan a través del sistema de computación. Un auditor lo expuso de esta forma: "a un grado justo, nosotros hemos perdido aquellas ancianitas sospechosas y nunca tendremos la habilidad de programas lo que ellos hicieron".

5.- Dificultad de Entender. No solo son los datos en la forma de lectura por máquina, sino también la lógica de programación, son difíciles de seguir y comprender, aún para el diseñador de programas. Como resultado, muchos gerentes (y demasiados auditores) ahora tienen problemas entendiendo el flujo básico de transacciones. Lo que es peor, muchos gerentes (quienes deberían saberlo mejor) han comenzado a tomar las cosas de buena fe".

6.- Cambios hechos sin Indicios. Anteriormente a la automatización, los registros, detalles, entradas, balances, etc., eran difíciles de cambiar sin dejar algun indicador como marca. El método de procesamiento fue aún más difícil de cambiar. Hoy, entradas (input), archivos de datos y los programas – la lógica o el proceso – pueden ser cambiados casi instantáneamente y sin pistas – Los duplicados pueden ser generados fácilmente y también de esa forma pueden ser destruidos sin indicios.

7.- Formas de Auditoría Degradada. En un número de casos los nuevos sistemas basados en computadoras carecen de formas de Auditoría adecuada.

SABOTAJE.

Quizás el riesgo más espantoso para un complejo PED es el sabotaje. Por muchas razones, los centros de computación en la educación y los negocios han sido blancos para los radicales y los descontentos. En la Universidad Sir George Williams en Montreal, los estudiantes ocuparon el centro de computación y cuando atacaron, destrozaron dos grandes computadoras con hachas. Lo que no pudieron cortar, los quemaron. En la Universidad de Boston, vagos destruyeron una computadora con pinzas de cortar alambre y ácido. En Londres, dos computadoras compartidoras de tiempo en un buro de servicio fueron saboteadas por un empleado que sabía que cortar para prevenir un fácil diagnóstico. Durante el pasado año, bombas destruyeron o dañaron las computadoras en las Universidades de Kansas, Wisconsin y el Colegio Estatal de Fresno en California.

Los negocios que han intentado establecer programa apretados de seguridad han encontrado que la protección contra un saboteador es uno de los retos más difíciles. La Dow Chemicals recientemente fue atacada por un grupo radical asistido por un empleado. Con la ayuda de dicha persona, ellos pudieron entrar al cuarto de computadoras en un fin de semana y borraron todas las cintas magnéticas en la bóveda usando imanes de mano. Más de 1.000 cintas fueron borradas. Ellos también botaron cajones de tarjetas en pilas y escondieron los imanes en varias partes del cuarto.

Los imanes son armas populares para saboteador desde que un electroimán rápidamente borra una cinta cuando se le acerca. Las cintas no se necesitan sacar de sus estuches, así que un imán pasado cuidadosamente sobre un armario de cintas sería suficientes para borrarlos a todos.

Como es virtualmente imposible detectar la presencia de un imán en una instalación computarizada sin equipos costosos ($ 25 mil - $ 40 mil por instalación) la única solución factible es tener controles muy cerrados sobre las cintas. Esto significa que una persona debe estar presente todo el tiempo cuando la bóveda se abra. Muchas compañías tienen un bibliotecario en guardia durante el primer horario, pero luego la bóveda se mantiene abierta y desatendida el resto del tiempo.

Los centros de PED pueden ser destinados sin ganar acceso a las instalaciones o ni siquiera al edificio. El “Palacio de vidrio” o el centro PED es un blanco invitador para bombas incendiarias y otros proyectiles. El sucio, partículas de metal o aun gasolina, pueden ser echados en las entradas a nivel de tierra de los aires acondicionados. Líneas de comunicaciones o eléctricas pueden ser cortadas o hacer corto circuitos. Las bombas pueden ser ubicadas adyacentes al centro o si el computador es localizado en un edificio de multipisos, sobre el piso de arriba o debajo del centro de computación.

Empleados descontentos pueden ser particularmente peligrosos. El año pasado, un fabricante de productos farmaceúticos de New Jersey descubrió que sus archivos computarizados en – línea habían sido alterados por un empleado cesanteado a quien se le habían dado sus “últimas dos semanas”. La compañía ahora practica la “terminación inmediata” dentro de su centro de computación. La liquidación es aún pagada pero a la vez

de notificar al empleado de su despido, el empleado es escoltado fuera del edificio. Si el debe vaciar su oficina, lo hace ese día en presencia de un oficial de seguridad de planta.

MEDIDAS DE SEGURIDAD

1.- RESPALDO. DATOS DE SOFTWARE.

