AUDITORIA

* INTERNA: la empresa tiene un área que asegura que se cumplan los controles y normas. Los auditores no pueden cumplir tareas operativas y conocen bien el negocio.
* EXTERNA: reasegura que los controles puestos en cada una de las aéreas se cumplan y sirvan, y que los estados financieros reflejen la realidad. Auditan la razonabilidad de los estados contables, comparando los balances anteriores con el actual y el proyectado

RIESGOS

* Estratégicos: son aquellos que corre la gerencia para mantenerse en el mercado. Hacen al corazón del negocio. No se pueden cambiar ni auditar
* Inherentes: es la susceptibilidad a errores o irregularidades que dependen de la naturaleza del negocio. Ejemplo: cosas que no puedo no hacer 🡪 Facultad, no puede no enseñar. No se eliminan siempre, a los sumo se baja el nivel de riesgo. Se evalúa la naturaleza del negocio, de los componentes y de los sistemas de información
* Control: es cuando los sistemas de control en vigencia no pueden detectar o evitar errores o irregularidades en forma oportuna.
  + Generales: propios del entorno y del área de sistemas
  + Directos: propios de la aplicación

CONTROLES

Para ser efectivo un sistema de control debe:

* Ocuparse de los riesgos inherentes percibidos
* Incorporar una adecuada segregación de funciones incompatibles
* Poseer un alto grado de cumplimiento

Grupos de control

* Interno: analiza el MN y P para ver si esta vigente o si hay que actualizarlo. Revisa y verifica que los controles se cumplan
* Estados contables: analiza los balances y proyecciones
* Control interno sistemático: audita los sistemas y procesos, seguridad.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Control Interno | Estados Contables | Control Interno Sistemático |
| Interno | X | --- | X\* |
| Externo | X\* | X | X |

X\*: hay que capacitarlos fuertemente

AUDITOR

* Tiene que tener documentación de respaldo
* Fundamentarse en hechos
* Ser independiente de la empresa y sin intereses en común
* Ubicado en alto rango en la empresa

MAPA DE RIESGO

En base a esto se planifica la auditoria. Se le da relevancia a cada proceso de negocio

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| RELEVANCIA DEL PROCESO DE NEGOCIO |  |  |  |  |
| ALTO |  | **ZONA DE TERAPIA** | **ZONA DE MUERTE** |  |
| MEDIO |  |  | **ZONA DE TERAPIA** |  |
| BAJO |  |  |  |  |
|  | ADECUADO | MEJORABLE | DEBIL | ESTADO DE CONTROL |

La Zona de Muerte es donde el ciclo más importante de la empresa tiene el control más Débil.

En base a esto se planifica la auditoria que se comunica al gerente del área. Se arma el plan con cada circuito, tiempo, recursos, programación de trabajo, etcétera.Además este maneja información confidencial; es un acuerdo entre auditoría y el gerente de las distintas áreas.

Ejemplo: Si Producción y Compras están en la zona de muerte, intervienen

**A-**Sistemas y **B-**Finanzas. Así como está, el año siguiente Producción y Compras no deben estar en la zona de muerte. Entonces el objetivo será achicar el Riesgo de Control.

TIPOS DE CONTROLES

* Preventivos: identifican el riesgo antes de que se produzca. Son aquellos que reducen la frecuencia con que ocurren las causas del riesgo, permitiendo cierto margen de violaciones.
* Detectivos: una vez materializado el riesgo, ahí lo detecto. Son más importantes para el auditor. En cierta forma sirven para evaluar la eficiencia de los controles preventivos. Por ejemplo: “Que los precios a pagar sean correctos!” “Proveedores que entregan mercadería 🡪Pago, pero si encuentro un problema de Calidad 🡪 reclamo al proveedor!”
* Correctivos: posterior al riesgo, para corregirlo

CATEGORIAS DE CONTROL INTERNO

* Ambiente de sistemas de información
* Ambiente de control
* Controles generales: son aquellos que contribuyen a la efectividad de los controles directos
* Controles directos: son aquellos diseñados para evitar o detectar errores o irregularidades que afectarían la información generada por el sistema

DIFERENCIA ENTRE CONTROLES DIRECTOS Y GENERALES

La efectividad de los controles directos depende de los controles generales pero estos últimos por si solos no proporcionan satisfacción a la auditoria.

