**Ultra Resumen Final de Ingeniería III**

**Calidad**

La calidad no tiene una definición en concreto, pero una definición puede ser:

“El grado de uso de un producto o servicio presenta ausencia de defectos e imperfecciones y completa o conforma los requerimientos explícitos e implícitos de un cliente/usuario, logrando la satisfacción del mismo”

En una empresa existen diferentes áreas en las cuales se tiene que establecer una norma de calidad. Calidad de la Empresa:

* Calidad de los procesos de negocio (no se estudia)
* Calidad de los Sistemas de Información(SI)
  + Calidad de la Infraestructura: incluye, por ejemplo, la calidad de las redes, y sistemas de software.
  + Calidad de Software: de las aplicaciones de software construidas, o

mantenidas, o con el apoyo de IS.

* + Calidad de Datos: Que ingresan en el sistema de información.
  + Calidad de Información : está relacionada con la calidad de los datos.
  + Calidad de gestión : incluye el presupuesto , planificación y programación.
  + Calidad de servicio : incluye los procesos de atención al cliente

Dentro de la calidad de Software se pueden clasificar en 2 tipos diferentes, y dentro de las mismas podemos ver los requisitos o aspectos que abarcan cada uno:

* Calidad de Producto de software
  + Calidad Interna
  + Calidad Externa
  + Calidad de Uso
* Calidad de Proceso de software
  + Que produzca los resultados esperados.
  + Que estén basados en una correcta definición.
  + Que sean mejorados en función de los objetivos de negocio.

La calidad de proceso busca que el proceso produzca los resultados esperados en base al producto que se desea lograr, siendo los procesos, basados en una correcta definición y que estos sean mejorados en función de los objetivos de negocio.

Las metas que se establezcan para el producto deseado va a comprometer el objetivo del proceso de desarrollo

**Atributos de la calidad interna/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.
* Usabilidad: 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.

**Atributos de la calidad en uso:**

* Efectividad: Capacidad del producto software para permitir a los usuarios alcanzar objetivos especificados con exactitud y completitud, en un contexto de uso especificado.
* Productividad: Capacidad del producto software para permitir a los usuarios gastar una cantidad adecuada de recursos con relación a la efectividad alcanzada, en un contexto de uso especificado.
* Seguridad física: Capacidad del producto software para alcanzar niveles aceptables del riesgo de hacer daño a personas, al negocio, al software, a las propiedades o al medio ambiente en un contexto de uso especificado.
* Satisfacción: Capacidad del producto software para satisfacer a los usuarios en un contexto de uso especificado.

**Normas y Modelos de calidad**

**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 término 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, fundada en 1947 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,electrónico y tecnologías relacionadas. Fundada en 1906 que en la actualidad cuenta con 83 países miembros.

**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.

**Familia de las ISO**

* Calidad de Producto software:
  + ISO/IEC 9126 - ISO/IEC 14598 - ISO/IEC 25000
* Calidad de Proceso software
  + ISO/IEC 12207 - ISO/IEC 15504 – ISO/IEC 29110
* Sistema de gestión de la calidad de software
  + ISO/IEC 9001 - ISO/IEC 90003

**Calidad del Producto**

IRAM-NM- ISO/IEC 9126 – Calidad de Producto de software. Está dividida en 4 partes:

* IRAM-NM- ISO/IEC 9126-1: Modelo de Calidad
* IRAM-NM- ISO/IEC 9126-2: Métricas Externas
* IRAM-NM- ISO/IEC 9126-3: Métricas Internas
* IRAM-NM- ISO/IEC 9126-4: Métricas de calidad de uso.

IRAM-ISO/IEC 14598 – Evaluación del producto de software. Está dividida en 6 partes:

* IRAM - ISO/IEC 14598-1 Descripción General.
* IRAM - ISO/IEC 14598-2 Planificación y Gestión.
* IRAM - ISO/IEC 14598-3 Proceso para desarrolladores.
* IRAM - ISO/IEC 14598-4 Proceso para compradores .
* IRAM - ISO/IEC 14598-5 Proceso para evaluadores
* IRAM - ISO/IEC 14598-6 Documentación de los módulos de evaluación

**Calidad de los datos**

Calidad de datos se refiere a los procesos, técnicas, algoritmos y operaciones encaminados a mejorar la calidad de los datos existentes en empresas y organismos**.**

ISO/IEC 25012 (datos): La norma entiende por calidad de datos a la capacidad de las características de los datos de satisfacer necesidades explícitas e implícitas bajo determinadas condiciones de uso.

