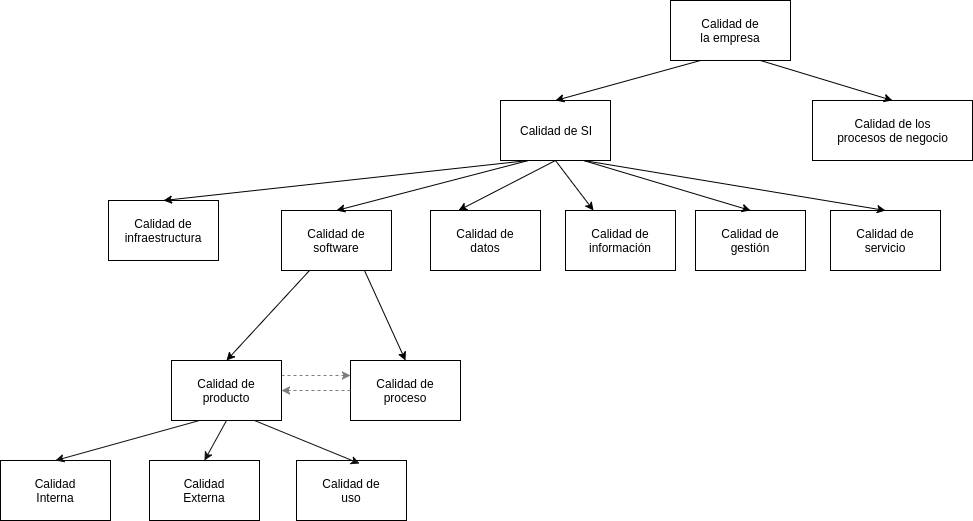
Ingeniería de software 3

Calidad



Definición de calidad:

Calidad es un concepto:

**Relativo (depende de la persona):** La calidad está en los ojos del observador y es relativa a las personas, su edad y circunstancias, al espacio, tiempo...

**Multidimensional (estudia varias cualidades):** Referida a varias cualidades: Funcionalidad, Oportunidad, Costo

**Sujeta a restricciones:** Presupuesto disponible

**Ligado a compromisos aceptables**: Plazos de fabricación.

No es ni totalmente subjetiva (porque ciertos aspectos pueden medirse) ni totalmente objetiva (ya que existen cualidades cuya evaluación sólo puede ser subjetiva).

**» La calidad realizada (la que se logró):** la que es capaz de obtener la persona que realiza el trabajo.

**» La calidad programada (la que se quería lograr)**: la que se ha pretendido obtener

**» La calidad necesaria:** la que el cliente exige.

Definiciones de calidad:

1.f. Propiedad o conjunto de propiedades inherentes a algo, que permiten juzgar su valor. “Esta tela es de buena calidad”.

2.f. Buena calidad, superioridad o excelencia. “La calidad del vino de Jerez ha conquistado los mercados”.

3.f. Carácter, genio, índole.

4.f. Condición o requisito que se pone en un contrato.

5.f. Estado de una persona, naturaleza, edad y demás circunstancias y condiciones que se requieren para un cargo o dignidad

“Conjunto de propiedades o características de un producto o servicio que le confieren aptitud para

satisfacer unas necesidades expresadas o implícitas” (ISO 8402)

Si tenemos en cuenta la primera definición, se habla de propiedades que pueden ser juzgadas, dando a lugar a pensar que la calidad es un término totalmente subjetivo que depende del juicio de la persona que la evalúe.

Gurús de calidad, conjunto de personas que han desarrollado filosofías de calidad, algunas puestas a prueba con resultados satisfactorios.

Shigeo Shingo: Poka Yoke

Un ***poka-yoke*** es una técnica de calidad que se aplica con el fin de evitar errores en la operación de un sistema. Por ejemplo, el conector de un USB tipo A es un poka-yoke puesto que no permite conectarlo al revés.

