Proyecto

Un proyecto es una secuencia de actividades única, complejas y conectadas que tienen un objetivo o propósito y que deben ser completadas en un tiempo específico, dentro del presupuesto y de acuerdo a las especificaciones.

Es cualquier actividad que dé como resultado un producto o un “entregable”.

Es una organización temporal creada con el propósito de entregar uno o más productos empresariales dentro de las restricciones de costo, calidad y recursos.

Características

- Los proyectos tienen un alcance limitado con productos concretos.
- El éxito se mide por el presupuesto, el tiempo de entrega y los productos que cumplen las especificaciones.
- Durante la ejecución de un proyecto, se trata de mantener los cambios al mínimo.
- El proyecto es dirigido y coordinado por una persona responsable - líder o gerente de proyecto; quien administra el tiempo, los recursos y el presupuesto.

Responsable del proyecto

Líder de 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.

- Coordina el trabajo de técnicos y especialistas y la comunicación con interesados.
- Son jugadores de equipo que motivan al personal usando sus conocimientos y habilidades.
- Realizan una planificación detallada para administrar la entrega de productos y servicios.

Tareas del responsable del proyecto:

- Desarrollar el plan del proyecto.
- Identificar requerimientos y el alcance del proyecto.
- Comunicar y reportar a interesados.
- Administrar recursos humanos y materiales.
- Controlar tiempos.
- Identificar y controlar riesgos.
- Administrar costos y presupuesto.
- Asegurar la calidad.
- Evaluar el desempeño del proyecto.

Parámetros de un proyecto:

1. Alcance.
2. Calidad.
3. Costo.
4. Tiempo.
5. Recursos

Son interdependientes - un cambio en una, implica un cambio en las demás.

Alcance: es un enunciado que define los límites del proyecto. Dice lo que se va a hacer, pero implícitamente también dice lo que no se va a hacer.

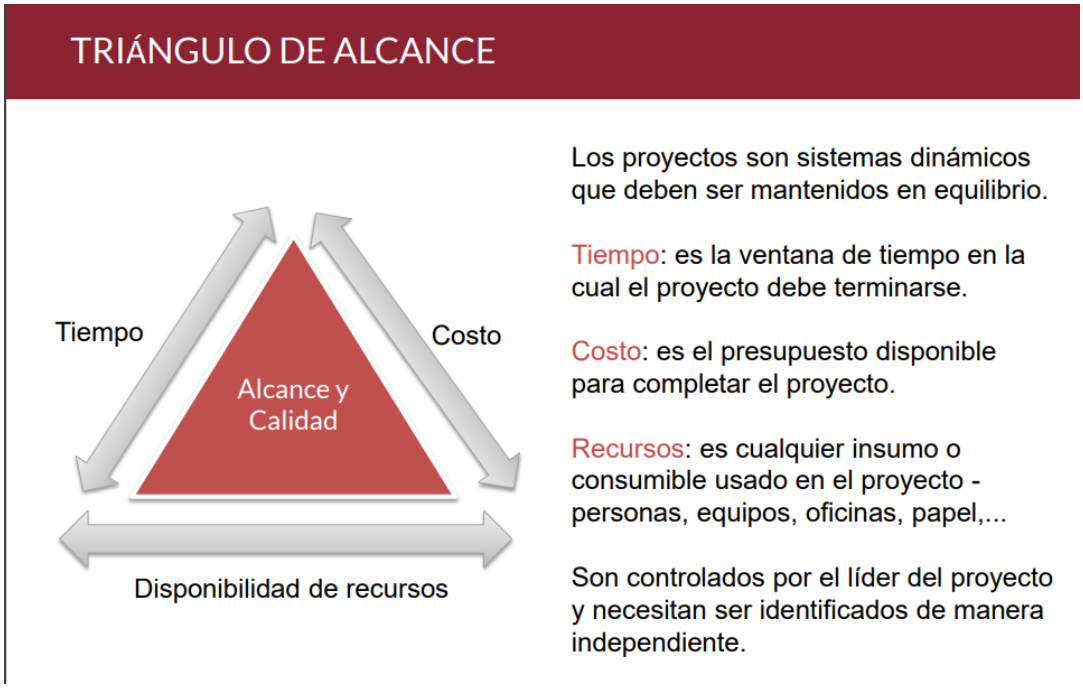
- es crítico que el alcance sea correcto.
- el alcance puede cambiar.

