Auditoria

RAZONES PARA CONTROLAR

1. COSTOS POR PÉRDIDAS DE DATOS

“Los datos proveen a la organización de una imagen de sí misma, de su entorno, de su historia, y su futuro”. Si la imagen es exacta, la organización aumenta las posibilidades de adaptarse y sobrevivir a un entorno cambiante. Si la imagen es inexacta, se puede incurrir en pérdidas sustanciales.

2. COSTOS POR DECISIONES INCORRECTAS

La alta calidad en la toma de decisiones depende, en parte, de:
• la calidad de los datos,
• la calidad de las reglas de decisión que existen en los SI automatizados.
La importancia de datos exactos depende del tipo de decisiones hechas por personas que tienen algún interés en la organización.
Alta Gerencia → decisiones de planeamiento estratégico → probablemente acepten algunos errores en los datos
Gerencia Media → decisiones de control administrativo y de control operativo → requieren datos más exactos

El tener reglas de decisión exactas en un sistema de información (SI) depende del tipo de decisiones hechas por personas que tienen algún interés en la organización.

3. COSTOS POR ABUSO COMPUTACIONAL

Definición: un abuso computacional es un incidente asociado con tecnología informática, en el cual una víctima sufre o podría haber sufrido pérdida, y un perpetrador con intención logra o podría lograr ganancia
El promedio de pérdidas por abusos computacionales pareciera ser sustancialmente mayor que las pérdidas producidas por fraudes convencionales.

Tipos de abusos:
1) hacking: Una persona logra un acceso no autorizado a un sistema de computación para leer, modificar o borrar datos o programas para discontinuar un servicio.
2) virus: Son programas que atacan a archivos ejecutables, áreas del sistema, o archivos de datos que contienen macros, para causar una disfunción en las operaciones computacionales o dañar datos y programas [Nachenberg, 1997].
3) acceso físico ilegal; Una persona logra un acceso físico no autorizado a facilidades del computador. Como resultado, pueden causar daño físico al hardware o hacer copias no autorizadas de programas y datos
4) abuso de privilegios: Una persona usa privilegios, que le han sido asignados, para propósitos no autorizados.

CONSECUENCIAS DE ABUSOS
a) Destrucción de activos.
b) Sustracción de activos.
c) Modificación de activos.
d) Violación de privacidad.
e) Interrupción de operaciones.
f) Uso no autorizado de activos.
g) Daño físico a personas.

4. COSTOS POR ERRORES DE COMPUTACIÓN
Los costos por un error de computación pueden ser altos, en términos de:
1) pérdida de vida humana,
2) privación de libertad,
3) daño al medio ambiente.

5. VALOR DE HW, SW Y PERSONAL
Recursos críticos en las organizaciones:
1) Datos - ¿qué pasa si la competencia obtiene información confidencial?
2) Hardware - ¿qué pasa si un componente crítico deja de funcionar?
3) Software - ¿qué pasa si se destruye?
4) Personal - ¿qué pasa si un profesional calificado deja la empresa?

6. MANTENIMIENTO DE PRIVACIDAD
Muchos datos se recolectan sobre los individuos: impuestos, obras sociales, trabajo, residencia.
Con sistemas automatizados se puede integrar y buscar información.
Se podrían utilizar datos de genética humana para obtener información detallada sobre una persona y usarla en su contra.

7. EVOLUCIÓN CONTROLADA DEL USO
Se argumenta que la confiabilidad de los sistemas computarizados complejos no está garantizada.
Las consecuencias de usar sistemas no confiables puede ser catastrófica.
¿Qué efectos físicos y mentales tienen las computadoras en los usuarios?
Debe existir interés para evaluar y controlar la implementación de esta tecnología.

AUDITORÍA DE SISTEMAS DE INFORMACIÓN

Definición:
La auditoría de sistemas de información es el proceso de recolectar y evaluar evidencia para determinar si:
1) el sistema automático preserva los activos,
2) mantiene la integridad de los datos,
3) permite que los objetivos organizacionales se alcancen con eficacia,
4) usa los recursos con eficiencia.

Muchas veces la auditoría tiene otro propósito: asegurar que la organización cumple con determinadas regulaciones, reglas y condiciones, ya sea voluntaria o involuntariamente.

IMPACTO DE LA AUDITORÍA EN SI

1. SALVAGUARDA DE ACTIVOS
Los activos de los SI incluyen: hardware, software, facilidades, personas (conocimientos), archivos de datos, documentación de sistemas, insumos...

2. INTEGRIDAD DE LOS DATOS
Es un estado que en el cuál los datos poseen ciertos atributos:
- ✔ completitud
- ✔ consistencia
- ✔ veracidad
- ✔ correctitud

Si la integridad de los datos de una organización no es mantenida, no posee representación de sí misma o de los eventos. Sin integridad de datos se pueden producir pérdidas de ventajas competitivas.

El valor de un dato depende de:
1) el valor del contenido informacional de un ítem de dato para los tomadores de decisiones
[El contenido informacional de un ítem de dato se refiere a cuánto puede aportar el dato para modificar el nivel de incertidumbre que envuelve a una decisión]
2) el grado en el cuál el ítem de dato es compartido entre los tomadores de decisiones
3) el valor del ítem de dato para los competidores

3. EFECTIVIDAD DE LOS SISTEMAS

Un sistema de información es efectivo si satisface sus objetivos.
Formas de evaluar la efectividad de los sistemas:

1) durante el proceso de desarrollo para garantizar que se satisfacen los requerimientos de los usuarios
2) mediante una post-auditoría

Para poder evaluar la efectividad de un sistema de información se deben conocer:

1) las características de los usuarios,
2) el entorno de toma de decisiones .

4. EFICIENCIA DE LOS SISTEMAS

Un SI es eficiente si usa los recursos mínimos para satisfacer sus objetivos. Recursos de un sistema de información:

- ✔ tiempo de procesador
- ✔ periféricos
- ✔ software
- ✔ trabajo manual

Muchas veces el uso de los recursos no se puede estudiar con respecto a un sólo sistema. Generalmente, la eficiencia se estudia cuando se agotan los recursos.

Los objetivos de la auditoría sólo se pueden lograr si la alta gerencia implementa un sistema de control interno.

SISTEMA DE CONTROL INTERNO

Un sistema de control interno incluye:
1) separación de obligaciones,
2) delegación clara de autoridad y responsabilidades,
3) reclutamiento y entrenamiento de personal calificado,
4) sistema de autorizaciones,
5) documentos y registros adecuados,
6) control físico y documentación sobre los activos,
7) chequeos independientes de performance,
8) comparación periódica de activos con registros contabilizados

El uso de computadoras afecta de varias maneras la implementación de los componentes de un sistema de control interno.

1) SEPARACIÓN DE OBLIGACIONES

En un sistema manual, personas diferentes deben realizar las tareas de iniciar la transacción, registrar la transacción, y prevenir errores o detectar irregularidades
En un sistema automatizado, es el mismo programa el que realiza todas las funciones.
En los sistemas automatizados, la separación de obligaciones se aplica distinto: se tiene que separar la capacidad de ejecutar el programa, de la capacidad de modificar el programa.

2) DELEGACIÓN
Una delegación clara de autoridad y responsabilidad es esencial tanto en sistemas manuales como automatizados.
En un sistema automatizado, hacer esto de una manera no ambigua puede ser dificultoso.

3) PERSONAL COMPETENTE Y CONFIABLE
A las personas responsables de desarrollar, implementar y operar los sistemas de información se les delega mucho poder. El personal responsable de los sistemas automatizados tiene delegado mayor poder que los empleados que realizan tareas manuales.

No es fácil para las organizaciones asegurar que el personal de sistemas sea competente y confiable.
La alta rotación de este personal es común.
La gerencia tiene poco tiempo para evaluar a este personal.
El rápido desarrollo de la tecnología inhibe a la gerencia de evaluar el perfil de este personal.