* Imposibilitar de algún modo el error humano; por ejemplo, los cables para la recarga de baterías de teléfonos móviles y dispositivos de corriente continua sólo pueden conectarse con la polaridad correcta, siendo imposible invertirla, ya que los pines de conexión son de distinto tamaño o forma.
* Resaltar el error cometido de tal manera que sea obvio para el que lo ha cometido. Shingo cita el siguiente ejemplo: un trabajador ha de montar dos pulsadores en un dispositivo colocando debajo de ellos un muelle; para evitar la falta de este último en alguno de los pulsadores se hizo que el trabajador cogiera antes de cada montaje dos muelles de la caja donde se almacenaban todos y los depositase en una bandeja o plato; una vez finalizado el montaje, el trabajador se podía percatar de inmediato del olvido con un simple vistazo a la bandeja, algo imposible de hacer observando la caja donde se apilaban montones de muelles.

Crosby: Para las compañías que estaban “enfermas” en cuanto al nivel de calidad, La vacuna propuesta por Crosby cuenta con integridad, sistemas, comunicaciones, operaciones y políticas, que deberán combinarse para producir el efecto esperado.

Las definiciones de calidad de los gurús coinciden en estos puntos y su interrelación:

* Capacidad de un producto o servicio para servir satisfactoriamente a los propósitos del usuario mediante su utilización (**capacidad de** **satisfacer al usuario**)
* Conformidad con los requisitos explícitos e implícitos de un cliente
* Ausencia de defectos e imperfecciones

Pero la evaluación de los mismos continúa dependiendo de la evaluación de sus características particulares, de manera subjetiva. En consecuencia, lo más importante es definir claramente las características que nos interesa evaluar y su forma de evaluación.

Calidad de los sistemas de Información (SI)

La importancia de los SI en la actualidad hace que las empresas de tecnología hagan mucho hincapié en los estándares de calidad.

El análisis de la calidad de una empresa se divide en la **Calidad de los procesos de negocio** (no lo damos) y la **calidad del sistema de información**

**La calidad del sistema de información** consiste de:

1. Calidad de la Infraestructura: incluye, por ejemplo, la calidad de las redes, y sistemas de software.
2. Calidad de Software: de las aplicaciones de software construidas, o mantenidas, o con el apoyo de IS.
3. Calidad de Datos: Que ingresan en el sistema de información.
4. Calidad de Información: está relacionada con la calidad de los datos.
5. Calidad de gestión: incluye el presupuesto, planificación y programación.
6. Calidad de servicio: incluye los procesos de atención al cliente

**Calidad del software:**

Se divide en **calidad del producto obtenido** y **calidad del proceso de desarrollo**, estas dos son dependientes ya que sin un buen proceso de desarrollo es casi imposible obtener un buen producto.

Las metas que se establezcan para la calidad del producto van a determinar los objetivos del proceso de desarrollo, ya que la calidad del primero va a depender, entre otros aspectos, de éstos.

Diferentes aspectos en la medición de la calidad del producto:

• Calidad interna: Medible a partir de las características como el código fuente.

• Calidad externa: Medible en el comportamiento del producto.

• Calidad en uso: Medible durante la utilización efectiva por parte del usuario.

Los requisitos de calidad más significativos del proceso de software son:

• Que produzca los resultados esperados

• Que estén basados en una correcta definición.

• Que sean mejorados en función de los objetivos de negocio.

Clasificación de Normas y Modelos de Calidad

Familia de normas ISO

» Calidad de Producto

ISO/IEC 9126 - ISO/IEC14598 - ISO/IEC 25000

» Calidad de Proceso

ISO/IEC 12207 - ISO/IEC 15504 – ISO/IEC 29110

» Sistema de gestión de la calidad

ISO/IEC 9001 - ISO/IEC90003

Definiciones:

» Norma: Regla que se debe seguir o a que se deben ajustar las conductas, tareas, actividades, etc.

» Estándar: Que sirve como tipo, modelo, norma, patrón o referencia

El termino norma es más fuerte ya que define las reglas a ser seguidas mientras que estándar es una sugerencia a un modelo a seguir, comúnmente se los utiliza como sinónimos

Identificación de las normas:

»ISO

Organización Internacional de Normalización - (International Organization for Standardization) es una organización no gubernamental con el objetivo de promover una estandarización a nivel

internacional de normas técnicas en diferentes ramas de la industria.

»IEC

International Electrotechnical Commission, es una organización de normalización en los campos: eléctrico, lectrónico y tecnologías relacionadas.

»ISO/IEC

Las normas relacionadas con el software son desarrolla por los dos organismos y se publican bajo la

denominación ISO/IEC.