- en caso de que se produzca un cambio al alcance, detectarlo y decidir cómo acomodar el plan del proyecto es un desafío del líder de proyecto.

Calidad: Existen dos calidades a tener en cuenta en el desarrollo: Calidad del producto y Calidad del proceso.

Recursos: son activos, tales como personas, equipos, facilidades físicas, o artefactos necesarios para la realización del proyecto.

- tienen disponibilidad limitada, su uso puede planificarse, o puede ser contratado a una tercera parte.
- algunos son fijos y otros variables a largo plazo.
- son centrales a la planificación de las actividades del proyecto y para la finalización ordenada del mismo
- para los proyectos de desarrollo de sistemas, las personas constituyen el recurso más importante.



Clasificación de proyectos:

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

Administración de Proyectos

Definiciones:

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.

Se trata de las habilidades, herramientas y procesos de gestión necesarios para llevar a cabo un proyecto con éxito.

Administración de Proyectos de Software:

El objetivo de administrar un proyecto de software es aplicar buenos principios y técnicas de administración de proyectos y de ingeniería de software a fin de que el producto se entregue al mínimo costo, mínimo tiempo y sea de buena calidad.

Desafíos de la Administración de Proyectos:

- Alto nivel de innovación.
- Complejidad.
- Requerimientos ambiguos.
- Cumplir con plazos.
- Tratar con proveedores.
- Retener personal calificados.
- Administrar personal con diferentes niveles de productividad.

Principios de una buena administración:

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

Programa

Conceptos:

Es un grupo de proyectos relacionados que se gestionan de manera coordinada para obtener beneficios.

Se ocupa de los resultados.

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.

Diferencias entre Proyectos y Programas:

Proyectos	**Programas**
Los proyectos tienen un alcance limitado con productos concretos	Los programas tienen un amplio alcance que puede cambiar para satisfacer las expectativas de beneficios
El director del proyecto trata de mantener el cambio al mínimo	Los directores de programas deben esperar cambios e incluso aceptarlos
El éxito se mide por el presupuesto, el tiempo de entrega y los productos que cumplen las especificaciones	El éxito se mide en términos de retorno de la inversión (ROI), nuevas capacidades y prestaciones para la organización
El estilo de liderazgo se centra en la entrega de las tareas y orientado hacia el cumplimiento de los criterios de éxito	Los directores de programas deben facilitar y gestionar los aspectos políticos de la gestión de las partes interesadas

Los gerentes de proyectos manejan técnicos, especialistas, etc.	Los directores de programas gestionan los líderes de proyectos
Los gerentes de proyecto son jugadores de equipo que motivan al personal usando sus conocimientos y habilidades	El estilo de liderazgo se centra en la gestión de las relaciones y la resolución de conflictos
Los gerentes de proyecto realizan una planificación detallada para administrar la entrega de productos y servicios	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:

Un programa vincula proyectos de varias maneras:

- 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.

Calidad

Definiciones:

- Calidad es un concepto manejado con bastante frecuencia, su significado es percibido de distintas maneras.
- Al hablar de bienes y/o servicios de calidad, se relaciona normalmente con bienes de lujo, con precios elevados.
- Su significado sigue siendo ambiguo y muchas veces su uso depende de lo que cada uno entiende por calidad, por lo cual es importante comenzar a unificar su definición.
- Calidad es un concepto:
    - **Relativo**: La calidad está en los ojos del observador y es relativa a las personas, su edad y circunstancias, al espacio, tiempo, ...
    - **Multidimensional**: 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).
- Puntos de vista:
    - **TRASCENDENTAL**: es algo que se reconoce pero no se define. Se puede concebir como un ideal al que se intenta alcanzar.
    - **USUARIO**: es adecuación al propósito.