Los procedimiento de respaldo (back–up) son los elementos críticos en cualquier programa de seguridad de computadoras. El primer es identificar aquellos datos, información, software, documentación, etc., que son vitales a la organización y que deben ser protegidos para asegurar la salud continua de la organización. Algunas compañías tienen escalas complejas midiendo todos los datos dentro de varias clasificaciones de seguridad. La más simple y quizás el método más efectivo de todos es solo una clasificación entre “crítica” y “otros”. Todas las cosas juzgadas “criticas” son incluidas dentro del sistema de respaldo.

Un programa completo de respaldo debe incluir:

1.- ARCHIVOS DE DATOS.

Incluye archivos maestros de cintas magnéticas, archivos de cambios, depósitos de caracteres y discos, y tal vez los archivos de tarjetas perforadas.

2.- PROGRAMAS DE APLICACIONES.

Todos los programas de aplicaciones considerados “críticos” deben ser respaldados en su forma más recientemente auditada, incluyendo todos los arreglos y comandos.

3.- SOFTWARE DE SISTEMAS.

Ciertamente todo el software de costumbre será incluido, pero muchas organizaciones también duplican y guardan el software de vendedor más reciente, particularmente si este representa una cantidad sustancial de conveniencia a la instalación.

4.- DOCUMENTACIÓN DE PROGRAMAS.

Es tan necesario como los programas mismos, sin embargo, los centros PED que usan almacenamiento fuera de sitio fallan en considerar es el elemento importante.

5.- MANUALES DE OPERACIÓN, DIARIOS, BIBLIOTECAS, ETC.

La examinación cuidadosa a menudo produce otros documentos que son vitales a la operación continúa del centro de datos.

Es sorprendente como muchas organizaciones alcanzan con gran esfuerzo el almacenar algunas cosas y luego completamente ignoran otras de igual o mayor importancia. El sentido común va por un largo camino descubriendo tales debilidades. Por ejemplo, un fabricante de New Jersey mantenía una gran biblioteca de cintas en una bóveda a prueba de incendios. Todos los archivos importantes eran duplicados y enviados a otra compañía cada tres días. Un inventario sofisticado de cintas era mantenido por el bibliotecario de software. Aún así, el archivo de inventario y los listados fueron mantenidos en su escritorio. Fuera de la bóveda y ellos no tenían respaldo alguno. Todos los duplicados eran inútiles sin ese inventario de archivo diciendo lo que había en las cintas,

La forma más efectiva y menos costosa de respaldo es duplicar el almacenamiento fuera de sitio. La duplicación a menudo puede ser logrado con poco o quizás ningún costo adicional. La firma Iron Mountain Security Storage de New York aconseja el siguiente método:

"Si los datos a ser respaldados son actualizados sobre una base periódica, el viejo archivo maestro y los cambios pueden ser guardados sin costo adicional. Los cambios son frecuentemente ubicados primero en cinta y luego ordenados, antes de correr la actualización. La cinta no ordenada de cambio es una buena candidata para almacenarla fuera de sitio mientras que el archivo actualizado y ordenado puede ser dejado en el centro de datos".

De esta manera. La duplicación puede ser lograda sin procesamiento adicional, el cual puede ser particularmente importante para las organizaciones con grandes archivos o archivos que son frecuentes actualizados.

Las características más importante acerca de la ubicación fuera de sitio, es que sea remota del centro de datos. Servicios comerciales existen en muchas ciudades para proveer dicho almacenamiento o puede ser cumplido a través de la cooperación con una firma basada en intercambios. Muchas compañías con múltiples centros de PED intercambian archivos duplicados entre los centros.

Es importante que dichos arreglos sean seguidos rutinariamente. Un método de chequeo debería ser desarrollados para asegurar que el sistema de duplicación está operando como fue planeado y que los viajes al sitio de almacenamiento sean hechos como se planeó. Ejercicios de emergencia deberían ser conducidos sobre una base continua para validar el funcionamiento y condición del plan de respaldo.

2.- RESPALDO DEL HARDWARE.

Una vez fue considerado buena práctica el "respaldar" el hardware de computación, buscando un sistema compatible en la vecindad, el cual pudiera ser usado en caso de emergencia. En la práctica, está idea nunca trabajo muy bien, porque raramente se podía localizar un sistema compatible con capacidad disponible. Los sistemas de hardware están constantemente cambiando y la capacidad ociosa no existe. Actualmente, la posibilidad de respaldo genuino alcanza rápidamente a cero, tan pronto como las opciones del hardware y software crecen y el uso promedio de equipos se incrementa. Adicionalmente, debe ser notado que el uso de cualquier tipo de sistemas de comunicación de computadoras impide el respaldo.