»IRAM

Asociación civil sin fines de lucro fundada en 1935 con el fin de desarrollar normas con alcance Nacional.

Promueve el uso de las normas ISO en Argentina y es el responsable de realizar las traducciones oficiales.

Las normas ISO que han sido adoptadas por IRAM, se las denomina IRAM – ISO

»NM

Identificación de las normas, indica que fue aprobada por la Asociación Mercosur de Normalización (AMN) y es reconocida por todos los países integrantes del Mercosur.

»ISO – 9001:2008 - Quality management system – Requirements

Norma publicada por ISO en el año 2008.

»IRAM – ISO 9001:2008 – Sistema de gestión de la calidad – Requisitos

Norma publicada por ISO y traducida por IRAM.

»IRAM-ISO/IEC 14598 – 1:2006 – Evaluación del producto de software Parte 1: Descripción general.

Traducción publicada por IRAM en el año 2006 de la primera parte de la evaluación del producto de

software.

Calidad de producto

IRAM-ISO/IEC 9126 /14598 - ISO/IEC 25000 - ISO/IEC 25010 - ISO/IEC 2504

Calidad de Producto de software: IRAM-NM- ISO/IEC 9126 –

Está dividida en 4 partes:

1. Modelo de calidad
2. Métricas externas
3. Métricas internas
4. Métricas de calidad de uso

Evaluación del producto de software: IRAM-ISO/IEC 14598

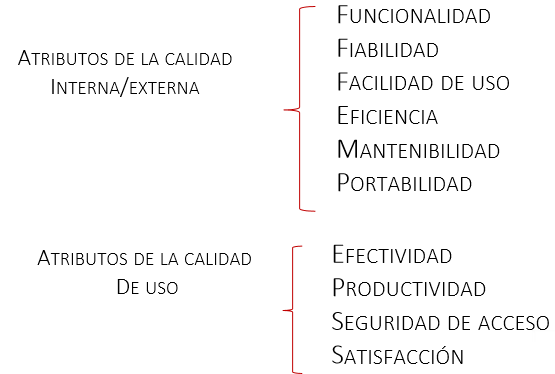
Está dividida en 6 partes:

1. Descripción general
2. Planificación y gestión
3. Proceso para desarrolladores
4. Proceso para compradores
5. Proceso para evaluadores
6. Documentación de los módulos de evaluación

La ISO 9126 define los estándares de calidad de un producto de software, mientras que la ISO 14598 establece los estándares de evaluación del producto. Están relacionadas.

ISO 9126:

Mide atributos de la calidad Interna/externa y de la calidad de uso.



Atributos de calidad interna y externa

**Funcionalidad:** Capacidad del producto del software para proveer funciones que cumplan con necesidades específicas o implícitas, cuando es utilizado bajo condiciones específicas.

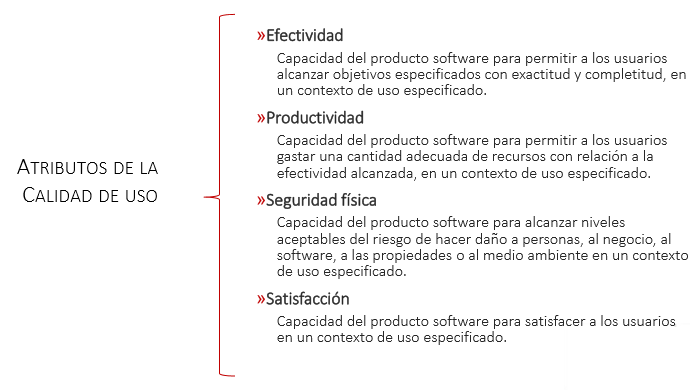
**Fiabilidad:** Capacidad del producto de software para mantener un nivel especificado de rendimiento cuando es utilizado bajo condiciones especificadas.

**Facilidad de uso:** Capacidad del producto de software para ser atractivo, entendido, aprendido y utilizado por el usuario bajo condiciones específicas.

**Eficiencia:** Capacidad del producto de software para proveer un rendimiento apropiado, relativo a la cantidad de recursos utilizados, bajo condiciones específicas.