4) SISTEMA DE AUTORIZACIONES
La gerencia debe establecer dos tipos de autorizaciones:
1) autorizaciones generales: establecen las políticas que la organización debe seguir.
2) autorizaciones específicas: aplicables a transacciones individuales.
En los sistemas automatizados las autorizaciones están embebidas dentro de los programas.
Los auditores deben controlar las autorizaciones definidas en los procedimientos, como así también la veracidad del procesamiento de los programas.

5) DOCUMENTOS Y REGISTROS
Se debe asegurar que los documentos y registros sean adecuados.
En un sistema automatizado no es necesario un documento para iniciar una transacción.
En un sistema bien diseñado debería haber mayores registros de auditoría que en un sistema manual
Se deben prever controles de acceso y facilidades de acceso (login) para asegurar que los rastros de auditoría sean exactos y completos.

6) CONTROL DE ACCESO FÍSICO
El control de acceso físico a los activos y a los registros es crucial, tanto en sistemas manuales como automáticos. Diferencia:
• sistema manual: puede tener que acceder a varios sitios
• sistema automatizado: todos los registros necesarios se pueden mantener en un sólo lugar.
La concentración de información aumenta la posibilidad de pérdida que puede surgir por abuso o desastre.

SUPERVISIÓN GERENCIAL ADECUADA
En sistemas manuales se facilita, ya que empleados y supervisores, generalmente, comparten el lugar físico.
En sistemas automatizados, las comunicaciones permiten que los empleados estén cerca de los clientes. La supervisión se debe llevar a cabo en forma remota.
Los controles para supervisión deben estar construidos dentro del sistema.
El gerente debe acceder a los registros de auditoría para evaluar la gestión de los empleados.

7) CHEQUEOS DE PERFORMANCE

En sistemas manuales, los chequeos realizados por otra persona ayudan a detectar errores o irregularidades.
En sistemas automatizados, los programas siempre ejecutan el mismo algoritmo, a excepción de una falla de hardware o de software.
Los auditores deben evaluar los controles establecidos para desarrollar, modificar, operar y mantener programas.

8) COMPARACIÓN PERIÓDICA

Periódicamente, se deben controlar los datos que representan los activos con los activos reales, a fin de determinar falta de completitud o inexactitud de los datos.
En sistemas automatizados se deben preparar programas para que hagan esto.
Son importantes la implementación de estos controles durante el desarrollo de sistemas.

LA COMPUTACIÓN EN AUDITORÍA

La función de auditoría no cambia. En sistemas automatizados es más complicado recolectar evidencia. Es más difícil evaluar las consecuencias de las fortalezas y debilidades de los controles en pro de la confiabilidad general del sistema.

Los errores en los sistemas manuales tienden a ser estocásticos. Ejemplo: periódicamente el empleado se equivoca al actualizar un precio.
Los errores en los sistemas automáticos:
1) tienden a ser determinísticos
2) se generan a mayor velocidad
3) es mas costoso arreglarlos
Los controles internos que aseguran la alta calidad en el diseño, implementación, operación y mantenimiento de los sistemas, son críticos.

FUNDAMENTOS DE LA AUDITORÍA

AUDITORÍA TRADICIONAL

Aporta conocimientos y experiencia sobre técnicas de control interno. Aporta la filosofía de los controles. Ejemplo: los programas deben asegurar que todas las transacciones fueron procesadas correctamente.
Involucra examinar los SI con una mente crítica, siempre con una visión cuestionadora sobre la capacidad de los SI para:
1) salvaguardar activos,
2) mantener integridad de datos,
3) lograr objetivos eficiente y eficazmente.

ADMINISTRACIÓN DE SISTEMAS DE INFORMACIÓN
Aporta:
1) técnicas de administración de proyectos.
2) documentación, estándares, presupuestos.
A raíz de los fracasos al comienzo, ahora aporta nuevos métodos para mejorar el desarrollo y la implementación de sistemas. Ejemplo: metodologías de desarrollo de sistemas.

CIENCIAS DEL COMPORTAMIENTO
Una resistencia de comportamiento para con el sistema pone en peligro los objetivos de la auditoría. Usuarios descontentos pueden intentar sabotaje o circunscribir controles. Lo mismo sucede con diseñadores, y entre estos y los usuarios. Los auditores deben comprender las situaciones que dan lugar a conflictos de comportamiento y como resultado posible, el fracaso del sistema.

CIENCIAS DE LA COMPUTACIÓN
Los Ingenieros de Software deben colaborar con los objetivos de la auditoría. Ejemplo: investigar sobre cómo probar la correctitud de un programa formalmente.
El conocimiento técnico en profundidad desarrollado por esta disciplina causa problemas y beneficios a los auditores.
• beneficios: se pueden preocupar menos por la confiabilidad de algunas componentes.
• problemas: pueden tener dificultades para determinar abusos.

CONTROLES

Definición.: Un control es un sistema que previene, detecta, o corrige eventos ilegales.
Hay tres aspectos claves en esta definición:
1) un control es un sistema
   Habitualmente, tendemos a nombrar los controles, teniendo en cuenta sólo un aspecto del control. Una password se convierte en control, sólo en el contexto de un sistema que asegure:
   1) seguridad para elegir passwords,
   2) correcta validación de passwords,
   3) almacenamiento seguro de las passwords,
   4) seguimiento en el uso indebido de passwords
   5) ...
2) eventos ilegales
   ¿Cómo puede surgir un evento ilegal?
   1) si se ingresan al sistema inputs no autorizados, inexactos, incompletos, redundantes, ineficaces o ineficientes,
   2) si el sistema transforma el input de una manera no autorizada, inexacta, incompleta, ineficiente o ineficaz
3) los controles son usados para prevenir , detectar o corregir eventos ilegales.
   TIPOS DE CONTROLES
   Control Preventivo: instrucciones de cómo completar un formulario. Nota: las instrucciones no son el control.
   Control Detectivo: un programa que valida datos de input, rechazando los erróneos.
   Control Correctivo: un programa que detecta el ruido en comunicaciones y permite corregir datos corruptos.

OBJETIVO DE LA AUDITORÍA
Reducir las pérdidas esperadas por eventos ilegales mediante:
1) controles preventivos: reducen la probabilidad que estos eventos ocurran.

2) controles detectivos y correctivos: reducen la cantidad de pérdidas cuando los eventos ilegales ocurren.
La tarea del auditor es determinar si los controles están ubicados y funcionan para prevenir los eventos ilegales.

¿CÓMO ADMINISTRAR LA COMPLEJIDAD?

Para administrar la complejidad, se sugiere:
1) factorizar el sistema en subsistemas

FACTORIZACIÓN
El primer paso para comprender un sistema complejo es particionarlo en subsistemas.
Un subsistema es un componente de un sistema que:
1) realiza ciertas funciones básicas necesarias para el sistema en general,
2) le permite atender sus objetivos fundamentales.
Los subsistemas son componentes lógicas y no físicas.
El proceso de particionar en subsistemas se denomina factorización.
El proceso de factorización termina cuando se ha particionado el sistema en partes lo suficientemente pequeñas, de tal modo que puedan ser entendidas y evaluadas.

Para poder factorizar, se necesita un criterio.
Criterio: La esencia de un subsistema es la función que realiza. Los auditores deben identificar primero, las principales funciones que el sistema realiza para cumplir sus objetivos.
OTROS CRITERIOS
ACOPLAMIENTO: Cada subsistema debería ser relativamente independiente de otros subsistemas. Sistemas con poco acoplamiento son más fáciles de comprender.
COHESIÓN: Cada subsistema debe ser internamente cohesivo. Todas las actividades realizadas por el sistema apuntan a cumplir la función principal del subsistema.