**Puntos de vista:**

* Inherente: Capacidad de las características de los datos de tener el potencial intrínseco para satisfacer las necesidades explícitas e implícitas.
  + 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
* Dependiente del sistema: Capacidad del sistema informático de alcanzar y preservar la calidad de los datos cuando los datos se utilizan en determinadas condiciones
  + 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 mantienen y preservan un nivel especificado de operaciones y de calidad, incluso en caso de fallo
* Inherentes y dependientes
  + 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 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

**Modelo de Calidad de los Procesos Software**: Un modelo de calidad software puede definirse como una herramienta que guía a las organizaciones a la mejora continua y a la competitividad, proporcionando un conjunto de buenas prácticas para el ciclo de vida del software. Un modelo no es una metodología, dice qué hacer pero no cómo hacerlo.

**SGC - Sistema de gestión de la calidad IRAM – ISO 9001:2008/2015**

Los Sistemas de Gestión de la Calidad son un conjunto de normas y estándares internacionales que se interrelacionan entre sí para hacer cumplir los requisitos de calidad que una empresa requiere para satisfacer los requerimientos acordados con sus clientes a través de una mejora continua, de una manera ordenada y sistemática.

**ISO 9001:** Determina los requisitos mínimos para un SGC orientado a asegurar:

conformidad del producto aumentar la satisfacción del cliente la mejora de la eficacia del sistema

**Auditoría**

**Parte 1**

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.

aunque también se puede enfocar en “asegurar que la organización  
cumple con determinadas regulaciones, reglas y condiciones, ya sea voluntaria o  
involuntariamente”.

Impacto de la auditoría:

* *Mejora la salvaguarda de activos:* hardware, software, facilidades, personas (conocimientos), archivos de datos ,documentación de sistemas, insumos.
* *Mejora la integridad de los datos*: Es un estado en el cual los datos poseen ciertos atributos: completitud, consistencia, veracidad, correctitud.

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 dato es compartido entre los tomadores de decisiones
3. El valor del dato para los competidores

* Mejora la efectividad de los sistemas:

Un sistema de información es efectivo si satisface sus objetivos.

Formas de evaluar la efectividad de los sistemas:

* durante el proceso de desarrollo para garantizar que se satisfacen los requerimientos de los usuarios
* 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.

* Mejora la 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**, que incluye:

1. *separación de obligaciones*: En un sistema automatizado, es el mismo programa el que realiza todas las funciones. 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
4. *sistema de autorizaciones*: La gerencia debe establecer dos tipos de autorizaciones: Generales o Específicas. 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
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. 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 sistemas automatizados es más complicado recolectar evidencia. Los errores en los sistemas automáticos tienden a ser determinísticos, 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:**

*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 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.

*Ciencias del comportamiento*: Una resistencia de comportamiento para con el sistema pone en peligro los objetivos de la auditoría. Usuarios descontentos pueden intentar sabotaje. 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. 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.

**Parte 2**

CONTROLES: Un control es un sistema que previene, detecta, o corrige eventos ilegales.

Aspectos claves en la definición de control:

1. Un control es un sistema:
2. Control de 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.

**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:

* Controles preventivos: reducen la probabilidad que estos eventos ocurran.
* 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.

Para administrar la complejidad, se sugiere:

**1)-Factorizar el sistema en subsistemas**: El primer paso para comprender un sistema complejo es particionarlo en subsistemas. Un subsistema es un componente de un sistema que:

* realiza ciertas funciones básicas necesarias para el sistema en general
* le permite atender sus objetivos fundamentales.

Los subsistemas son componentes lógicas y no físicas. El proceso de particionar en subsistemas se denomina factorización.

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. 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.

Además de las funciones, existen otras dos guías:

* **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:**

* 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.
* Funciones de aplicación: tareas que son necesarias ejecutar para realizar un procesamiento de información confiable. Los sistemas de información que soportan una organización, se dividen en ciclos. Cada ciclo es factorizado en uno o más sistemas de aplicación.