**Mantenibilidad:** Capacidad del producto para ser modificado.

**Portabilidad:** Capacidad del producto de software para ser transferido de un ambiente a otro.

****

**Calidad de Producto ISO/IEC 14598:**

5-En la descripción de la norma, en el apartado 5 describe la relación entre el proceso de evaluación y las normas de apoyo, como parte de la evaluación define que las características y métricas a utilizar en la evaluación son las definidas por la ISO 9126

6- Define el proceso de evaluación.

* Establecer los requisitos de evaluación
* Especificar evaluación
* Diseñar evaluación
* Ejecutar evaluación

7- Establece los requisitos de la evaluación, como, por ejemplo:

* Propósito de evaluación
* Tipos de productos a evaluar
* Modelo de calidad

8- Especifica la evaluación:

* Selección de las métricas
* Establecer los niveles de puntuación
* Establecer los criterios de evaluación

9- Diseñar la evaluación 9.1 Elaborar el plan de evaluación Describir los métodos de evaluación y el calendario de acciones a evaluar.

10- Realizar la evaluación 10.1 Hacer mediciones 10.2 comparar criterios 10.3 evaluar resultados

11- Proceso de apoyo

Calidad de los datos (ISO 25012)

» Necesidad de una visión coherente e integrada de los datos para garantizar la interoperabilidad de los sistemas

» La dispersión y la reproducción de estos datos entre diferentes organizaciones

» La necesidad de reducir la ambigüedad semántica entre entidades en bases de datos: la misma definición se utiliza para diferentes fenómenos, o lo contrario

» La frecuencia de intercambio de datos en internet, en algunos casos sin saber la calidad del proceso de producción de los mismos

» La necesidad de realizar comparaciones internacionales

» La necesidad de cumplir con leyes internacionales o reglamentaciones

» La necesidad de reducir los costos por falta de calidad de los datos

**Inherente**

Capacidad de las características de los datos de tener el potencial intrínseco para satisfacer las necesidades explícitas e implícitas Este punto de vista está más relacionado con los aspectos del dominio gestionados por los expertos del negocio

**Exactitud:** Los datos representan de forma correcta el verdadero valor

**Completitud:** Los datos tiene valores para todos los atributos esperados

**Consistencia:** Los datos están libre de contradicciones y están coherentes con el resto de los datos **Credibilidad:** Los usuarios consideran que los datos son creíbles

**Actualidad:** Los datos tienen un tiempo adecuado

**Dependientes del sistema**

Capacidad del sistema informático de alcanzar y preservar la calidad de los datos cuando los datos se utilizan en determinadas condiciones Este punto de vista suele ser responsabilidad de los técnicos del sistema

**Disponibilidad:** Los datos pueden ser recuperados por los usuarios autorizados

**Portabilidad:** Los datos pueden ser instalados, reemplazados o movidos de un sistema a otro **Recuperabilidad:** Los datos se mantiene y preservan un nivel especificado de operaciones y de calidad, incluso en caso de fallo

**Inherentes y dependientes del sistema**

**Accesibilidad:** Se puede acceder a los datos, en especial por personas con discapacidades **Cumplimiento:** Los datos se adhieren a estándares convenciones o normas

**Confidencialidad:** Los datos son accesibles e interpretados por los usuarios autorizados

**Eficiencia:** Los datos pueden ser procesados y proporcionan el nivel de rendimiento esperado **Precisión:** Los datos son exactos

**Trazabilidad**: Los datos proporcionan la información necesaria para poder auditar los accesos y las modificaciones que se les han realizado

**Compresibilidad** Los datos pueden ser leído e interpretados por los usuarios

ISO 9001: Determina los requisitos mínimos para un Sistema de gestión de la calidad orientado a asegurar: conformidad del producto, aumentar la satisfacción del cliente y la mejora de la eficacia del sistema.

»Enfocada al cliente

»Liderazgo

»Participación del personal

»Enfoque basado en procesos

»Enfoque de sistemas para la gestión

»Mejora continua

»Enfoque basado en hechos para la toma de decisión

»Relaciones mutuamente beneficiosas con los proveedores

Auditoria

**Razones para realizar auditorías de sistemas de información (SI):**

Los motivos por los cuales queremos realizar auditorías son: Costos por Perdida de datos, toma de decisiones incorrectas, abusos computacionales, errores de computación, valor de hardware/software/personal, mantenimiento de privacidad.