FORMAS DE FACTORIZACIÓN
1) funciones gerenciales - las funciones que se deben realizar para asegurar que el desarrollo, la implementación, operación y mantenimiento de los sistemas de información proceden de una forma planificada y controlada. Ejemplo Parte 2 - PAG 18
2) funciones de aplicación - tareas que son necesarias ejecutar para realizar un procesamiento de información confiable. Relacionado con “ciclos”. Ejemplo Parte 2 - PAG 21

2) determinar la confiabilidad de cada subsistema, y las implicancias de cada uno de ellos en el nivel de confiabilidad general del sistema.
CONFIABILIDAD DE SUBSISTEMAS
Primero - determinar el menor nivel de los subsistemas.
Segundo - evaluar la confiabilidad de los controles en cada subsistema.
CONFIABILIDAD DE CONTROLES
Para evaluar la confiabilidad de los controles:
1) se deben identificar todos los posibles tipos de eventos que pueden ocurrir en el subsistema.
2) se deben considerar todos los eventos válidos o ilegales.
Para identificar los eventos, hay que considerar las principales funciones que realiza el subsistema.

CONSIDERAR LAS PRINCIPALES FUNCIONES
Para cada función:
1) analizar cómo debería realizarse
2) evaluar cómo el subsistema cumple con esa visión normativa.
Para determinar si un evento es legal o ilegal se deben considerar las transacciones que pueden ocurrir como input al subsistema.

Todos los eventos en un sistema de aplicación deben surgir de una transacción.

EVENTOS Y TRANSACCIONES
Cuando un evento ocurre, el sistema recibe una transacción de input. Cuando la transacción se recibe como input el sistema cambia de estado. Otros cambios de estado ocurren a medida que el sistema procesa la transacción.
Para identificar todos los eventos que pueden ocurrir en un sistema como resultado de la transacción, se debe entender cómo el sistema procesa la transacción.

PROCESAMIENTO DE TRANSACCIONES
Generalmente los auditores aplican técnicas de walk-through:
1) se considera una transacción particular,
2) se identifican todos los componentes del sistema que procesan la transacción
3) se trata de entender cada paso de procesamiento que ejecuta cada componente
4) se considera cualquier error o irregularidad (evento ilegal) que pueda ocurrir en el camino.

CLASES DE TRANSACCIONES
Generalmente es muy costoso realizar este proceso para todas las transacciones.
Por eso, se trabaja con clases de transacciones:
1) se agrupan transacciones que tengan un procesamiento similar,
2) se trata de entender esas transacciones, y los eventos que puedan surgir como resultado de esas transacciones como grupo,
3) se tratan sólo aquellas transacciones que se consideran importantes para los objetivos de la auditoría.

¿QUÉ EVENTOS?
Usando esta técnica, no se identifican todos los eventos que puedan surgir en un sistema.
A pesar de esto, los auditores deberían examinar todas aquellas transacciones y eventos que consideren importantes.
Una vez que se han identificado los eventos que pueden ocurrir, los auditores deben evaluar:
1) si los controles están correctamente ubicados, y
2) si funcionan para detectar eventos ilegales.

CONFIABILIDAD DE LOS CONTROLES

Los auditores deben recolectar evidencias sobre la existencia y confiabilidad de los controles, para determinar si las pérdidas por los eventos ilegales se reducen a niveles aceptables.
Para cada evento ilegal, se debe considerar:
1) cómo los controles cubren a ese tipo de evento,
2) cuánto de confiable son los controles,
3) si puede ocurrir un error material o una irregularidad.

Se publican listas que ayudan a realizar esta tarea. Estas listas muestran por ejemplo:
1) las caídas en los sistemas de información,
2) errores e irregularidades que ocurren en diferentes tipos de transacciones.
Las listas muestran los controles que se pueden realizar para reducir las pérdidas esperadas por errores o irregularidades.

ESTIMAR LA CONFIABILIDAD

La evaluación de la confiabilidad procede de abajo hacia arriba en el nivel de estructura de los sistemas. Los subsistemas de menor nivel son componentes de los de mayor nivel.Cuando se haya evaluado la confiabilidad de los subsistemas de menor nivel, se puede analizar:
1) el impacto
2) la naturaleza, y
3) la frecuencia de los eventos ilegales
en los sistemas de mayor nivel.

ESTIMAR LA CONFIABILIDAD – PASOS
En cualquier nivel de la estructura, los pasos de evaluación son:
1) identificar las transacciones que ingresan al sistema
2) considerar los eventos legales e ilegales que puedan ocurrir
3) asegurar la confiabilidad de los controles que detectan los eventos ilegales

DETECTAR NUEVOS CONTROLES
A medida que se evalúan los sistemas de más alto nivel, se pueden encontrar nuevos controles debido a:
1) Los controles en sistemas de bajo nivel pueden funcionar mal. Ejemplo: se divide el trabajo en varias personas y un superior controla el funcionamiento general.
2) Podría ser más efectivo en costos implementar controles a alto nivel. Ejemplo: en lugar de que cada uno controle su trabajo, un superior aleatoriamente supervisa el trabajo por muestreo.
3) Algunos eventos no se manifiestan como ilegales excepto en los niveles altos. Ejemplo: consultas a una base de datos sin violar confidencialidad.

Riesgos

RIESGOS DE LA AUDITORÍA
Recordemos los objetivos de la auditoría, salvaguardar activos, asegurar integridad de los datos, asegurar que los sistemas son efectivos, y asegurar que los sistemas son eficaces
Para poder cumplir con los objetivos, se debe recolectar evidencia.
Para esto, se debe medir, y se podría fallar al detectar las pérdidas materiales reales o potenciales.

Definición: El riesgo de auditoría es el riesgo de que un auditor fracase al detectar las pérdidas materiales reales, o potenciales, o los registros incorrectos.

RDA = RI * RC * RD
RDA: Riesgo Deseado de Auditoría
RI: Riesgo Inherente
RC: Riesgo de Control
RD: Riesgo de Detección

TIPO DE RIESGOS
1) Riesgo Deseado: el riesgo que se desea correr.
2) Riesgo Inherente: refleja la probabilidad que una pérdida material o una imputación errónea exista en algún segmento de la auditoría, antes de que sea considerada la confiabilidad de los controles internos.
3) Riesgo de Control: refleja la probabilidad que en algún segmento de la auditoría, los controles internos no prevengan, detecten o corrijan pérdidas materiales o imputaciones erróneas que puedan surgir.

4) Riesgo de Detección: refleja la probabilidad que los procedimientos de auditoría utilizados en algún segmento, fallen en detectar pérdidas materiales o imputaciones erróneas.

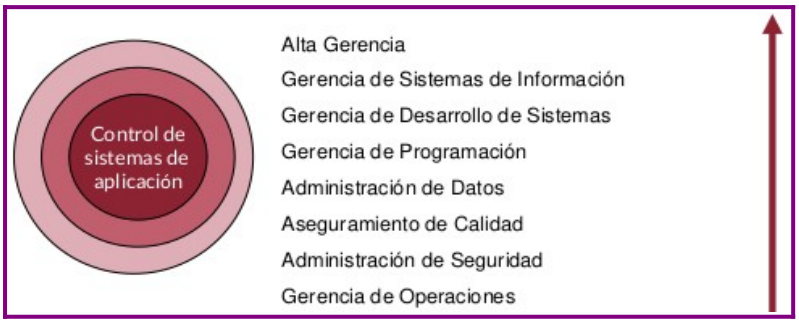
– Primero los auditores eligen el nivel de RDA. Evalúan las consecuencias de fracasar en detectar las pérdidas materiales reales o potenciales.

– Luego, se considera el nivel de RI. Los auditores consideran factores generales tales como la naturaleza de la organización (la posición en el mercado), la industria en la que opera, las características del gerenciamiento, intereses contables y de auditoría...
Se consideran luego los RI asociados con diferentes segmentos de la auditoría (ciclos, sistemas de aplicación, ...). Para cada segmento, se consideran factores tales como:

1) sistemas financieros
   Proveen controles financieros sobre los principales activos de la organización.
   Poseen alto RI.
   Son el blanco de acciones delictivas y fraudes.
2) sistemas estratégicos
   Proveen ventajas competitivas para la organización.
   Comprometen clientes, proveedores, secretos de marca.
   Tienen alto RI.
   Son blanco de espionaje industrial, o acciones indebidas de la competencia.
3) sistemas de operación crítica
   Aquellos sistemas que pueden paralizar a la organización si fallan.
   Generalmente tienen alto RI.
4) sistemas de tecnología avanzada
   Sistemas que usan tecnología de punta.
   Tienen alto RI, debido a la falta de experiencia en ese tipo de sistemas.