**2)-Determinar la confiabilidad de cada subsistema,** y las implicancias de cada uno de ellos en el nivel de confiabilidad general del sistema.

* Determinar el menor nivel de los subsistemas.
* Evaluar la confiabilidad de los controles en cada subsistema.

Confiabilidad de los 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. 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.

**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,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. Sí puede ocurrir un error material o una irregularidad.

**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: el impacto, la naturaleza, y la frecuencia de los eventos ilegales en los sistemas de mayor nivel.

**Pasos para estimar la confiabilidad:** 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**

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

**Tipos de riesgos:**

* Riesgo Deseado: el riesgo que se desea correr.
* 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
* 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.
* Riesgo de Detección: refleja la probabilidad que los procedimientos de auditoría utilizados en algún segmento, fallen en detectar pérdidas materiales o imputaciones erróneas.

**Riesgo deseado de una auditoria**: Primero los auditores eligen el nivel de RDA. Evalúan las consecuencias de fracasar en detectar las pérdidas materiales reales o potenciales.

**Riesgo inherente de sistemas:** 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 (¿la industria está sujeta a cambios rápidos?)

las características del gerenciamiento (¿es agresivo y autocrático?)

intereses contables y de auditoría (¿se usan técnicas?)

* Riesgo inherente de sistemas financieros: Proveen controles financieros sobre los principales activos de la organización. Poseen alto RI. Son el blanco de acciones delictivas y fraudes.
* Riesgo inherente de sistemas estratégicos: Proveen ventajas competitivas para la organización. Tienen alto RI. Son blanco de espionaje industrial, o acciones indebidas de la competencia.
* Riesgo inherente de sistemas críticos: Aquellos sistemas que pueden paralizar a la organización si fallan. Generalmente tienen alto RI.
* Riesgo inherente de sistemas de tecnología avanzada: Sistemas que usan tecnología de punta. Tienen alto RI, debido a la falta de experiencia en ese tipo de sistemas.

**Riesgos de control**: 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.

Controles 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

**Riesgos de detección:** 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:

* los auditores no recolectan la cantidad de evidencia que ellos desearían
* deben ser astutos para determinar en dónde aplicar los procedimientos de auditoría, y cómo interpretar la evidencia recolectada.

**Parte 3**

**PROCEDIMIENTOS DE UNA AUDITORÍA**

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

* 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, 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: Los testeos substantivos de detalle de transacciones están diseñados para detectar: errores monetarios o irregularidades, en transacciones que afectan los estados financieros.
4. testeos substantivos de detalle de balances contables: Los tests substantivos de detalle de balances contables se focalizan en los registros contables finales, en el balance.
5. 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.

* Determinar la eficiencia y eficacia de las operaciones

se utilizan tipos de 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.
5. procedimientos de revisión analítica. Ejemplo: modelos de simulación.

**Pasos de una auditoría**. La primera etapa es la planificación. Las tareas que se realizan en esta etapa varían dependiendo si es una:

* **Auditoría interna:** 
  + La etapa de planificación incluye:
    - asignar personal adecuado a las auditorías
    - obtener información del cliente
    - realizar procedimientos de revisión analíticos para comprender el negocio del cliente
    - identificar áreas de riesgo

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

* **Auditoría externa**: La etapa de planificación incluye:
  + investigar nuevos clientes
  + asignar personal adecuado a las auditorías
  + obtener el contrato
  + obtener información del cliente
  + realizar procedimientos de revisión analíticos para comprender el negocio del cliente
  + identificar áreas de riesgo

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

**Testeo de controles**: El testeo de controles evalúa cuán 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 los controles gerenciales. Si los controles gerenciales, demuestran contrariamente a lo supuesto, que no operan eficientemente 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: 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.

Los estándares en varios países requieren que la opinión sea:

* **opinión excusada**: en base al trabajo realizado no se puede emitir opinión.
* **opinión adversa**: se concluye que han ocurrido pérdidas materiales o que los estados financieros están distorsionados.
* **opinión con calificación**: se concluye que han ocurrido pérdidas materiales o existen registros incorrectos, pero las cantidades no son considerables.
* **opinión sin calificación**: el auditor considera que no han ocurrido pérdidas materiales o no existen registros incorrectos.