**Costos por pérdidas de datos:** Evitar pérdidas de datos como por ejemplo cuentas bancarias. Esto podría reducir la confianza en la organización.

**Toma de decisiones incorrectas:** La alta calidad en la toma de decisiones depende de la calidad de los datos y la calidad de las reglas de decisión.

Los sistemas informáticos deben tener reglas de decisión exactas definidas por personas con gran interés en la organización ya que una regla de decisión incorrecta puede generar por ejemplo perdidas millonarias.

**Costos por 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.

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: 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

3) acceso físico ilegal: Una persona logra un acceso físico no autorizado a facilidades del computador. Pudiendo dañarlo o robar información

4) abuso de privilegios: Una persona usa privilegios, que le han sido asignados, para propósitos no

autorizados. Ejemplo: hacen copias no autorizadas de los datos a los cuales se les otorgó

acceso.

**Costos por errores de computación:** Los costos por errores de computación pueden ser altos, como por ejemplo un cohete que explota, un respirador que falla, etc.

**Valor de hardware/software/personal:**

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?

**Mantenimiento de privacidad:** Muchos datos se recolectan en los SI sobre las personas, es importante que no se divulguen.

**Evolución controlada del uso:**

Se argumenta que la confiabilidad de los sistemas computarizados complejos no está garantizada. Las consecuencias de usar sistemas no confiables pueden ser catastróficas.

Debe existir interés para evaluar y controlar la implementación de esta tecnología.

**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.

También busca asegurar que la organización cumple con determinadas regulaciones, reglas y condiciones, ya sea voluntaria o involuntariamente

Impacto de la auditoría en SI:

**Salvaguarda de activos:**

Los activos de los SI incluyen:

* hardware
* software
* facilidades
* personas (conocimientos)
* archivos de datos
* documentación de sistemas
* insumos

**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, y puede perder ventajas competitivas.

**El valor de los datos:**

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]

1. el grado en el cuál el ítem de dato es compartido entre los tomadores de decisiones
2. el valor del ítem de dato para los competidores

**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.

**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.

Los objetivos de la auditoría solo se pueden lograr si se implementa un sistema de gestión interno.

Un sistema de control interno incluye:

1. separación de obligaciones (sistema manual personas realizan las tareas, Sistema automatizado, el programa realiza todo, se deben separar bien las obligaciones)
2. delegación clara de autoridad y responsabilidades: Es difícil de lograr en un sistema automatizado, tiene que estar bien definido para solventar los problemas de control de los sistemas
3. reclutamiento y entrenamiento de personal calificado: El personal tiene mucho poder y responsabilidad ya que se les confían sistemas influyentes
4. sistema de autorizaciones: Se establecen dos tipos, autorizaciones generales (Políticas que la organización debe seguir, como lista de precios) y 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.

1. documentos y registros adecuados: en un sistema automatizado bien diseñado debería haber mayores registros de auditoría que en un sistema manual, hay que implementar control de acceso para asegurar que los registros sean exactos y completos.
2. Control de acceso físico: En sistema manual los registros están esparcidos pero la supervisión gerencial es fácil, en sistemas automatizados los registros pueden estar todos en un mismo lugar, pero la supervisión debe hacerse remotamente, el gerente debe acceder a los registros de auditoría para evaluar la gestión de los empleados
3. chequeos independientes de performance: En sistemas manuales una persona ayuda a detectar errores, en automatizados los programas siempre ejecutan el mismo código. Los auditores deben evaluar los controles establecidos para desarrollar, modificar, operar y mantener programas.
4. comparación periódica de activos con registros contabilizados: 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. Ejemplo: control de inventarios. Nuevamente, son importantes la implementación de estos controles durante el desarrollo de sistemas.

Computación en auditoría

La función de auditoría no cambia en SI.

Es más complicado recolectar evidencia y evaluar las consecuencias de las fortalezas y debilidades de los controles en pro de la confiabilidad general del sistema.

Los errores en los sistemas automáticos suelen ser:

Determinísticos (siempre mismo resultado), se generan a mayor velocidad y es más costoso arreglarlos.

Ejemplo: un programa erróneo siempre se va a ejecutar erróneamente. Los controles internos que aseguran la alta calidad en el diseño, implementación, operación y mantenimiento de los sistemas, son críticos.