– Para evaluar el nivel de RC asociado con cada segmento de la auditoría, se debe considerar la confiabilidad de los controles gerenciales y de aplicación. Generalmente, se identifican y evalúan primero los controles en los subsistemas gerenciales.

Los controles gerenciales actúan como capas de cebolla protectivas, por encima de los controles de aplicación.



El buen nivel de los controles externos garantizan el nivel de los controles internos.
Los controles gerenciales se evalúan en general, y no para cada aplicación.

– Finalmente, se calcula el nivel de RD que se debe lograr para cumplir con el RDA.
Se diseñan procedimientos de recolección de evidencia para intentar lograr el nivel de RD.
En general:
1) los auditores no recolectan la cantidad de evidencia que ellos desearían
2) deben ser astutos para determinar en dónde aplicar los procedimientos de auditoría, y cómo interpretar la evidencia recolectada.

Procedimientos

PROCEDIMIENTOS DE UNA AUDITORÍA
Existen diferentes procedimientos de auditoría, dependiendo de lo que se deseecontrolar:
1) determinar si ocurrieron pérdidas materiales o la información financiera es errónea

A fin de recolectar evidencia, para determinar si ocurrieron pérdidas materiales o la información financiera es errónea, se usan los siguientes procedimientos:
1) procedimientos para comprender los controles
2) testeo de controles
3) testeos substantivos de detalle de transacciones
4) testeos substantivos de detalle de balances contables
5) procedimientos de revisión analítica

2) determinar la eficiencia y eficacia de las operaciones

Para determinar la eficiencia y eficacia de las operaciones se utilizan procedimientos similares:
1) procedimientos para comprender los controles
2) testeo de controles
3) testeos sustantivos de detalle de transacciones.
4) testeos sustantivos de resultados generales - la noción de balances contables no es aplicable en este caso. Ejemplo: testeos de performance.
5) procedimientos de revisión analítica. Ejemplo: modelos de simulación.

1) procedimientos para comprender los controles
2) testeo de controles
3) testeos sustantivos de detalle de transacciones.
4) testeos substantivos de detalle de balances contables / testeos sustantivos de resultados generales
5) procedimientos de revisión analítica.

PROCEDIMIENTOS PARA COMPRENDER LOS CONTROLES
Los procedimientos incluyen cuestionarios, inspecciones, observaciones
Para determinar si los controles existen, analizar cómo están diseñados, si funcionan.

TESTEO DE CONTROLES
Son para evaluar si los controles están actuando efectivamente.
Ejemplos: cuestionarios, inspecciones, observaciones, reprocesos.

DETALLE DE TRANSACCIONES
Los testeos substantivos de detalle de transacciones están diseñados para detectar:
1) errores monetarios o
2) irregularidades
en transacciones que afectan los estados financieros. Ejemplo: controlar la facturación

DETALLE DE BALANCES CONTABLES
Los tests substantivos de detalle de balances contables se focalizan en los registros contables finales, en el balance. Ejemplo: se puede circularizar a una muestra de clientes para controlar que los saldos registrados sean correctos.

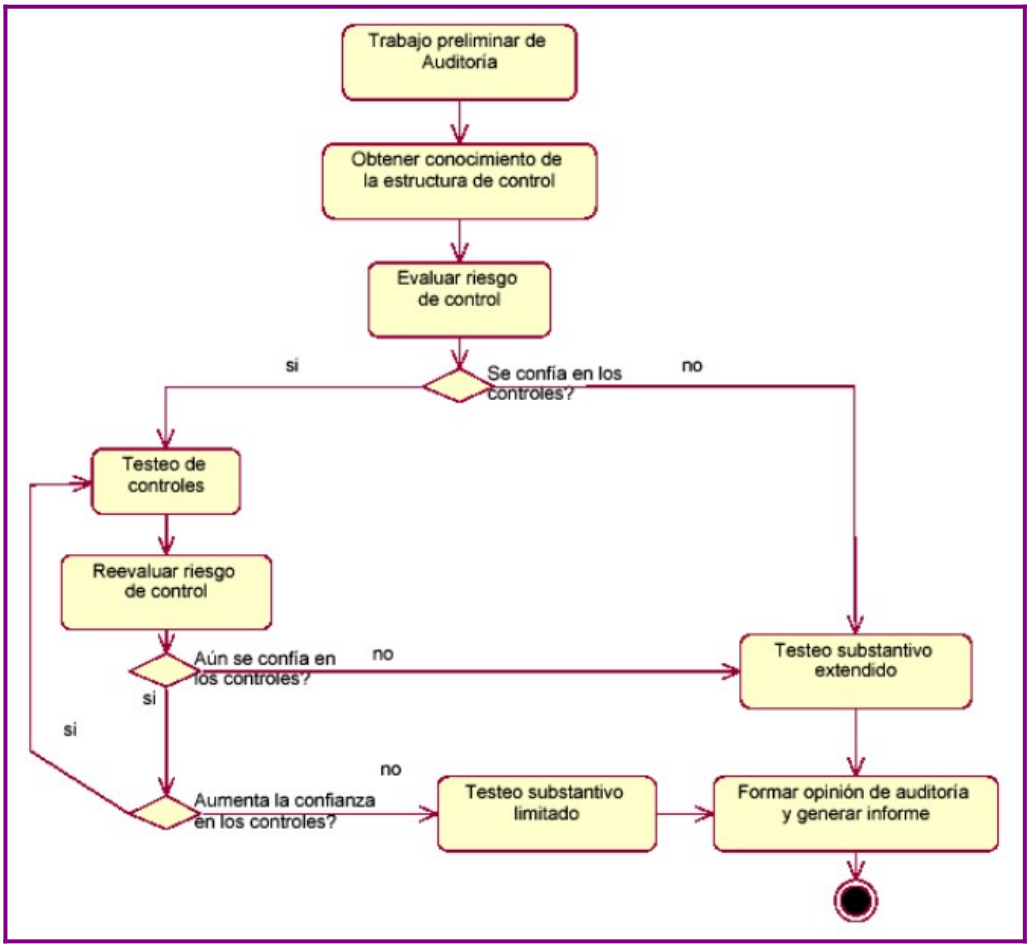
PROCEDIMIENTOS DE REVISIÓN ANALÍTICA
Los procedimientos de revisión analítica se focalizan en las relaciones entre los ítems de datos. El objetivo es identificar áreas que requieran un trabajo de auditoría posterior. Ejemplo: medir ingresos por ventas durante un período.

El orden de los testeos de menos costosos a más costosos es:

1) procedimientos de revisión analítica
2) procedimientos para comprender los controles
3) testeo de controles
4) testeos sustantivos de detalle de transacciones
5) testeos sustantivos de resultados generales/balances contables

El orden es a la inversa si se evalúa la confiabilidad y el contenido de la información de la evidencia provista por los procedimientos.

Tareas



PLANIFICACIÓN DE UNA AUDITORÍA

La primera etapa es la planificación.
Las tareas que se realizan en la etapa de planificación varían dependiendo si es una:
1) auditoría interna

La etapa de planificación incluye:
1) asignar personal adecuado a las auditorías
2) obtener información del cliente
3) realizar procedimientos de revisión analíticos para comprender el negocio del cliente
4) identificar áreas de riesgo

Los auditores internos se preocupan por el tamaño de las pérdidas que pudiera haber por operaciones ineficientes o ineficaces.

2) auditoría externa

La etapa de planificación incluye:
1) investigar nuevos clientes
2) asignar personal adecuado a las auditorías
3) obtener el contrato
4) obtener información del cliente
5) realizar procedimientos de revisión analíticos para comprender el negocio del cliente
6) identificar áreas de riesgo

Los auditores externos se preocupan por el tamaño de los errores en los estados financieros.

TAREAS DE PLANIFICACIÓN

1) determinar el alcance de la auditoría,

Determinar qué se va a auditar:
1) un sistema
2) un conjunto de sistemas
3) un área del tecnología informática

2) emitir una opinión sobre el RDA,

Se emite un RDA en general para toda la tarea de auditoría.