Estudios recientes han sido conducidos bajo la factibilidad del concepto de "reserva ociosa", a través del cual un grupo de usuarios con sistemas aproximadamente compatibles, formarían una prueba conjunta para operar un sistema con el tamaño suficiente y las opciones disponibles para soportar las necesidades de todos los miembros del grupo. Este equipo estaría desocupado excepto por pruebas rutinarias del procedimiento de respaldo y quizás para procesamiento ocasional sobrecargado. El respaldo sería entonces garantizado para los miembros del grupo si uno de sus sistemas fuera destruido o se "cayera". El concepto parece tener mérito particular para compañías dentro de la misma industria, tales como bancos.

Quizás el único paso práctico que una compañía puede tomar, es tratar de desarrollar todos los programas críticos (nómina, control de inventario, horarios, etc.) para que ellos no usen lenguajes especiales, hardware, etc. y puedan ser corridos en los burós de servicios. Con la integración de archivos de sistemas y datos, esto se vuelve acrecentadamente difícil.

EL AUDITOR DEL SIGLO XXI

¿CÓMO FORMARLO?

Como nos aproximamos al siglo XXI. Muchos auditores esperan que aparezcan algo mágico para un cambio completo en el mundo de Auditoría:

- Hemos tenido una década de promesas para el nuevo siglo.
- Queremos cambiar la manera de hacer las cosas.
    - Cansado del SSDD, SSDG, SSDM
- Somos complacientes
    - Esperando que el "Nuevo auditor" aparezca mágicamente
- Esto no pasará
    - Para que los sueños lleguen a ser una realidad debemos implementar nueva tecnología.

- Ejemplo de motivación

1.- Las herramientas ya están aquí:

- La tecnología corriente será usada para crear el nuevo auditor:
  - Disponibilidad de microcomputadores de bajo costo.
  - Lenguaje de recuperación simplificador (SQL)
  - Entonces de inter-redes de multi-computador central.
  - Paquetes amigables del auditor
  - Renovaciones de Auditoría de Literatura de computador.

- Conceptos de Auditoría automatizada abundantes tanto en teoría como en práctica
  - Auditoría silenciosa
  - Auditoría remota
  - Programa investigativo
  - Sistemas de Auditoría
  - Bases de conocimiento

- Los mayores obstáculos que enfrentamos nosotros mismos:
  - Tendencia a retirarse famoso
  - Sobre énfasis en objetivos a corto plazo
  - Escasez de tiempo para “Procesos Pensados”

- Pensamiento hacia delante
- Pensamiento lateral
  - Falla de almacenamiento conveniente
  - Carencia de casos de negocios
  - Saltos gigantes versos pequeños pasos firmes
  - Productos total más bien que tareas de objetivos orientadas

- Resultado: La Gerencia no consolidará nuevos proyectos y estamos estancados en el mismo lugar
  - Le concierne a Ud. Hacer una diferencia
  - Ya hemos oído las excusas
  - “Porque yo. Permita que alguien más lo haga”
  - “Hemos tomado demasiado de mi plato”
  - “El jefe es demasiado anticuado. El no va con eso”
  - “Si soy automático. Estaré eliminando mi propio trabajo”
  - La razón real es que queremos hablar acerca de nuevas ideas. Tememos asumir el riesgo de implementarlas.

2.- La implementación del estamento mental

- "Si usted quiere el trabajo bien hecho. Hágalo ud. Mismo"
  - Primero usted: Debe aceptar su responsabilidad en crear el nuevo auditor.
  - Prepárese usted mismo para la tarea
- Investigación
- Desarrollar ideas
- Organizar presentaciones
- Crear plan de trabajo con muchos pasos pequeños
- Empezar con tareas fáciles. Elaborar tareas más difíciles.
- Preparar documentación de visión de Auditoría
- Presentación formal
- Yo he resumido el proceso: pero debe ser familiar para usted.
  - En el mismo proceso solo que los auditores recomiendan a otros

¿Debemos practicar lo que predicamos?