Fundamentos de la auditoría de SI

**1-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.

**2-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.

**3-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.

**4-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.

Controles de sistemas:

Para poder auditar una compañía se necesita implementar sistemas de control.

Un control es un sistema que previene, detecta y corrige eventos ilegales.

Un control es un sistema, una password por sí sola no es un control, necesita validación, almacenamiento seguro, etc.

Un evento ilegal puede surgir de un ingreso de input no autorizado, inexacto o incompleto, o también del sistema transformando de manera errónea el input.

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.

La auditoría del sistema busca reducir la probabilidad que los eventos ilegales ocurran (controles preventivos) y reducir las pérdidas en caso de que ocurran (controles detectivos y correctivos).

Esta tarea de auditoría de sistemas puede ser compleja, por eso se sugiere:

* Factorizar el sistema en subsistemas.
* Determinar la confiabilidad de cada subsistema

Factorización

El proceso de factorización termina cuando los subsistemas pueden entenderse y evaluarse.

Un subsistema es un componente lógico de un sistema que permite realizar funcionas básicas que atienden al objetivo general del sistema.

Criterios de factorización:

Para factorizar se necesita un criterio, por ejemplo, por funciones, que consta que un subsistema es la función que realiza.

Criterio acoplamiento: Cada subsistema debería ser relativamente independiente de otros subsistemas. Estos subsistemas pueden desarrollar por completo una tarea.

Criterio Cohesión: Cada subsistema debe ser internamente cohesivo. Cada subsistema tiene una función, y en conjunto cumplen 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.
2. funciones de aplicación-tareas que son necesarias ejecutar para realizar un procesamiento de información confiable. Relacionado con “ciclos”.

Factorización en base a funciones generales

**Alta Gerencia:** Debe asegurar que las funciones de los SI estén bien administradas. Decisiones de políticas a largo plazo de cómo serán usados los SI.

**Gerencia de Sistemas de Información:** Responsabilidad general de planificar y controlar todas las actividades de los SI. Aconseja a la alta gerencia de las decisiones políticas de largo plazo y las traduce en metas y objetivos de corto plazo.

**Gerencia de Desarrollo de Sistemas:** Responsable del diseño, implementación y mantenimiento de los sistemas.

**Gerencia de Programación:** Responsable de la programación de nuevos sistemas, mantenimiento de los viejos y soporte general.

**Administración de Datos:** Responsable de lograr los objetivos de planificación y control en relación al uso de los datos de la organización

**Gerencia de Aseguramiento de Calidad:** Responsable de asegurar que el desarrollo, operación y mantenimiento de los sistemas es conforme a los estándares de calidad establecidos.

**Administración de Seguridad:** Responsable por los controles de acceso y seguridad física de las funciones de los SI.

**Gerencia de Operaciones:** Responsable de la planificación y control de las operaciones diarias.

Factorización en base a funciones de aplicación

En la factorización en base a funciones de aplicación, los sistemas de información de una organización se dividen en ciclos, estos varían según la organización, pero son, por ejemplo:

Ventas y cobranzas, compras y pagos, producción, inventario y almacenaje, etc.

Cada ciclo puede ser factorizado en uno o más sistemas de aplicación, por ejemplo, ventas puede dividirse en Administración de clientes, captura de pedidos, facturación.

Los distintos subsistemas serían:

**Limítrofe:** Componentes que establecen las interfaces entre el usuario y el sistema.

**Input:** Componentes que capturan, preparan e ingresan comandos y datos al sistema.

**Comunicaciones**: Componentes que transmiten datos entre los subsistemas y sistemas.

**Procesamiento**: Componentes que realizan toma de decisiones, cálculos, clasificación, ordenamiento y sumarización de datos dentro del sistema.

**Base de Datos:** Componentes que definen, agregan, acceden, modifican o eliminan datos.

**Output:** Componentes que buscan y presentan los datos al usuario.

Confiabilidad de controles

Para evaluar la confiabilidad de los controles hay que identificar todos los posibles eventos que pueden ocurrir en el subsistema, separando los ilegales de los válidos.

Para identificar los eventos hay que considerar las principales funciones del subsistema, y para cada función hay que analizar cómo debería realizarse y evaluar cómo el subsistema cumple con esa visión o normativa.