**Parte 4**

**Gobernanza y Peritaje**

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.

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 decisiones estratégicas de TI deben ser tomadas por una junta directiva corporativa

Las metas que busca la gobernanza son:

* asegurar que las inversiones en TI generen valor
* mitigar riesgos asociados con TI

**Conceptos Diferentes**

* Gobernanza TI: se trata de quien toma las decisiones en TI
* Administración TI: se trata de tomar e implementar las decisiones en TI.

**Cobit**

OBJETIVOS DE CONTROL PARA INFORMACIÓN Y TECNOLOGÍA RELACIONADA (COBIT) es un conjunto de recursos que contienen toda la información que las organizaciones necesitan para adoptar un marco de gobernanza y control de TI.

Principios de cobit

* 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.
* 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.
* 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.
* 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.
* 5) Separar las funciones principales
  + Establecer una distinción clara entre las funciones de gobernanza y administración.

**Procesos de Cobit (**2tipos**)**

**1- Procesos de la Gobernanza**

Contiene cinco procesos de gobernanza. Para cada proceso se definen prácticas de evaluar, dirigir y monitorear (**EDM**):

1. Asegurar el marco de gobernanza, el establecimiento y el mantenimiento
2. Asegurar la entrega de beneficios
3. Asegurar la optimización de riesgos
4. Asegurar la optimización de recursos
5. Asegurar la transparencia de las partes interesadas

Estos procesos aseguran 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**).

**2- Procesos de la Administración**

Cobit clasifica la administración en 4 dominios:

* Alinear,Planificar y Organizar(**APO**)
  + Proporciona direcciones a la entrega de soluciones y servicios. Abarca estrategias y tácticas y se interesa en la forma que TI puede contribuir a alcanzar los objetivos de negocio.
* Construir, Adquirir e Implementar(**BAI**)
  + Provee soluciones a DSS para la entrega de servicios. Abarca soluciones de TI que necesitan ser identificadas, desarrolladas o adquiridas, implementadas e integradas en el proceso de negocio
* Entrega de Servicio y de Soporte(**DSS**)
  + Recibe soluciones y las hace utilizables para los usuarios finales. Trata sobre la entrega efectiva de los servicios requeridos, incluyendo operaciones, seguridad y capacitaciones de continuidad.
* Monitorear y Evaluar(**MEA**)
  + Monitorea todos los procesos para asegurar que se siga la dirección provista. Trata de la evaluación regular de los procesos de TI para controlar su calidad y el cumplimiento de los requisitos de control.

**PERITAJE INFORMÁTICO:** Esclarecimiento de las cuestiones dudosas por medio de informes o dictámenes establecidos por el perito especialista en el área informática.

**Administración**

**(Parte 1)**

Proyecto: Es una secuencia de actividades complejas y conectadas que buscan cumplir un objetivo o propósito en un tiempo determinado, y con un presupuesto acorde a las especificaciones.

El resultado de un proyecto, es un producto o un “entregable” que cumple con las restricciones de costo, calidad y recursos empleados.

Características del proyecto:

1. Alcance limitado con productos concretos
2. Su éxito se mide por el presupuesto, tiempo de entrega y que tanto cumplen las especificaciones los productos.
3. Cantidad de cambios al proyecto (mantenerla al mínimo)
4. Es coordinado por un responsable que administra el tiempo, los recursos y el presupuesto.

Responsable del proyecto: Es el responsable de detectar las necesidades de los usuarios y gestionar los recursos económicos, materiales y humanos, para obtener los resultados esperados en los plazos previstos y con la calidad necesaria.

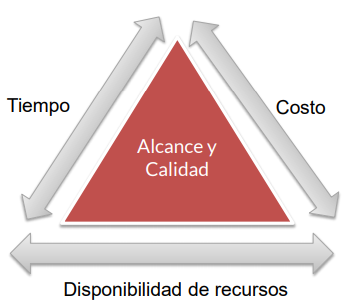
Para cumplir sus objetivos, un responsable de proyecto debe coordinar y motivar el trabajo en equipo de técnicos y especialistas y la comunicación con los interesados. Y realizar una planificación detallada para administrar la entrega de productos y servicios.