DIFERENCIA ENTRE CONTROLES DIRECTOS Y FUNCIONES COMPUTARIZADAS

Algunas funciones de procesamiento (edición, validación, etc.) también representan controles ya que son diseñados para evitar o detectar errores o irregularidades y otras no.

EL COSTO DEL CONTROL DEBE SER MENOR QUE EL COSTO DE OCURRENCIA DEL RIESGO

PLANIFICACION DE LA AUDITORIA

Uno de los primeros puntos a considerar es a la obtención de un conocimiento global del ente objeto de auditoria:

* Ambiente de sistemas de la información
  + Estructura organizativa de las operaciones del sistema
  + Naturaleza de la configuración de los sistemas (principales centros de proceso, lugar, interconexión)
  + Naturaleza y alcance del procesamiento computarizado para las principales aéreas del negocio (Objetivo del sistema, interfaces, volumen de transacciones)
* Ambiente de control: conjuntos de condiciones en el cual operan los sistemas de control. Es función de la gerencia del departamento de sistemas crear y mantener el ambiente de control. Algunos temas importantes son:
  + Enfoque hacia el control por parte del directorio y la gerencia superior
  + Organización gerencial
  + Marco para el control gerencial

PLAN DE TRABAJO

Objetivo

Alcance

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Riesgo asociado | Objetivo de control | Control a relevar | Pruebas | Efectividad del control | Observaciones | Work paper |
| Pasar a producción algo con fallas | Todos los cambios a programas se prueban y aprueban antes de la PO | Procedimiento de cambios de los programas | Que hacer para probar el riesgo | Probar el control, obtener evidencia de que el control es efectivo, se toman muestras | Lo que produce la efectividad del control | Modificaciones realizadas |

DESARROLLO DE LA AUDITORIA

Una vez obtenida la visión global del ente es posible determinar cuales son los sistemas y/o aspectos a auditar:

* Los riesgos relacionados con el entorno de procesamiento se mitigan con controles generales
* Los riesgos relacionados con cada aplicación se mitigan con controles directos

CONTROLES GENERALES

1. Estructura organizativa del área de sistemas

Puede que el entorno no contribuya a generación de datos confiables para esto deben estar definidos los roles.

DBA: no tiene acceso a los datos. Se encarga de la performance, crecimiento de la base, deadlocks, table spaces, e implementa cambios.

Aplicaciones (Desarrolladores)

* No pueden poner en marcha la computadora
* No deben tener acceso a producción

Operadores

* No pueden hacer cambios de programa ni datos

Sistemas

* No debe iniciar y aprobar transacciones ni acceder a la documentación

En general se analiza:

* los empleados no realicen funciones incompatibles
* las actividades de los encargados de soporte técnico y otros empleados técnicamente capacitados sean supervisados y la utilización del software sensitivo sea controlado

Controles compensatorios

* Responsabilizan a departamentos de usuarios de una adecuada supervisión de los informes de salida
* Supervisión permanente de las operaciones del computador y del uso de utilitarios
* Controles sobre accesos físicos
* Desarrollo de programas
* Manuales de operación y controles operativos diarios
* Supervisión de usuarios privilegiados
* Control sobre software sensitivo

1. Procedimientos de cambios a los programas

Incluye las tareas necesarias para que el software continúe operativo y adaptarlo a los cambiantes requerimientos del usuario.

Debe incluir

1. Motivo para el cambio (Documentado y aprobado)
2. Cambios introducidos primero en testing y no en producción
3. Cambios realizados por personal de sistemas o programación (no operadores o usuarios)
4. Cambios respaldados por documentación
5. Pruebas deben ser realizadas primero por los programadores
6. Procedimientos de catalogación de cambios que se introducen en versiones de prueba

Los datos son transferidos por el DBA

Los fuentes son transferidos por el administrador de servidores

Controles sobre cambios a los programas

* Iniciación, aprobación, documentación
* Procedimientos de pruebas
* Procedimientos de implantación
* Es recomendable utilización de soft de control de versiones
* Es recomendable utilización de soft de comparación de código fuente
* Mantenimiento
* Segregación de funciones

Metodologías CMMI, ITIL

1. Acceso general (a los datos o programa de aplicación)

Personas no autorizadas pueden hacer cambios en datos o programas.