* 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. Ejemplo: toma de pedidos.
* 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

Para procesar una transacción se aplican técnicas de walkthrough

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.

Como hacer esto para TODAS las transacciones es muy costoso se agrupan las transacciones en clases:

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.

Una vez realizado esto se identifican casi todos los eventos que puedan surgir en un sistema, luego se evalúa si los controles están correctamente ubicados y si pueden detectar los eventos ilegales.

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.

Para esta tarea se publican tablas que muestran, por ejemplo, las caídas en los sistemas, errores e irregularidades en las distintas transacciones.

Las tablas muestran los controles que se pueden realizar para reducir las pérdidas esperadas por errores o irregularidades.

Para estimar la confiabilidad de los controles se evalúa primero los subsistemas de menor nivel y se escala hacia los de mayor nivel

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

Pero todo esto es para evaluar controles ya existentes, a medida que se evalúan los sistemas se pueden encontrar nuevos controles debido a:

Controles en sistemas de bajo nivel que funcionan mal, podría ser más efectivo en costos hacer controles de alto nivel y quitar los de bajo nivel, o eventos que no se muestran ilegales en bajo nivel pero si alto nivel.

Riesgos de la auditoría

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

1) Riesgo Deseado Auditoría (RDA): el riesgo que se desea correr.

2) Riesgo Inherente(RI): 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(RC): 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(RD): refleja la probabilidad que los procedimientos de auditoría utilizados en algún segmento, fallen en detectar pérdidas materiales o imputaciones erróneas.

Primero se evalúan las consecuencias de fracasar en detectar las pérdidas materiales reales o potenciales, y en base a esto se asigna el nivel de RDA

Luego se considera el nivel de RI, para eso se consideran factores como la naturaleza de la organización (posición en el mercado), la industria en la que opera, características del gerenciamiento, y los intereses contables y de auditoría.

Luego se consideran los Riesgos Inherentes asociados con diferentes segmentos de la auditoría. Para cada segmento se consideran:

* sistemas financieros
* sistemas estratégicos
* sistemas de operación crítica
* sistemas de tecnología avanzada

**RI de sistemas financieros:**

* Proveen controles financieros sobre los principales activos de la organización.
* Poseen alto RI.
* Son el blanco de acciones delictivas y fraudes.
* Ejemplo: sistema de facturación

**RI de 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.
* Ejemplo: el sistema que soporta la operatoria comercial de una empresa

**RI de sistemas críticos:**

* Aquellos sistemas que pueden paralizar a la organización si fallan.
* Generalmente tienen alto RI.
* Ejemplo: sistemas de control de producción, sistemas de reservas.

**RI de sistemas avanzados:**

* 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 protectoras, por encima de los controles de aplicación.

El buen nivel de los controles externos garantiza el nivel de los controles internos.

Los controles gerenciales se evalúan en general, y no para cada aplicación.

RD

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.

El proceso de una auditoría de SI

Existen diferentes procedimientos de auditoría, dependiendo de lo que se desee controlar:

1) determinar si ocurrieron **pérdidas** materiales o la **información financiera es errónea**

2) determinar la eficiencia y eficacia de las operaciones

**Pérdida o información 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: Los procedimientos incluyen cuestionarios, inspecciones y observaciones para determinar: Si los controles existen, analizar cómo están diseñados y si funcionan.

2) testeo de controles: Son para evaluar si los controles están actuando efectivamente.

3) testeos substantivos de detalle de transacciones: Diseñados para detectar errores monetarios o irregularidades en transacciones que afectan los estados financieros, por ejemplo, controlar facturación.

4) testeos substantivos de detalle de balances contables: Se focalizan en los registros contables finales (balance).

5) 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).

**Eficiencia y Eficacia**

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.

Pasos de una auditoría

La primera etapa es la planificación, las tareas dependen de si se realiza una auditoría **interna** o **externa.**

**Auditoría interna**

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

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

**Auditoría externa**

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

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

Tareas de planificación

1) determinar el alcance de la auditoría: Determinar qué se va a auditar: un sistema, un conjunto de sistemas, un área de la 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, este depende del segmento a auditar, para cada segmento evaluar los factores que conducen a RI, como, por ejemplo: Sistema con majeo de efectivo.

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.

Controles internos:

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.