Tareas del responsable del proyecto:

1. Desarrollar el plan del proyecto
2. Identificar requerimientos y el alcance del proyecto
3. Comunicar y reportar a interesados
4. Administrar recursos humanos y materiales
5. Controlar tiempos
6. Identificar y controlar riesgos
7. Administrar costos y presupuesto
8. Asegurar de la calidad
9. Evaluar el desempeño del proyecto

Existen 5 parámetros/restricciones de un proyecto, y estas son interdependientes, lo que significa que un cambio en una, implica un cambio en las demás:

1. Alcance: Define los límites del proyecto (lo que se va a hacer y lo que no), puede cambiar, y es el líder del proyecto quien debe ajustar la planificación ante los cambios.
2. Calidad: Tiene en cuenta la calidad del producto y del proceso.
3. Costo: Presupuesto disponible para completar el proyecto.
4. Tiempo: Ventana de tiempo en la cual el proyecto debe terminarse
5. Recursos: Son los activos, como personas, equipos, hardware, etc.



Triángulo de alcance: El triángulo de alcance determina que el balance del: costo, tiempo y disponibilidad de recursos, van a definir el alcance y la calidad del proyecto.

Los proyectos son sistemas dinámicos que deben ser mantenidos en equilibrio.

Son controlados por el líder del proyecto y necesitan ser identificados de manera independiente.

Clasificación de proyectos:

1. Duración
2. Riesgo
3. Complejidad
4. Valor comercial
5. Costo

Administración: Es la planificación, la delegación, el seguimiento y el control de todos los aspectos del proyecto y la motivación de los participantes para alcanzar los objetivos del proyecto dentro de los objetivos de rendimiento esperados en términos de tiempo, costo, calidad, alcance, beneficios y riesgos.

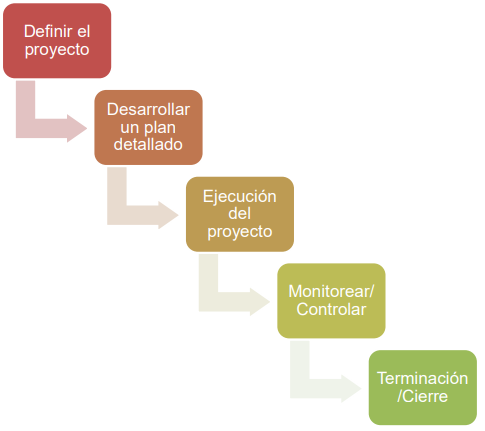
La administración de proyectos es la aplicación de conocimientos, habilidades, herramientas y técnicas a actividades de proyectos para satisfacer los requisitos del proyecto

La administración del proyecto se logra mediante el uso de los procesos tales como: **iniciar, planificar, ejecutar, controlar y cerrar.**

Principios de una buena administración:

1. Los proyectos siempre necesitan ser gestionados para tener éxito
2. El proyecto es un proceso finito con un comienzo y un final definidos
3. Se requiere un compromiso sincero de todos los interesados
4. Normalmente se requiere entrenamiento.

Ciclo de vida de un proyecto:



**Programa:**

* Es un grupo de proyectos relacionados que se gestionan de manera coordinada para obtener beneficios.
* Se ocupa de los resultados de los proyectos.
* Proporciona un paraguas bajo el cual estos proyectos pueden ser coordinados.
* Integra los proyectos de modo que pueda producir un resultado mayor que la suma de sus partes.

Los programas y proyectos se diferencian por sus características,

Las **características de proyecto** son:

* Los proyectos tienen un alcance limitado con productos concretos
* El director del proyecto trata de mantener el cambio al mínimo
* El éxito se mide por el presupuesto, el tiempo de entrega y los productos que cumplen las especificaciones
* El estilo de liderazgo se centra en la entrega de las tareas y orientado hacia el cumplimiento de los criterios de éxito
* Los gerentes de proyectos manejan técnicos, especialistas, etc.
* Los gerentes de proyecto son jugadores de equipo que motivan al personal

usando sus conocimientos y habilidades

* Los gerentes de proyecto realizan una planificación detallada para administrar

la entrega de productos y servicios

las **características de programa** son:

* Los programas tienen un amplio alcance que puede cambiar para satisfacer las expectativas de beneficios.
* Los directores de programas deben esperar cambios e incluso aceptarlos
* El éxito se mide en términos de retorno de la inversión (ROI), nuevas capacidades y prestaciones para la organización
* Los directores de programas deben facilitar y gestionar los aspectos políticos de la gestión de las partes interesadas
* Los directores de programas gestionan los líderes de proyectos
* El estilo de liderazgo se centra en la gestión de las relaciones y la resolución de conflictos
* Los directores de programas son líderes que proporcionan visión y liderazgo
* Los directores de programas crean planes de alto nivel que proporcionan orientación a los proyectos

**Relación** entre programas y proyectos:

* Interdependencias de tareas entre proyectos
* Limitaciones de recursos a través de múltiples proyectos
* Actividades de mitigación del riesgo
* Escalamiento de problemas, cambios de alcance, calidad, gestión de comunicaciones, riesgos, etc

**Administración**

**(Parte 2)**

WBS (Word Breakdown Structure): Es un modelo de descripción jerárquica del trabajo el cual divide un proyecto en diferentes actividades, que a su vez se subdividen en tareas para el cumplimiento de un proyecto. Este modelo permite:

1. Diseñar y planificar el trabajo: permite a los integrantes del equipo visualizar cómo puede definirse y administrarse el trabajo del proyecto
2. Diseñar la arquitectura: es un gráfico del trabajo del proyecto, muestra cómo se relacionan los distintos ítems de trabajo a realizar.
3. Planificar: se debe estimar esfuerzo , tiempos, y recursos para el último nivel.
4. Informar el estado del proyecto: es usada como una estructura para mostrar el grado de avance.

Formas de construcción:

Top down (equipo completo):

1. Todos los miembros del equipo participan de la descomposición.
2. Se comienza con el nivel 0 (el de la meta) y se particiona sucesivamente hasta que los participantes estén satisfechos de que el trabajo ha sido suficientemente definido.
3. Debido a que las actividades se definen con el suficiente nivel de detalle, las estimaciones de costo, tiempo y recursos son más exactas.
4. Una vez que las actividades se han definido, se deben secuenciar.
5. Se debe analizar qué actividades se pueden hacer concurrentemente.
6. Ventaja: brinda la oportunidad de que todos presten atención al WBS, y se discuta en el momento.

Top down (Sub-equipos):

1. El equipo completo acuerda la partición del primer nivel.
2. Se crean tantos sub-equipos como actividades haya en el nivel uno.
3. Cada sub-equipo particiona una actividad (se le asigna la actividad para la cual tenga más experiencia).
4. Un sub-equipo puede solicitar ayuda externa.
5. Demanda menos tiempo que el enfoque anterior.

Bottom Up (subequipod):

1. Se asemeja a una lluvia de ideas (brainstorming).
2. El equipo completo acuerda la partición del primer nivel
3. Se crean tantos sub-equipos como actividades haya en el nivel uno.
4. Cada sub-equipo particiona una actividad (se le asigna la actividad para la cual tenga más experiencia).
5. Cada grupo hace una lista de actividades en las cuales se descompone la actividad de nivel 1 asignada.
6. Los integrantes presentan ideas sobre las tareas que involucra cada una de esas sub-actividades.

Para determinar la completitud de una actividad, hay que considerar las siguientes 6 características:

* Estado medible: En cualquier momento se debería poder determinar el estado en que se encuentra.
* Acotada: evento de comienzo -> fecha de comienzo, evento de fin->fecha de fin
* Producir un entregable: Producto, documento, autorización para pasar a otra tarea, etc.
* Tiempo y costo estimable: Realizar la estimación de tiempo y costo para las tareas de menor nivel, permite luego agregar y calcular el costo y tiempo total del proyecto.
* Duración aceptable: Las tareas no deben tardar más de un tiempo determinado en completarse.
* Independiente: Una vez que se comenzó una actividad se debe poder continuar razonablemente sin interrupciones y sin la necesidad de un input adicional.

El modelo WBS puede construirse con 3 distintos enfoques, por sustantivos, por verbos y por enfoque organizacional.