3) emitir una opinión sobre el RI,

El RI depende del segmento a auditar.
Algunos segmentos son más susceptible a errores, irregularidades, ineficiencias, o ineficacias.
Para cada segmento evaluar los factores que conducen a RI, por ejemplo:
o sistema con manejo de efectivo: posibilidades de defraudaciones.
o sistema complejo tecnológicamente: posibilidades de mal uso de recursos.

4) emitir una opinión sobre el RC,

La decisión más difícil está en emitir el juicio en el nivel de RC asociado con cada segmento de la auditoría. Para esto, los auditores deben comprender los controles internos usados dentro de la organización.

Los controles internos (CI) comprenden 5 componentes relacionados:

1) controles de entorno

Incluye evaluar los elementos que establecen el contexto de control en el cual deben operar los sistemas y los procedimientos de control.

2) evaluación de riesgo

Incluye evaluar:
1) los elementos que identifican y analizan los riesgos a los cuales se enfrenta la organización y
2) cómo son administrados.

3) actividades de control

Incluye evaluar los elementos que operan para asegurar que:
1) las transacciones son autorizadas,
2) las responsabilidades se separan,
3) los documentos y registros se mantienen adecuadamente, etc.

Se clasifican en:
1) controles contables: elementos que operan para asegurar distintos niveles de autorizaciones y responsabilidades
2) controles administrativos: elementos para asegurar eficiencia y eficacia.

4) información y comunicación

Incluye evaluar los elementos en los cuales se:
1) identifica,

2) captura,
3) intercambia información
en tiempo y forma.
Permite asignar responsabilidades del personal adecuadamente.

5) monitoreo

Incluye evaluar los elementos que aseguran que los controles internos operan de manera confiable en el tiempo.

COMPRENDER LOS CONTROLES
Comprender los controles internos incluye factorizar y examinar los controles gerenciales y de aplicación. Los controles gerenciales varían sustancialmente de organización a organización.

5) calcular el RD que se debe lograr para cumplir con el RDA,

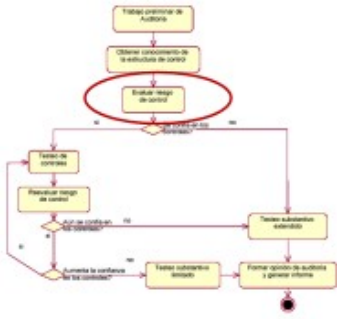
6) recolectar evidencia

Existen distintas técnicas para recolectar evidencia:
1) revisión de papeles de trabajo de auditorías previas
2) entrevistas con alta gerencia y personal superior
3) observación de cómo se desarrollan las actividades
4) revisión de documentación de sistemas

7) documentar evidencia

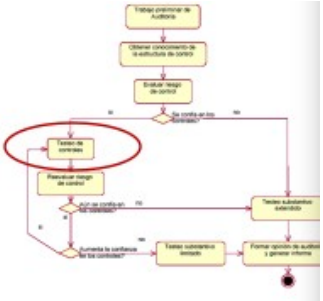
La evidencia se documenta:
1) completando cuestionarios
2) construyendo diagramas de flujo de alto nivel
3) construyendo tablas de decisión
4) redactando descripciones narrativas.
5) utilizando herramientas CASE
No invertir demasiado tiempo en esta etapa. El necesario para comprender los controles internos y decidir cómo proseguir con la auditoría.
Finalmente se debe evaluar el riesgo.

EVALUACIÓN DE RIESGO DE CONTROL



Si se evalúa que el RC < el nivel máximo =>
1) identificar los controles materiales que se relacionan con la evaluación
2) testear los controles para determinar si operan efectivamente.
Premisa: los testeos de controles probarán, que si los controles funcionan correctamente, se puede reducir la necesidad de un testeo sustantivo.
Si se evalúa que el RC es de nivel máximo => no se testean los controles.
Se podría concluir que los controles internos no son efectivos.
Se debería realizar un testeo amplio.

TESTEO DE CONTROLES



El testeo de controles evalúa cuan confiables y específicos son los controles.
Se testean, sólo si el RC se determinó menor al máximo.

Se confía en los controles como una base para reducir el costo de un testeo más amplio.
A esta altura, los auditores no saben si los controles identificados operan efectivamente.

CONTROLES GERENCIALES – TESTEO
Se comienza por los controles gerenciales.
Si los controles gerenciales, demuestran contrariamente a lo supuesto, que no operan eficientemente => no tiene sentido testear los controles de aplicación.

CONTROLES DE APLICACIÓN – TESTEO
Si los controles gerenciales funcionan efectivamente, se procede a evaluar los controles de la aplicación.

Luego de evaluados los controles, se vuelve a estimar el riesgo.

TESTEO DE CONTROLES – CONCLUSIÓN

Se puede concluir que los controles internos son más fuertes o más débiles a lo anticipado.

Si los controles son más fuertes a lo pensado, se puede pensar en reducir testeos.
Si los controles son más débiles, se pueden ampliar los testeos.

ACTITUD DEL AUDITOR
Durante esta etapa los auditores externos e internos pueden tener distintas actitudes.
Situación: se detecta que los controles son débiles
1) auditor interno: puede expandir sus investigaciones para lograr una mejor comprensión a cerca de la naturaleza e implicancias de estas debilidades.
2) auditor externo: puede cortar sus investigaciones (sobre causas) y realizar testeos más amplios.

TESTEO DE TRANSACCIONES
Se realiza para evaluar si un procesamiento erróneo o irregular puede ocasionar pérdidas.

Desde un punto de vista operativo, el testeo de transacciones sirve para determinar si el procesamiento es efectivo y eficiente.

TESTEO DE RESULTADOS GENERALES
Se realizan con el fin de obtener evidencia suficiente para realizar un juicio final sobre el grado de pérdidas que podrían ocurrir cuando el sistema falla en: salvaguardar activos, mantener la integridad de los datos y lograr efectividad y eficiencia.
En general, este tipo de testeos, son los más caros de las auditorías.

TESTEO DE RESULTADOS ...
Si los auditores confían en que los controles son confiables, pueden limitar el número y alcance de estos testeos.
Si es a la inversa, aumentarán el grado de control para estimar mejor las pérdidas.

EVALUAR EFECTIVIDAD Y EFICIENCIA
Evaluar efectividad y eficiencia es más complejo.
Se puede trabajar con los usuarios estimando las pérdidas por no haber tomado una decisión por no contar con la información en tiempo y forma.

COMPLETAR LA AUDITORÍA
En la etapa final, se realizan testeos adicionales para cerrar la evidencia.
Finalmente, se formula la opinión sobre cómo ocurrieron las pérdidas materiales o registros incorrectos en un informe.

INFORME

Un informe típico debería incluir:
1) una introducción que describa los objetivos de la auditoría,
2) el enfoque general utilizado,
3) un resumen de las conclusiones críticas,
4) recomendaciones para abordar las conclusiones críticas,
5) datos que respalden las conclusiones críticas.

OPINIONES DE AUDITORÍA
Los estándares en varios países requieren que la opinión sea:
1) opinión excusada: en base al trabajo realizado no se puede emitir opinión.
2) opinión adversa: se concluye que han ocurrido pérdidas materiales o que los estados financieros están distorsionados.
3) opinión con calificación: se concluye que han ocurrido pérdidas materiales o existen registros incorrectos, pero las cantidades no son considerables.
4) opinión sin calificación: el auditor considera que no han ocurrido pérdidas materiales o no existen registros incorrectos.