2.1.- Examinemos el estamento mental requerido

- Visión - Crear una imagen del nuevo auditor
- Foco - En los componentes críticos del auditor
- Investigación - Ver si el concepto es posible
- Inventario - Herramientas y productos existentes
- Desarrollo - Un cuadro del nuevo auditor
- Concentración - En aquellos aspectos que son alcanzables
- Documentación - Su plan si aceptara una forma de administración
- Mercadeo - Su plan y su habilidad para volver el plan una realidad
- Crear - El producto
- Implementar - En una base alternada gradual
- Evaluar - Los éxitos y fracasos
- Repetir - El proceso debe ser un lazo continuo
- Miremos esto en más detalle

3.- Creación del auditor del siglo XXI

3.1.- La visión

- El primer paso es parar y pensar libremente
  - Buena idea de la visión de lo que es el nuevo auditor
- ¿Qué rasgos diferentes de carácter quiere usted que tenga el nuevo auditor?
  - Mago técnico
  - Astuto politicamente
  - Sentido de negocios
  - Habilidad de contable
  - Habilidades especiales
  - ¿Otros?
- ¿Qué mezcla de carácter queremos nosotros?
- ¿Qué herramientas contemplamos?
  - Bancos de Taller
  - Enlaces de satélite
  - Sistemas expertos
  - Software etc.

- ¿Qué trabajo queremos ejecutar?
- ¿Dónde se hará el trabajo?
- ¿Qué espera la gerencia?

4.- Foco en componentes claves

- Una vez usted tenga la visión. Usted debe descomponerla en establecimiento de habilidades y herramientas requeridas.

- Foco en reducción de trabajo y aumento en cubrimiento de Auditoría.

- Desarrollar requerimientos externos para componente de habilidades críticas para el nuevo auditor

- Determinar que herramientas se necesitarán

  - Sentido de negocio
  - Creatividad
  - Conocimiento de Auditoría
  - Control orientado I.S.
  - Conocimiento del programa
  - Habilidad de escritura / Presentación
  - Habilidad eficaces técnicas
  - Flexibilidad
  - Noticias rápidas

- Persistencia
- Sofisticado
- Pensamiento hacia delante
- Mercadeo orientado

5.- Investigación

- Una vez usted sabe lo que le gustaría. Determine justo lo que es factible y lo que no es.

  - Coloque los artículos que usted estime factibles en su plan
  - Catalogue otras ideas para el archivo de “mañana”
- La investigación no es derecho hacia delante y una mente abierta
- La información esta disponible en muchos lugares
  - Otros departamentos de Auditoría
  - Las bibliotecas y universidades
  - El instituto de auditores EDP

6.- Inventario de productos útiles al nuevo auditor

- Los productos de software referentes a auditores deben ser rastreados.

- ACL
- FOCAUDIT
- PANAUDIT
- ETC.

- Suscribirse a los diarios de Auditoría y retomar las tarjetas de servicio.
  - Los proveedores le enviaran a usted sistemas (demostrativos)
  - Con frecuencia asistir a identificación de áreas donde los productos se pueden usar.
  - Suministrará lista de clientes.

- Desarrollar un inventario activo de productos y precios

- Mantener el inventario actual de tal manera que usted pueda tener solución empacada para requerimientos de la gerencia.

7.- Desarrollo de herramientas requeridas

- El siguiente paso es construir un banco de taller
  - Una cubierta de software que conecte las herramientas diseñadas a las necesidades de un individuo
  - Tratar de mantener estándares comunes pero deben considerarse requerimientos únicos.

- Algunos programas tendrán que ser desarrollados
  - Contratar un programador. No trate de hacerlo usted mismo.
  - Estudiantes de últimos grados o internos son una buena fuente de trabajo no costoso ellos también van al final del trabajo si están documentados apropiadamente. Usted puede ser capaz de vender su producto.

Ejemplo: Idea desarrollada por un auditor general para Canadá.

- Recuerde que una vez desarrollado el programa tendrá que ser sustentado.

8.- Concentración en lo que usted esta construyendo.

- Para ser exitoso ustedes debe permanecer en el curso
- No se permite a sí mismo desviarse
- Rompa el proyecto en pequeños trozos, módulos y concéntrese en completar cada trozo módulo a tiempo.
- Esto mantiene su entusiasmo elevado y permita a la gerencia ver el progreso.
- Esto asegurará fondos continuos

9.- Documente sus productos

- Para que el auditor del siglo XXI sea una realidad.
  Usted debe tener buena documentación

  - Asegúrese que las habilidades puedan ser verdaderamente inculcadas al personal existente.
  - Suministre instrucciones paso por paso. Así, ellos no sentirán frustados con los cambios.
  - Incluya un modulo de administración para asistirlos en la supervisión de adquisición de habilidades habilidad para detectar a aquellos que se retiran famosos.