Duración:

Duración: Es la cantidad de días laborables que toma completar una tarea.

Esfuerzo de Trabajo: Es la labor requerida para completar una actividad (puede medirse en horas).

La duración de una actividad es influenciada (existen otros aspectos a parte de los recursos, que permiten lograr la medición de la duración) por la cantidad de recursos planificados para trabajar en ella.

Se conoce como Crash de actividad al acto de asignar recursos a una actividad para mantener su duración dentro de los límites planificados.

Crashpoint de la Actividad: es el punto en el cual agregar más recursos aumenta la duración de la actividad.

Otra consideración importante es que al asignar recursos a una actividad hay que considerar el impacto del riesgo de esta decisión (puede aumentar el riesgo).

Variaciones de la duración de una actividad:

Existen 4 motivos por los cuales la duración de una actividad pueden variar:

1. Variación en los perfiles de las personas
2. Eventos inesperados (Demoras de proveedores, fallas de energía, enfermedades, etc.).
3. Eficiencia del tiempo de trabajo (Cuanto más interrupciones se den en el ambiente de trabajo, menor será la productividad.)
4. Errores e interpretaciones erróneas (Esto puede implicar rehacer trabajo ya hecho).

Métodos de estimación de la duración de una actividad

1- Similitud con otras Actividades: Estimar en base a las estimaciones de actividades similares de otros proyectos

2- Datos Históricos: Estimar en base a las estimaciones registradas de otros proyectos.

3- Juicio Experto: Las estimaciones las realizan consultores externos con experiencia en la metodología o tecnología.

4- Técnica Delphi: Es una técnica de grupo que extrae y resume el conocimiento del grupo para arribar a una estimación. Se le pide a cada miembro del grupo a que realice su estimación.

Esta técnica se aplica en 3 pasadas:

Pasada 1: Se expone la estimación de cada miembro en una tabla.

Pasada 2: Se defienden las posiciones extremas y luego de escuchar los argumentos, se les pide a los miembros que vuelvan a estimar.

Pasada 3: Se realiza una nueva estimación, se realizan ajustes finales, y se obtiene un promedio.

5- Técnica de 3 puntos: Estimación = (Optimista + 4\*Media + Pesimista)/6

6- Técnica de Delphi de Banda Ancha:

* Es una combinación de la técnica Delphi y la de 3 Puntos.
* Se basa en la técnica Delphi pero a cada integrante se le pide que haga las 3 estimaciones. Se recopilan los resultados y se eliminan los extremos
* Se calculan los promedios de optimistas, pesimistas y medias.
* Se calcula con la fórmula de 3 Puntos utilizando los promedios.

**Administración**

**(Parte 3)**

Costos:

Estimación de Costos: predicciones de cuánto tiempo, esfuerzo y perfiles de RRHH son requeridos para construir un sistema de software.

Técnicas de estimación:

Opinión Experta: toma ventaja de la experiencia de un personal de desarrollo senior.

Analogía: los estimadores comparan el proyecto propuesto con proyectos pasados.

Descomposición: El análisis se focaliza en el producto o en las tareas requeridas para construirlo.

Modelos: son técnicas que identifican contribuyentes claves al esfuerzo, generando fórmulas matemáticas que relacionan estos items al esfuerzo. (bottom-up. Top-Down).

La Estimación de Costos tiene dos usos:

1) en planificación: se necesita saber cuántos recursos va a insumir

2) en control: se necesita saber cuanto se hizo y cuánto falta

Cálculo de esfuerzo:

Se calcula mediante la fórmula: PM inicial= c KLOC k

El esfuerzo se puede corregir mediante **conductores de costos**, estos se clasifican en:

1) Atributos del Producto: confiabilidad, complejidad…

2) Atributos Computacionales: restricciones de tiempo de ejecución, de almacenamiento…

3) Atributos del Personal: existe personal experimentado …

4) Atributos del Proceso: se utilizan herramientas de software sofisticadas...