Gobernanza de TI

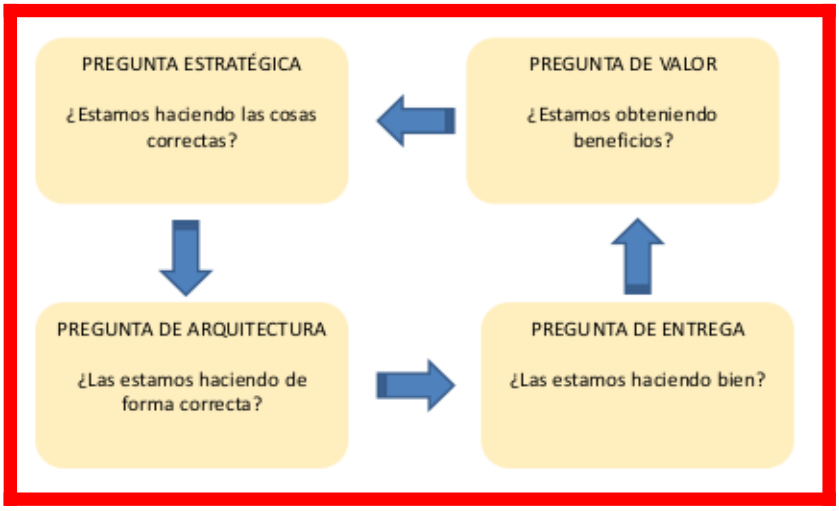
La Gobernanza de TI es un subconjunto de Gobierno Corporativo de las organizaciones que se centra en los sistemas de TI, su desempeño y los riesgos asociados.

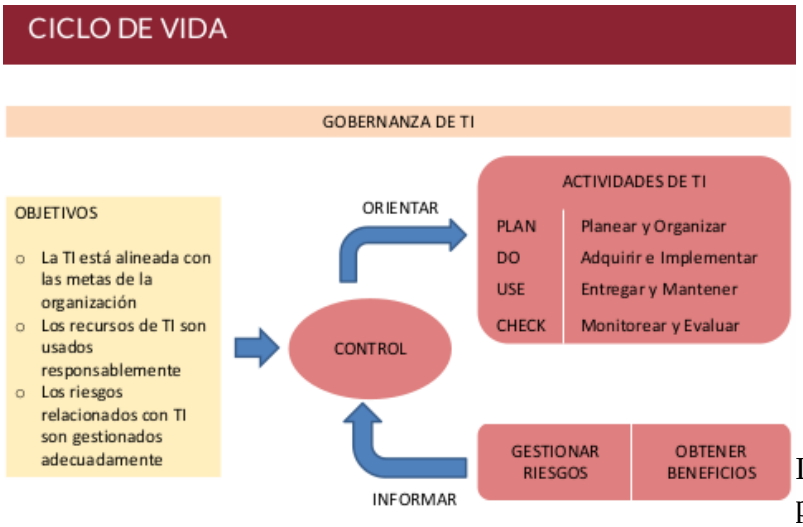
GOBERNANZA DE TI
o trata con la relación entre el enfoque empresarial y la gestión de TI
o destaca la importancia de las cuestiones de TI
o promueve que las decisions estratégicas de TI deben ser tomadas por una junta directiva corporativa
METAS
o asegurar que las inversiones en TI generen valor
o mitigar riesgos asociados con TI

INSTITUTO DE GOBERNANZA DE TI: son estructuras y procesos de liderazgo y organizativos que aseguran que las TI de la organización sostienen y extienden las estrategias y los objetivos de la organización

ADMINISTRACIÓN DE TI: se trata de tomar e implementar decisiones de TI
GOBERNANZA DE TI: se trata de quién toma las decisiones de TI
o quién tiene autoridad para tomar las decisiones importantes
o quién tiene información para tomar las decisiones importantes
o quién es responsible por implementar las decisions importantes

CINCO ÁREAS DE ENFOQUE – todas impulsadas por el valor de las partes interesadas
RESULTADOS
1) entrega de valor
2) manejo de riesgos
CONDUCTORES
3) alineamiento estratégico
4) manejo de recursos
5) mediciones de desempeño



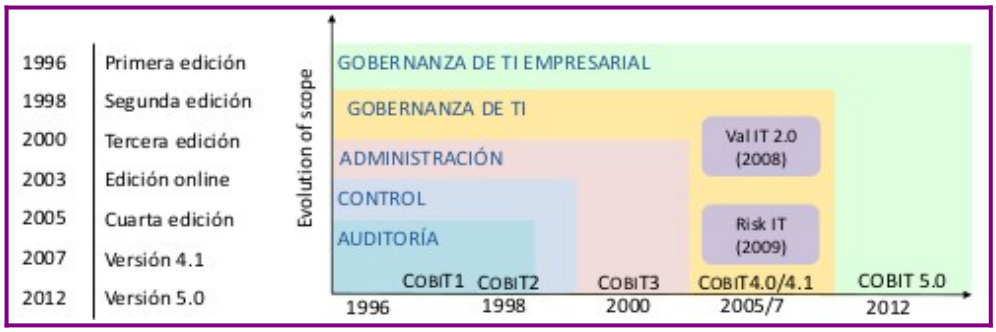


La Gobernanza de TI es apoyada por :
1 Gestión de los activos de TI
2 Gestión del portfolio de TI
3 Gestión de infraestructura de TI y arquitectura empresarial
4 Estándares de TI
5 Gestión de programas
6 Gestión de proyectos
7 Gestión de servicios de TI
8 Gestión de la seguridad de TI
... otros

COBIT

OBJETIVOS DE CONTROL PARA INFOMACIÓN Y TECNOLOGÍA RELACIONADA (COBIT)
Enfoque para estandarizar buenas practices de TI y control. Provee herramientas para accede y medir el desempeño de los procesos de gobernanza y administración de TI de una organización. Desarrollado y mantenido por el Instituto de Gobernanza de TI - http://www.itgi.org/

OBJETIVOS DE CONTROL PARA INFORMACIÓN Y TECNOLOGÍA RELACIONADA (COBIT) es un conjunto de recursos que contienen toda la información que las organizaciones necesitan para adopter un marco de gobernanza y control de TI.
Fue creado por la Asociación de Auditoría y Control de Sistemas de Información (ISACA, www.isaca.org) y el Instituto de Gobernanza de TI en 1992.
COBIT 5 consolida COBIT 4.1, Val IT y Risk IT en un marco y se ha actualizado para alinearse con las mejores prácticas actuales, por ejemplo ITIL V3 2011, TOGAF (El Marco de Arquitectura de Grupo Abierto).

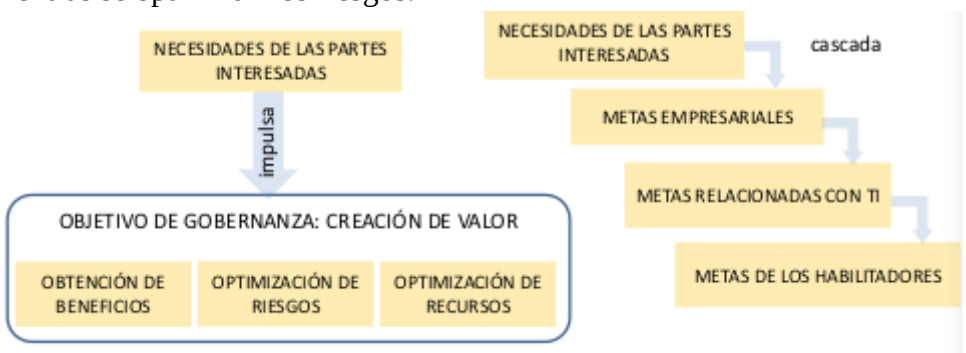


PRINCIPIOS

1) Satisfacer las necesidades de las partes interesadas
Garantizar que las empresas aporten valor a sus partes interesadas mediante la obtención de beneficios, la optimización del uso de los recursos y la gestión de riesgos.