10.- Mercadeo del auditor del siglo XXI

- Para que el auditor del siglo XXI llegue a ser una realidad. La idea debe venderse.
- Usted necesitará un plan de mercadeo y estrategia .
- La experiencia pasada muestra que es mejor tener un modelo demostrable antes de solicitar la aprobación de la gerencia.
  - Trabajar en casa creando un ejemplo del producto
  - Rastrear sus horas para varios productos
  - Asegúrese de documentar la curva de tiempo de aprendizaje separadamente.
- Una vez usted tenga varios programas de muestra.
  Construya un programa de mercadeo.
  - Donde las nuevas técnicas sean apropiadas
  - Ahorros de personal potencial

- Costo estimado para la primera fase de desarrollo
- Devolución inmediata estimada de la primera fase (TIR)
- Estimar derrotero de fases subsecuentes

- Para ser exitoso usted debe tener un pequeño equipo.
  Deseoso de trabajar duro.
  - La Gerencia no quiere invertir grandes sumas en personal adicional

11.- Creación e implementación del producto

- Esto sigue el ciclo normal de vida de desarrollo del sistema pero:
  - Recuerde mantener informado al Director de Auditoria.
  - Necesidad de transmitir productos frecuentemente
  - Rastrear ahorros en horas unid. Monet. (h/Bs).

12.- Evaluación y seguimiento permanente.

- Como en todos los proyectos. Los beneficios deben ser evaluados
- Sea realista. No todas las cosas trabajaran
- Asegúrese de identificar cualquier obstáculo
  - Personal
  - Equipo
  - Programas
  - Servicio
  - Etc.
- Su critica debe ser incluida en el estado de desarrollo (informes de avance o cortes)
- Asegúrese que todos los productos sean refinados
- Permita a los desarrolladores entender que trabaja y que no
- Proveer a la administración con información oportuna, exacta y significativa.

13.- Productos claves para el auditor del siglo XXI

- Banco de taller portátiles
- Paquetes de recuperación basados en PC.
- Bases de conocimiento
- Generación automática de reportes
- Sistemas de auto-Auditoría
- Auditoría silenciosa y remota
- Programa investigativo
- Sistema de Evaluación de Riesgos
- Administración del tiempo
- Interfases de plataforma múltiple
- Otros?

PROPUESTA PARA DIAGNOSTICO ORGANIZACIONAL

A continuación se presenta una propuesta del autor para la realización de un diagnostico organizacional.

Como ya se ha establecido, no se puede efectuar una auditoría si no existen procedimeintos o estándares contra los cuales constrastar la ejecución, en estos casos se realizaría un diagnóstico o una investigación. Lo más frecuente es un diagnóstico, pero a menudo los Auditores no han sido entrenados para este tipo de tarea, ni tienen idea de cuáles aspectos deben o pueden ser diagnósticados.

En el aparte siguiente se verán cuales aspectos pueden ser diagnósticados en una organización, ya sea en forma parcial o total.

1. ASPECTOS A SER DIAGNÓSTICADOS.

Para el diagnóstico de la organización se tomarían en cuenta los siguientes elementos o factores:

1.- Consideraciones generales:

- Antecedentes, evolución.
- Momento o situación actual y previsible.
- Dimensiones (actividades, recursos, etc.).

2.- Ambiente:

- Usuarios.
- Grupos de interés
- Relaciones con el entorno

3.- Gerencia:

- Liderazgo.
- Estilo gerencial dominante
- Estilos de decisión.
- Formas de participación.

4.- Estrategia:

- Misión de la organización.
- Objetivos.
- Estrategias.
- Políticas.
- Planes de largo, mediano y corto plazo.
- Presupuestos.
- Restricciones.

5.- Procesos:

- Principales procesos.
- Insumos.
- Servicios y/o productos.
- Tecnologías.

6.- Estructura:

- Criterios de estructuración.
- Funciones, responsabilidad principales.
- División del trabajo, especialización, diferenciación.
- Jerarquía y autoridad.
- Tramo de control.
- Mecanismos de integración.
- Usos de organizaciones ad-hoc y comités.
- Relaciones funcionales.
- Posiciones claves.
- Descripción de puestos.

7.- Sistemas:

- de planificación.
- De decisión.
- De administración.
- De control.
- De información.
- Ciclos de actividades.
- Procedimientos.

8.- Personal:

- Aspectos cuantitativos.
- Aspectos cualitativos.
- Aspectos demográficos.

- Adiestramiento.
- Desarrollo de carrera.
- Clima organizacional.
  ** Identificación con la organización.
  ** Motivación.

9.- Valores:

- Valores de la organización
- Símbolos.
- Rituales.
- Modelos.

10.- Infraestructura:

- Localización de actividades y recursos.
- Instalaciones (situación-ubicación)
- Equipos.