COCOMO (**Co**nstructive **Co**st **Mo**del):

Es una colección de tres modelos:

1) Básico: aplicable cuando se conoce muy poco del proyecto

2) Intermedio: aplicable luego de la especificación de requerimientos

3) Avanzado: aplicable cuando se termina el diseño

Los sistemas COCOMO se clasifican en:

* Orgánicos: involucra procesamiento de datos, uso de bases de datos y se focaliza en transacciones y recuperación de datos. Ejemplo: sistema de facturación
* Semi-embebido: entre orgánico y embebido – presenta mayor procesamiento de transacciones. Ejemplo: Monitoreo de una red
* Embebido: contiene software de tiempo real que es una parte integral de un sistema mayor basado en hardware. Ejemplo: control de ascensores

Una vez identificado el tipo de sistema del Sistema Informático, debemos elegir que modelo de COCOMO vamos a utilizar para estimar sus costos, esto dependerá de la cantidad de conocimiento que tengamos del proyecto.

**Modelo básico**: se utiliza para obtener una primera estimación del esfuerzo necesario para llevar a cabo el proyecto, se miden atributos como personas necesarias para realizar el proyecto y el tiempo de desarrollo.

En el **modelo intermedio**, para estimar el proyecto, además, se evalúan 15 distintos conductores de costos para incrementar la presición de la estimación, estos conductores se agrupan en 4 categorías:

1) atributos del producto (Rely, Data, Cplx)

2) atributos del hardware (Time, Stor, Virt, Turn)

3) atributos del personal (ACAP, PCAP, AEXP, VEXP, LEXP)

4) atributos del proyecto (MODP, TOOL, SCED)

El **modelo avanzado** de COCOMO va a clasificar los componentes del proyecto en una jerarquía entre módulo, sistema y subsistema, además va a separar el proyecto en 4 fases:

1) Requerimientos/planes: Se analiza el requerimiento, se muestra un Plan de Producto y se genera una especificación completa del producto.

2) Diseño del producto: COCOMO se preocupa de la determinación de la arquitectura del producto y de las especificaciones de los subsistemas.

3) Programación: COCOMO se subdivide en dos subfases: diseño detallado y prueba del código.

4) Prueba/integración: consiste principalmente en unir las diferentes unidades ya probadas.

Y por último aplica el modelo intermedio a cada componente para cada fase, para obtener una estimación de costos lo más precisa posible.

COCOMO 2.0 :

Objetivos:

1) Desarrollar modelos de costos y de estimación acordes a las prácticas actuales

2) Desarrollar bases de datos de costos y herramientas que soporten una mejora continua del modelo

3) Proveer un framework analítico cuantitativo, y un conjunto de herramientas y técnicas para evaluar los efectos de las mejoras en los costos de ciclos de vida y en las planificaciones

Modelos:

1) Modelo de la Aplicación: basado en Puntos Objeto

2) Modelo de Diseño Temprano: usado para obtener estimaciones de costo y duración antes de finalizar el diseño de la arquitectura

3) Modelo Post-Arquitectura: el modelo más detallado, con nuevos conductores de costos, y nuevas ecuaciones

COCOMO 2.0 provee un modelo para estimar costos en base a:

1) KLOC

2) Puntos Objeto (PO)

3) Puntos Función (PF)

Charla con la profe de inge 2:

Que la calidad de proceso, busca lograr un producto de calidad, también tiene que cumplir con ciertos requisitos que uno a impuesto para ese proceso especificamente.

Destacar que son totalmente dependientes.

Los requisitos que buscamos cumplir no son solo “los de la empresa”, también pueden ser los de la norma de calidad que se está tratando de cumplir. y/o los del cliente,

Nos van a preguntar, que ISOs

12207 y 15504 no sirven para medir, son las raíces de las demás, la que usa es la CMMI para grandes empresas y la 9001 con la guía 90003

29110 es la más nueva. es norma para medir la calidad del proceso.

Todas definen mejores prácticas.

La que mide la calidad del proceso es la 9001, que siendo aplicada bajo la guia de la 90003

La 9001 sirve para medir calidad de cualquier proceso, aplicada a la guia de la 90003, podemos medir la calidad del proceso de software.

Otro modelo para medir la calidad de proceso, es la 29110 para procesos de software de pymes.

**cmmi:**

CALIDAD DE PRODUCTO: 9126 se está dejando de lado. ahora se usa la 25000

14598