CASCADA DE METAS

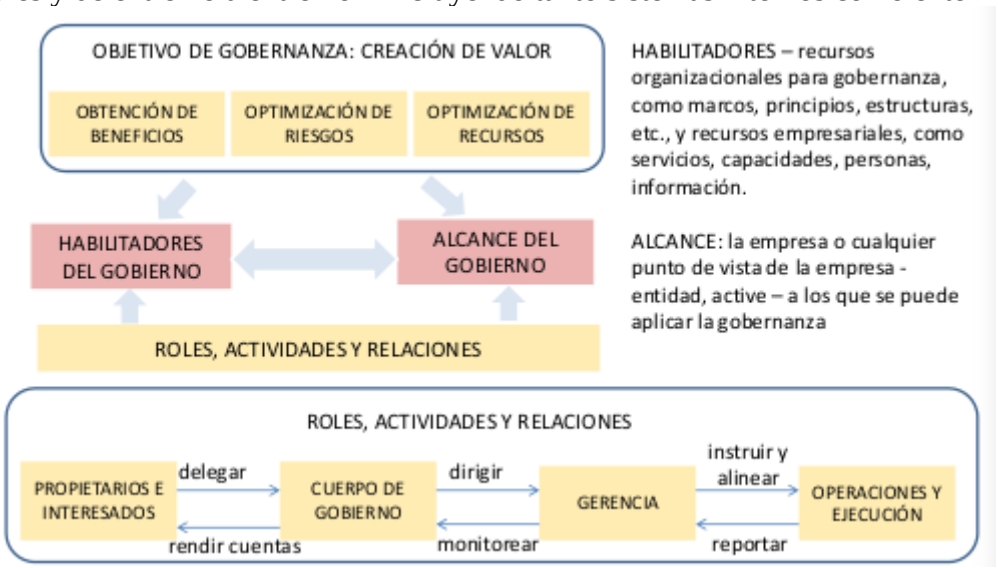
Todas las empresas deben aportar valor a sus partes interesadas. Por lo tanto, la creación de valor es un objetivo de gobernanza de toda organización.
El valor puede ser creado mediante la obtención de beneficios a un costo óptimo de recursos mientras se optimizan los riesgos.



Las necesidades de las partes interesadas necesitan ser transformadas en una estrategia empresarial. La cascada de metas es un mecanismo para transformar las necesidades de las partes interesadas en metas empresariales, metas relacionadas con TI y metas de los habilitadores.

2) Cubrir la empresa de extremo a extremo

Tener en cuenta todos los sistemas de gobernanza y administración relacionados con TI para que sean integrales y de extremo a extremo – incluyendo tanto sistemas internos como externos.



3) Aplicar un marco integrado

Alinearse con otros estándares y buenas prácticas relacionadas con TI, sirviendo de marco general para la gobernanza y administración de TI empresarial.
COBIT 5:

- ✔ Se alinea con los estándares y marcos más recientes y pertinentes
- ✔ Es completo en la cobertura de la empresa
- ✔ Proporciona una base para integrar efectivamente otros marcos, estándares y prácticas utilizadas
- ✔ Integra todo el conocimiento hasta ahora disperso en diferentes marcos de ISACA
- ✔ Proporciona una arquitectura simple para la estructuración de los materiales de orientación y la producción de un conjunto de productos compatibles

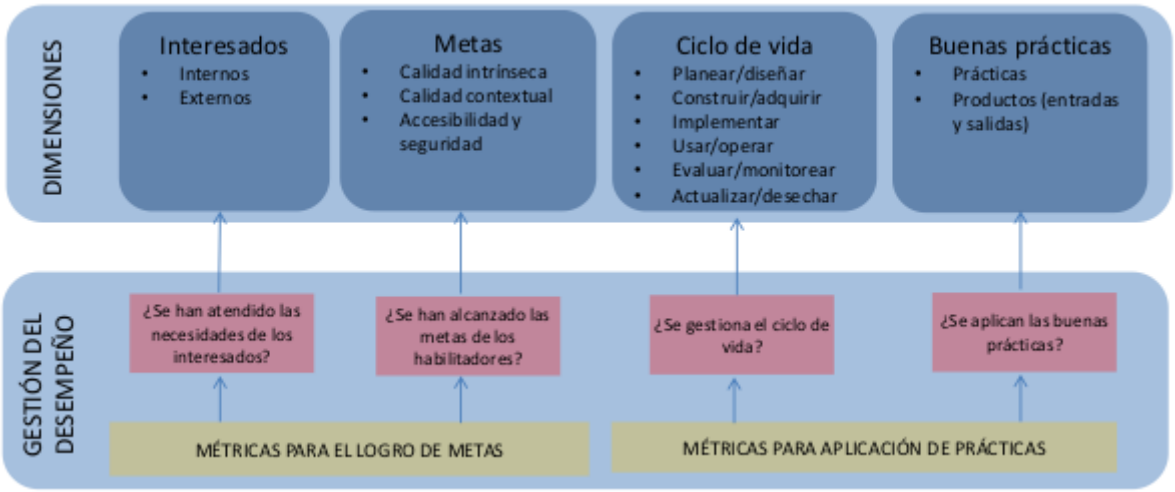
4) Habilitar un enfoque holístico

Tener en cuenta los elementos que interactúan, especificar un conjunto de habilitadores para definir un sistema integral de gobernanza y administración de TI empresarial.

Los habilitadores son factores que, de manera individual y colectiva, influyen en si algo funcionará, en este caso, la gobernanza y administración de TI de la empresa.
COBIT define siete categorías de habilitadores

Todos los habilitadores tienen un conjunto de dimensiones comunes:

- ✔ Es una forma sencilla y estructurada para tratar los habilitadores
- ✔ Le permite a una entidad gestionar sus complejas interacciones
- ✔ Facilita el éxito de los resultados de los habilitadores



5) Separar las funciones principales

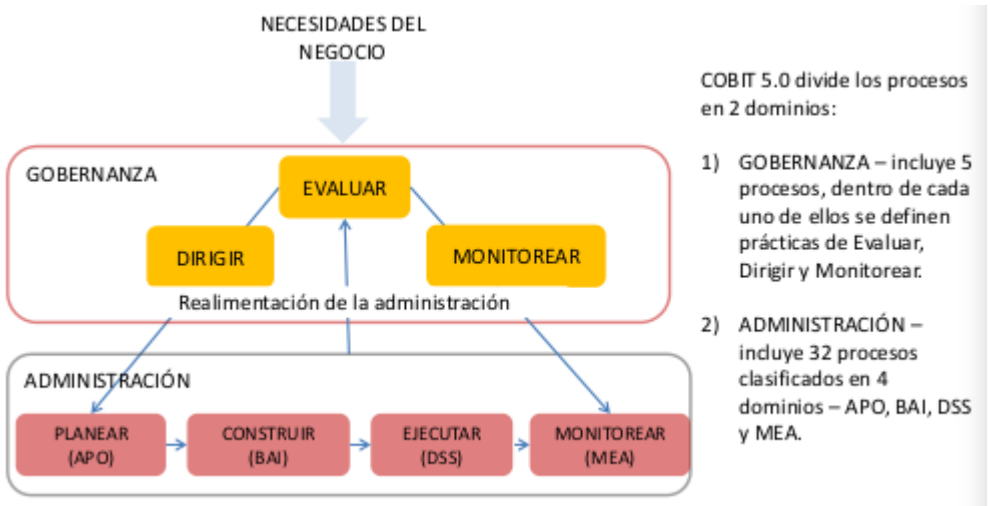
Establecer una distinción clara entre las funciones de gobernanza y administración.