Ejemplos:

-filosofía y estilo de gerenciamiento y operación,

-formas de asignar autoridad y responsabilidad,

-métodos para monitorear performance…

EVALUACIÓN DE RIESGO: Incluye evaluar los elementos que identifican y analizan los riesgos a los cuales se enfrenta la organización y cómo son administrados.

Ejemplos: 1) planificaciones de proyectos 2) documentos de administración de riesgos

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:

**controles contables:** elementos que operan para asegurar distintos niveles de autorizaciones y responsabilidades

**controles administrativos:** elementos para asegurar eficiencia y eficacia.

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.

Ejemplos: notificaciones, minutas de reuniones.

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

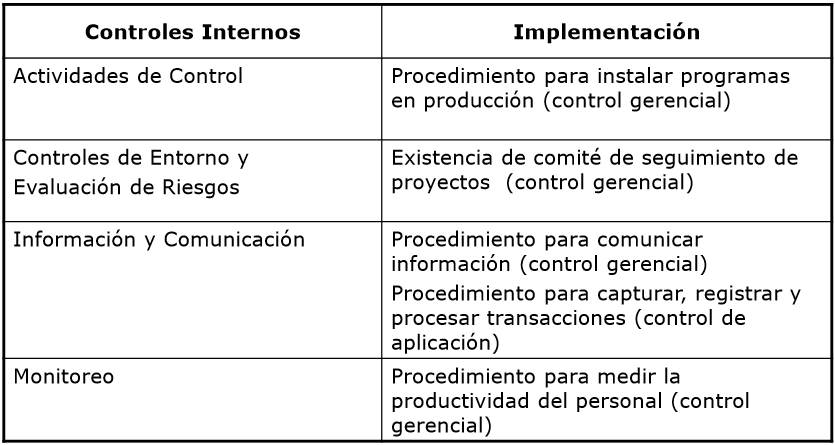
Ejemplos:

1) monitoreos de performance,

2) control de calidad

Comprender los controles internos incluye factorizar y examinar los controles gerenciales y de aplicación.

Los controles gerenciales varían sustancialmente de organización a organización. Ejemplo: los controles gerenciales son distintos si la empresa tiene: sistemas centralizados o descentralizados.



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

6) recolectar evidencia, tiene distintas técnicas:

* revisión de papeles de trabajo de auditorías previas
* entrevistas con alta gerencia y personal superior
* observación de cómo se desarrollan las actividades
* revisión de documentación de sistemas

7) documentar evidencia

La evidencia se documenta:

* completando cuestionarios
* construyendo diagramas de flujo de alto nivel
* construyendo tablas de decisión
* redactando descripciones narrativas.
* 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 es menor que 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

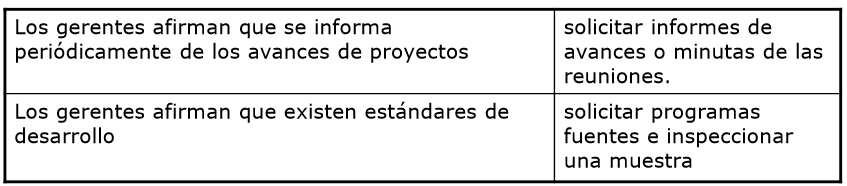
El testeo de controles evalúa cuan confiables y específicos son los controles.

Se testean, sólo si el RC se determinó menor al máximo.

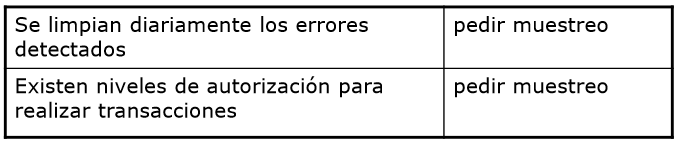
Se confía en los controles como una base para reducir el costo de un testeo más amplio.

A esta altura, los auditores no saben si los controles identificados operan efectivamente.

**Testeo de Controles gerenciales:** Se comienza por estos, ya que si los controles gerenciales demuestran que no operan eficientemente entonces no tiene sentido testear los controles de aplicación



**Testeo de Controles de aplicación:** Si los controles gerenciales funcionan efectivamente, se procede a evaluar los controles de la aplicación.



Conclusión de testeo de controles:

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

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.

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.

Un informe de auditoría 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.