Análisis de controles

* Identificación de usuario y contraseña
* No uso de usuario compartido
* Las contraseñas no son efectivas sino son confidenciales
* Software de control de acceso (recomendado)
* Software de control de acceso solo, no garantiza la confidencialidad

Controles

1. Restringir acceso en base a perfiles de seguridad
2. Definir funciones autorizadas para cada persona
3. Supervisar y registrar determinadas actividades y generar informes de acceso, interrupciones, intentos fallidos de acceso
4. Restricción de acceso físico

Perfiles sugeridos de acceso a recursos

1. Continuidad de procesamiento

Planificación de tareas a desarrollar ante una contingencia es responsabilidad de la gerencia superior.

Evaluación y clasificación de riesgos

* Críticos: funciones que no podrán ser realizadas salvo que se reemplacen por otras iguales
* Vitales: pueden hacerse manualmente por un periodo corto
* Sensibles: pueden hacerse manualmente por un periodo largo
* No criticas: pueden ser interrumpidas. Poco esfuerzo para ponerse al día.

Requerimientos de plan de continuidad

1. Lapso critico de recuperación (sin incurrir en perdidas)
2. Aplicaciones a recuperar dentro del lapso critico
3. Interrelación entre usuarios y procedimientos de datos (tal vez el usuario tenga que procesar datos una vez que se reanude la aplicación)
4. Prioridades de procesamiento
5. Instrucciones de cómo activar y usar el plan para cada área
6. Procedimientos detallados para la recuperación de cada área
7. Procedimientos formales para mantener actualizado el plan
8. Contemplar distintos escenarios para cada nivel de interrupción

Hardware alternativo y necesidades de software

* Hot sites: centros configurados y listos para operar en forma inmediata, con la información y los datos al día
* Warm sites: parcialmente configurados, con periféricos pero sin computador central, tienen CPUs de menor performance. Lapso corto.
* Cold sites: tienen el ambiente básico (cableado, aire acondicionado)
* Centro duplicado de procesamiento: sedes auto desarrollado que ofrecen backup a aplicaciones. Entre organizaciones similares
* Acuerdos recíprocos: contratos entre una o mas organizaciones con equipos similares

CONTROLES DIRECTOS

Para cada aplicación significativa se deben evaluar los riesgos relacionados con ella en forma independiente

Riesgos

1. Personas no autorizadas tengan acceso a la aplicación o datos

Puede reducirse si:

* Hay segregación de funciones incompatibles
* Control de accesos

Métodos: perfiles, MNyP, menús, acceso por programas

1. Datos o transacciones incorrectas, incompletas o duplicadas

Datos fijos: no se modifican con la operatoria diaria

* Datos de referencia general (dirección, teléfono)
* Datos contables

Se revisan en el momento de ingreso. Se utilizan rutinas para editar y validar datos fijos

Controles de edición y validación

* Formato
* Campos faltantes
* Limite y razonabilidad
* Validación (datos ingresados sean compatibles con datos maestros)
* Procesamiento duplicado
* Pruebas de correlación de campo (comparan datos diferente para probar su razonabilidad en base a criterios establecidos por ejemplo, el personal ejecutivo no le liquidan horas extras)
* Balanceo
* Digito verificador
* Doble ingreso o confirmación
* Controles de lote
* Conciliación del input se produce resumen de datos aceptados y rechazados
* Informes de control (confirma si los datos han sido procesados)

1. Datos rechazados o transacciones suspendidas

Se debe controlar cada transacción rechazada manteniendo un registro de la misma hasta que sea corregida, por el usuario apropiado que tome las medidas necesarias. Al ser reingresadas deben ser sometidas a los mismos procesos de validación.

Estos pueden ser

* Aceptada por el sistema e incluidos en una informe de excepción
* Incluido en archivo de partidas en suspenso dentro del sistema
* Completamente rechazados

1. Transacciones ingresadas en periodo contable incorrecto

Controles

* Formularios pre-numerados
* Controles de balanceo (asegurar exactitud e integridad de los datos)
  + Controles
    - Ciclo a ciclo
    - De actualización de archivos
    - Programa a programa
* Controles de lote
* Controles de rótulos internos de archivo
* Controles de transmisión de datos
* Procedimientos de reenganche y recuperación
* Controles de corte programados

INFORME DETALLADO

* Objetivo
* Riesgos encontrados
* Opinión
* Cursos de acción
* Responsable de soluciones

INFORME SINTETICO

* Situación actual
* Objetivo
* Alcance
* Diagnostico
* Principales cursos de acción