11.- METODOLOGIA.

a) Relevamiento de información. Se utilizará la técnica de la entrevista (especialmente en los niveles gerenciales) para relevar la información exigida por algunos de los elementos a ser estudiados. La aplicación de encuestas e instrumentos de diagnostico, en todos los niveles y la revisión documental que se considere necesaria.

b) Análisis de la información. A medida que se vaya relevando la información. Se procederá a efectuar los análisis correspondientes y preparar el informe sobre cada uno de los tópicos, que conformarán más tarde el informe final.

c) Informe y recomendaciones. El informe final contendrá los resultados del análisis y las recomendaciones para un plan de acción en función de los mismos.

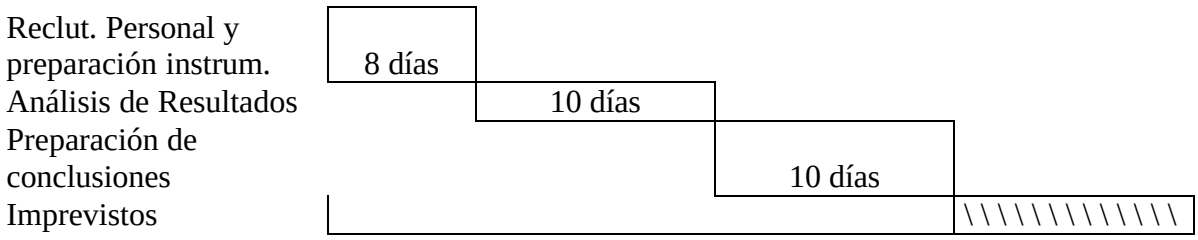
III. DURACIÓN.

El diagnóstico tendrá una duración de **bb** días hábiles, de acuerdo a la carta de Gannt anexa.

IV. COSTO.

El costo total del diagnóstico se estima en **xxxxxxxxmil bolivares (xx0.000,00Bs)** los cuales deberán ser cancelados por la Institución en dos partes, **50% al iniciar** el trabajo y **50% a la entrega del informe final.**

Carta de Actividades para el diagnóstico



METODOLOGIA PARA DISEÑAR CONTROLES DURANTE EL DESARROLLO DE UN NUEVO SISTEMA

¿QUÉ ES UNA AMENAZA?

Una **amenaza** se define como **un peligro potencial** o **un evento no buscado** que puede causar daño al sistema o a una organización. En otras palabras, una amenaza son actos que la organización busca prevenir para evitar perdida de sus activos.

¿QUÉ ES UN COMPONENTE?

Un **componente** se puede definir como una parte específica del sistema. Los componentes son los elementos sobre los cuales deseamos mantener controles.

Los componentes son piezas del sistema. La mayoría de la veces, los componentes son de naturaleza física.

¿CÓMO CONDUCIR UNA REVISIÓN DE CONTROLES?

PASO 1.- CREAR UNA MATRIZ DE CONTROL.

Amenazas / Componentes	Violación de Privacidad	Errores y omisiones	Acceso ilegal al sistema	Fraudes o Robos	Pérdidas o corrupción del mensaje	Desastres
Reportes		**1.2**		**6.7**	**1.2**	
Microcomput. o Terminales	**7.9**	**9.11**	**3.7**	**7.9**	**11**	**3.7**
Main o minicomputadores	**7**	**11**	**3.7**	**7**	**11**	**3.7**
Operadores de terminales	**12.13**	**1.2.3**	**12.13**	**12.13**	**12.11**	**13**
Circuitos de comunicación	**8**	**4**	**8**	**8**	**4.8**	
Archivos de bases de datos	**5.6**	**1.2.7.9**	**5.6.10**	**5.6.7**	**1.2.7.13**	**3**
Programas	**5.6**	**11**	**3.5.6.10**	**5.6.7**	**11**	**3**

Los controles se toman del libro sobre matrices de control de Fitzgerald, Jerry. También se pueden ir generando otros controles para complementar estas matrices, a medida que se tienen experiencias con diferentes sistemas.

Como puede verse la matriz de control está construida en función de las amenazas y los componentes del sistema.

Los controles contenidos en la matriz deben disminuir o detener las amenazas y salvaguardar o restringir los componentes identificados en el paso uno.