GOBERNANZA asegura:

- ✔ que las necesidades, condiciones y opciones de las partes interesadas son evaluadas para determinar objetivos empresariales a alcanzar equilibrados y acordados
- ✔ establecer la dirección a través de la priorización y la toma de decisiones
- ✔ supervisando el desempeño y cumplimiento contra la dirección y objetivos acordados

ADMINISTRACIÓN: planifica, construye, ejecuta y monitorea las actividades en consonancia con la dirección establecida por el cuerpo de gobierno para alcanzar los objetivos empresariales

MODELO DE REFERENCIA DEL PROCESO



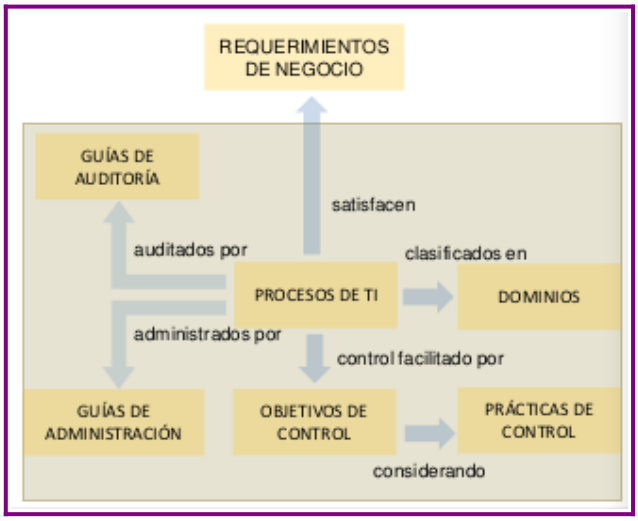
CARACTERÍSTICAS PRINCIPALES

- ✔ incorpora los principales estándares internacionales
- ✔ está centrado en los negocios, orientado a procesos, controlado y medido
- ✔ opera a un nivel más alto que los estándares de tecnología pura para la administración de sistemas de información
- ✔ puede ser adaptado por organizaciones mundiales comerciales, gubernamentales y profesionales

AUDIENCIA
GERENTES les ayuda a equilibrar el riesgo y control de la inversión en un ambiente de TI a menudo impredecible
USUARIOS les garantiza seguridad y control de los servicios de TI internos o proporcionados por terceros
AUDITORES les ayuda a definir el nivel de seguridad sobre el objeto particular a auditar los asesora sobre la gestión de los controles internos

ELEMENTOS

1 Procesos de TI y Dominios
2 Objetivos de Control
3 Prácticas de Control
4 Guías de Auditoría
5 Guías de Administración



PROCESOS DE GOBERNANZA

Contiene 5 procesos, para cada uno se definen prácticas de evaluar, dirigir y monitorear (EDM).

EDM se interesa en:
o establecer un marco de gobernanza
o crear valor para las partes interesadas
o asegura que los objetivos de la empresa sean alcanzados

- ✔ EVALUANDO las necesidades, condiciones y opciones de las partes interesadas,
- ✔ estableciendo DIRECCIÓN mediante la priorización y la toma de decisiones, y
- ✔ MONITOREANDO el desempeño, el cumplimiento y el progreso contra la dirección y los objetivos acordados (EDM).

EDM – PROCESOS DE TI
EDM1 Asegurar el marco de gobernanza, el establecimiento y el mantenimiento
EDM2 Asegurar la entrega de beneficios
EDM3 Asegurar la optimización de riesgos
EDM4 Asegurar la optimización de recursos
EDM5 Asegurar la transparencia de las partes interesadas

PROCESOS DE ADMINISTRACIÓN
COBIT clasifica la Administración de TI en 4 dominios:
Alinear, Planear y Organizar (APO): proporciona direcciones a la entrega de soluciones y servicios

Alinear, Planear y Organizar (APO) abarca estrategias y tácticas y se interesa en la forma que TI puede contribuir a alcanzar los objetivos de negocio.
APO se interesa en:
o la comprensión de la vision a planificar, comunicar y gestionar
o una organización e infraestructura adecuadas para su puesta en marcha

Construir, Adquirir e Implementar (BAI): provee soluciones a DSS para la entrega de servicios
Construir, Adquirir e Implementar (BAI) abarca soluciones de TI que necesitan ser identificadas, desarrolladas o adquiridas, implementadas e integradas en el proceso de negocio
BAI se enfoca en:
o los cambios en las soluciones de TI existentes
o el mantenimiento de sistemas existentes
o asegurar que las soluciones continúan cumpliendo con las metas empresariales

Entrega, Servicio y Soporte (DSS): recibe soluciones y las hace utilizables para los usuarios finales
Entrega, Servicio y Soporte (DSS) trata sobre la entrega efectiva de los servicios requeridos, incluyendo operaciones, seguridad y capacitaciones de continuidad.
DSS se enfoca en:
o la gestión de seguridad y continuidad del servicio
o el soporte de servicios para usuarios
o la administración de datos
o instalaciones operacionales

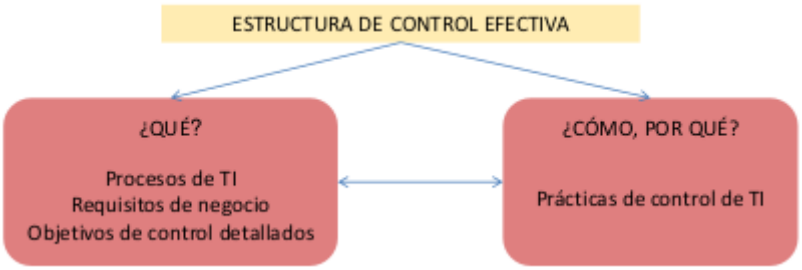
Monitorear y Evaluar (MEA): monitorea todos los procesos para asegurar que se siga la dirección provista
Monitorear y Evaluar (MEA) trata de la evaluación regular de los procesos de TI para controlar su calidad y el cumplimiento de los requisitos de control.
MEA se enfoca en:
o la gestión de desempeño
o el cumplimiento normativo
o el control interno

OBJETIVO DE CONTROL DE TI

Declaración del resultado o propósito a alcanzar mediante la implementación de procesos de control en una actividad particular de TI.
COBIT proporciona objetivos de control de alto nivel, uno para cada uno de los procesos de TI.
Cada objetivo de control de alto nivel se subdivide en una lista de objetivos de control detallados.
COBIT contiene 318 objetivos de control detallados

PRÁCTICAS DE CONTROL

Las prácticas de control de TI proporcionan el más detallado POR QUÉ y CÓMO que necesitan los administradores, los proveedores de servicios, los usuarios finales y los profesionales de control para implementar controles específicos basados en un análisis de los riesgos operacionales y de TI.



GUÍAS DE AUDITORÍA

Las guías de auditoria describen y sugieren las actividades de evaluación que se corresponderán a cada uno de los objetivos de TI de alto nivel
Proporcionan direcciones sobre:
o a quién entrevistar y qué preguntas hacer
o cómo evaluar el cumplimiento de los controles y las evaluaciones
o cómo comprobar el riesgo de que no se cumplan los controles identificados

GUÍAS DE ADMINISTRACIÓN

Las guías de administración proporcionan direcciones para:
o tener bajo control la información de la empresa y los procesos relacionados
o alcanzar los objetivos de la organización
o monitorear y mejorar el desempeño de cada proceso de TI
o comparar logros organizacionales
Para cada proceso de TI, las guías de administración incluyen:
o modelos de madurez (MMs),
o factores de éxito críticos (CSFs)
o Indicadores claves de metas (KGIs)
o indicadores claves de rendimiento (KPIs)

BENEFICIOS - GENERALES
o permite a los administradores públicos cerrar la brecha entre los requisitos de control, los problemas técnicos y los riesgos comerciales
o permite un desarrollo claro de políticas y buenas prácticas para el control de TI en todas las organizaciones gubernamentales
o enfatiza el cumplimiento regulatorio
o ayuda a las organizaciones del sector público a aumentar el valor obtenido de TI
o permite la alineación y simplifica la implementación de la gobernanza de TI en el sector público
o ayuda a los gobiernos a proporcionar servicios mejores y más personalizados a los ciudadanos y las empresas
o optimiza las inversiones en TI, garantiza una prestación de servicios efectiva y proporciona medidas

BENEFICIOS - ESPECÍFICOS
Departamento Estadounidense de Asuntos de Veteranos, EEUU
o cerrar las brechas entre los requisitos de control, los problemas técnicos y el riesgo comercial
o permitir un desarrollo claro de políticas y mejores prácticas
o enfatizar el cumplimiento regulatorio

Parlamento Europeo, Europa
El Parlamento Europeo identificó los proyectos adecuados para implementar y tiene una forma de hacer un seguimiento de los beneficios generados por estos proyectos.

Consejo de Pensión de Ontario, Canadá
o brindar mejores y más servicios personalizados
o establecer un marco integral para la gobernanza de TI que ayude a cerrar las brechas, optimizar las inversiones de TI, garantizar la prestación efectiva de servicios y proporcionar medidas