PASO 2.- EFECTUAR ANALISIS DE RIESGOS TANTO DE AMENAZAS COMO DE COMPONENTES

Para tal fin se utilizan las matrices que se muestran a continuación, y se aplica la técnica **DELPHI,** si los posibles **Técnica del Grupo Nominal** si se pueden reunir en la misma organización. El uso de estas técnicas tiene como finalidad evitar las discusiones y otros inconvenientes derivados de las reuniones o **grupos interactivos.**

Comparación de Riesgos Amenazas

	3					
Violación de Privacidad	**Violación de Privacidad**	**18**				
Errores y Omisiones	**1** **4**	**Errores y Omisiones**	**12**			
Acceso Ilegal al Sistema	**0.5** **4.5**	**4** **1**	**Acceso Ilegal al Sistema**	**13**		
Fraude y Robo	**1.5** **3.5**	**3** **2**	**2.5** **2.5**	**Fraude y Robo**	**9**	
Pérdida y corrupción de Mens.	**0** **5**	**4** **1**	**4** **1**	**4** **1**	**Pérdida y corrupción de Mens.**	**20**
Desastres	**0** **5**	**3** **2**	**0** **5**	**1** **4**	**1** **4**	**Desastres**

Comparación de Riesgos Componentes

Reportes	**Reportes**						
		75					
Micros o Terminales	**3** / **2**	**Micros o Terminales**	**140**				
Main o Mini	**6** / **0**	**1** / **4**	**Main o Mini**	**95**			
Operador de Terminal	**2** / **3**	**2.5** / **2.5**	**4** / **1**	**Operador de Terminal**	**105**		
Circuito Comunicación	**0.5** / **4.5**	**0** / **5**	**3** / **2**	**1** / **4**	**Circuito Comunicación**	**25**	
Archivo Base de Datos	**0** / **5**	**0** / **5**	**1** / **4**	**1** / **4**	**2** / **3**	**Archivo Base de Datos**	**19**
Programas	**1** / **4**	**2** / **3**	**2** / **3**	**1** / **4**	**1** / **4**	**4** / **1**	**Programas**

Observe que los valores colocados en las casillas son valores promedio obtenidos en las votaciones, de allí la aparición de números decimales.

Amenazas / Componentes	Desastres	Errores y omisiones	Fraudes o robos	Acceso ilegal	Pérdidas del mensaje	Violacion de privacidad
Archivos de Bases de Datos						
Programas						
Circuitos de comunicación						
Main o minicomputadores						
Reportes						
Operadores de terminales						
Microcomputadores o terminales						

Paso 3.- Realizar un análisis de riesgos

Para realizar el mismo se procede a vaciar los valores de resumen obtenidos en las dos matrices anteriores, en los rubros identificados tanto en componentes como en riesgos. (Ver valores colocados en amenazas y componentes).

Observe que tanto las **amenazas** como los **componentes** se ha reordenado en forma decreciente de acuerdo a esos valores.

Luego se **multiplican** los valores de **amenazas y componentes** y los resultados se colocan en las casillas correspondientes.

Se obtiene una nueva matriz como la se muestra a continuación.

Amenazas / Componentes	Desastres (20.0)	Errores y omisiones (18.0)	Fraudes o robos (13.0)	Acceso ilegal al sistema (12.0)	Pérdidas del mensaje (9.0)	Violación de privacidad (3.0)
Bases de datos (25.0)	**500**	**450**	**325**	**300**	**225**	**75**
Programas (19.0)	**380**	**342**	**247**	**228**	**171**	**57**
Circuitos de comunicación (18.5)	**370**	**333**	**240.5**	**222**	**166.5**	**55.5**
Main o Mini computadores (14.5)	**280**	**252**	**182**	**168**	**126**	**42**
Reportes (11.5)	**230**	**207**	**149.5**	**138**	**103.5**	**34.5**
Operadores de Terminales (9.5)	**190**	**171**	**123.5**	**114**	**85.5**	**28.5**
Micros o Terminales (7.5)	**150**	**135**	**97.5**	**90**	**67.5**	**22.5**

Paso 4 .- Se Jerarquizan Los Riesgos

Se procede a numerar en orden creciente las casillas con los valores de riesgos y luego se separan en zonas perfectamente delimitadas de ALTO, MEDIO Y BAJO RIESGO.

En el gráfico siguiente se puede ver el resultado final.

Sin embargo, una casilla colocada en una de las zonas puede ser jerarquizada de nuevo, haciendo una matriz para ella en función de determinados factores y volviendo a repetir el proceso.

Amenazas / Componentes	Desastres	Errores y omisiones	Fraudes o robos	Acceso ilegal al sistema	Pérdidas del mensaje	Violación de privacidad
Archivos de Bases de datos	**1** **500**	**2** **450**	**7**	**8**	**15** **225**	**34** **75**
Programas	**3** **380**	**5** **342**	**11** **247**	**14** **228**	**20** **171**	**36** **57**
Circuitos de comunicación	**4** **370**	**6** **333**	**12** **240.5**	**16** **222**	**22** **166.5**	**37** **55.5**
Main o Mini computadores	**9** **230**	**10** **252**	**19** **182**	**21** **138**	**27** **126**	**38** **42**
Reportes	**13** **230**	**17** **207**	**24** **149.5**	**25** **138**	**30** **103.5**	**39** **34.5**
Operadores de Terminales	**18** **190**	**20** **171**	**28** **123.5**	**29** **114**	**33** **85.5**	**40**
Micros o Terminales	**23** **150**	**26** **135**	**31** **975**	**32** **90**	**35**	**41** **22.5**

ALTO

MEDIO

BAJO

Paso 5. Evaluar los Controles

Para evaluar la eficiencia y los **costos/beneficios** de los controles que fueron diseñados para el nuevo sistema se debe escribir un informe que diga cuando deben ser usados y probados los controles (en fase de programación, prueba e implantación del nuevo sistema).

Paso 6. **Verificar y probar los controles**

Verificar y probar los controles diseñados para el nuevo sistema con la finalidad de garantizar su funcionamiento apropiado.

Paso No. 1
AMENAZAS
VIOLACIÓN DE PRIVACIDAD

Acceso no autorizado a datos confidenciales.

ERRORES Y OMISIONES

Errores que ocurren durante la preparación de los documentos, procesamiento o salidas del sistema.

ACCESO ILEGAL AL SISTEMA

Desautorizado acceso a las bases de datos, redes, programas de computación, documentos sensitivos y otros.

FRAUDES O ROBOS

El robo de los datos de organización o de otros documentos, tanto manuales o computarizados o de la red de la organización.

DESASTRES Y DESTRUCCIONES

Desastres físicos, incluyendo incendios, inundaciones, fallas eléctricas, terremotos y otros de la misma naturaleza.

COMPONENTES

REPORTES

Reportes y archivos manuales, documentos, etc.

MICROCOMPUTADORES O TERMINALES

Microcomputadores centrales, discos y unidades de cintas, y otros dispositivos relacionados con el hardware.
OPERADORES DE TERMINALES

Operadores de terminales, empleados temporales, otros empleados o personas de otros lugares quienes tienen acceso a terminales de la organización.

CIRCUITOS DE COMUNICACIÓN

Circuitos de comunicación que conectan a la organización a amplias áreas de redes (WANs) o la redes locales (LANs).

ARCHIVOS DE BASE DE DATOS

La organización de los datos en los dispositivos de almacenamiento, los gabinetes de archivos, o en los sitios de almacenamiento de larga duración (archivos históricos).

PROGRAMAS

Ambos programas de aplicación y software del mainframe o microputadores.

PASOS No. 2 Y 3

Estos dos pasos se realizan simultáneamente.

Estas son las dos preguntas que debemos realizar:

¿Cuáles amenazas puede este control ayudar a disminuir o parar?

¿Cuáles componentes puede este control ayudar a salvaguardar o restringir?

PASOS No. 4

Conduciendo un análisis de riesgos.

PASOS No. 5

Evaluando la eficiencia costo/beneficio de los controles.

Evaluar cada amenaza, componente y celda tomando en cuenta los siguientes cinco criterios.

1. **Eficiencia del control**
2. **Grado de riesgo (alto, medio, bajo)**
3. **Controles preventivos**
4. **Controles detectivos**
5. **Controles correctivos**

Una vez aplicado el DELPHI o la TGN se computan los votos

AMENAZAS

ITEM	VOTO TOTAL
Desastre	20
Error u omisión	18
Fraude y robo	13
Acceso ilegal	12
Pérdida y corrupción de mensaje	9
Violación de privacidad	3

COMPONENTES

ITEM	VOTO TOTAL
Base de datos	25
Programas	19
Circuito de comunicación	18,5
Main y Mini	14
Reportes	11,5
Operadores de terminal	9,5
Micros y terminales	7,5

luego se procede a llenar las matrices como se explico anteriormente para determinar las zonas de **alto medio y bajo riesgo.**

BIBLIOGRAFIA

1.- Cano Pérez y Asociados. **Auditoría de Sistemas de Información.** Mimeografiado. Valencia. 1987

2.- Fitzgerald, Jerry. **Controles Internos para sistemas de Computación.** Limusa Wiley. California 1982

3.- Fabregas, Llorens. **Control de Calidad de Sistemas.** Edit. Reverte. Valencia 1988

4.- Lott, Richard W. **Auditoría y Control de Procesamiento de Datos.** Edit. Norma. México. 1984.

5.- Thierauf. Roberat J. **Auditoría Administrativa.** Limusa Wiley. México. 1986.

6.- Thomas, A. J. Y Douglas, I. J. **Auditoría Informática.** Editorial Paraninfo. Madrid. 1988.

7.- Skinner R. M. Y Anderson R. J. **Auditoría (La censura de cuentas mediante diagramas dinámicos).** Edit. Anaya. Madrid. 1980.