    - **FABRICANTE**: es conformidad con las especificaciones. Vista centrada en el proceso.
    - **PRODUCTO**: es una visión interna ya que se centra en los atributos internos de los productos.
    - **Basada en VALOR**:depende de la cantidad que el cliente esté dispuesto a pagar.
- La calidad realizada: la que es capaz de obtener la persona que realiza el trabajo.
- La calidad programada: la que se ha pretendido obtener.
- La calidad necesaria: la que el cliente exige.
- Propiedad o conjunto de propiedades inherentes a algo, que permiten juzgar su valor.
- A lo largo de la historia se han desarrollado filosofías o culturas de calidad, de las cuales algunas han sobresalido porque han tenido resultados satisfactorios.
- A los que realizaron estas filosofías se los ha llamado Maestros o Gurús de la Calidad. Entre estos destacan Walter Shewhart, Edward Deming, Joseph Juran, Juancito Ferrari, etc.
- Las principales normas internacionales definen la calidad como:
    - "El grado en el que un conjunto de características inherentes cumple con los requisitos " (ISO 9000)
    - "Conjunto de propiedades o características de un producto o servicio que le confieren aptitud para satisfacer unas necesidades expresadas o implícitas" (ISO 8402)

Calidad de los Sistemas de Información:

- La importancia de los sistemas de información (SI) en la actualidad hace necesario que las empresas de tecnología hagan mucho hincapié en los estándares de calidad.
- Stylianou y Kumar plantean que se debe apreciar la calidad desde un todo, donde cada parte que la componen debe tener su análisis de calidad.
- **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.

Calidad de Producto y de Proceso

Producto (Hatton, 1995): Un producto es un bien tangible que es el resultado de un proceso. Aunque el software tiene aspectos intangibles, un producto software es sin embargo un bien en sí mismo La estandarización del producto define las propiedades que debe satisfacer el producto software resultante.

Proceso: Conjunto de actividades, métodos, prácticas y transformaciones que la gente usa para desarrollar y mantener software y los productos de trabajo asociados.

Diferentes aspectos en la medición de la calidad del **producto**:

- **Calidad interna**: Medible a partir de las características intrínsecas, 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.

No obstante, 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. Sin un buen proceso de desarrollo es casi imposible obtener un buen producto.

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.
ISO-9001:2015 - Quality management system – Requirements Norma publicada por ISO en el año 2015.
IRAM-ISO 9001:2015 – Sistema de gestión de la calidad – Requisitos Norma publicada por ISO y traducida por IRAM. La traducción se publicó en el año 2015.
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. La norma en su idioma original data del año 1999 (ISO/IEC 14598 – 1:1999)

Modelo de Calidad SQuaRE ISO/IEC 25010

Se divide en:

- **Portabilidad:**

        - Adaptabilidad.
        - Capacidad para ser instalado.
        - Capacidad para ser reemplazo.
    - **Seguridad:**
        - Confiabilidad.
        - Integridad.
        - No repudio.
        - Responsabilidad.
        - Autenticidad.
    - **Facilidad de mantenimiento:**
        - Modularidad.
        - Reusabilidad.
        - Capacidad para ser analizado.
        - Capacidad para ser modificado.
        - Capacidad de ser probado.
    - **Compatibilidad:**
        - Coexistencia.
        - Interoperabilidad.
    - **Funcionalidad:**
        - Completitud funcional.
        - Corrección funcional.
        - Adecuación funcional.
    - **Confiabilidad:**
        - Madurez.
        - Disponibilidad.
        - Tolerancia a fallos.
        - Recuperabilidad.
    - **Facilidad de uso:**
        - Capacidad para reconocer su adecuación.
        - Capacidad para ser usado.
        - Capacidad de aprendizaje técnico.
        - Protección contra errores de usuarios.
        - Estética de la interfaz de usuario.
        - Accesibilidad técnica.
    - **Eficiencia:**
        - Comportamiento temporal.
        - Utilización de recursos.
        - Capacidad.

SQuaRE - Proceso de Evaluación - ISO/IEC 25040

1. Establecer los requisitos de la evaluación.
    a. Establecer el propósito de la evaluación.
    b. Obtener los requisitos de calidad del producto.
    c. Identificar las partes del producto que se deben evaluar.
    d. Definir el rigor de la evaluación.
2. Especificar la evaluación.
    a. Seleccionar los módulos de evaluación.
    b. Definir los criterios de decisión para las métricas.

    c. Definir los criterios de decisión de la evaluación.
3. Diseñar la evaluación.
    a. Planificar las actividades de la evaluación (incluye cronogramas, detalles de las funcionalidades y casos de prueba).
4. Ejecutar la evaluación.
    a. Realizar las mediciones.
    b. Aplicar los criterios de decisión para las métricas.
    c. Aplicar los criterios de decisión de la evaluación.
5. Finalizar la evaluación.
    a. Revisar los resultados de la evaluación.
    b. Crear el informe de evaluación.
    c. Revisar la calidad de la evaluación y obtener feedback.
    d. Tratar los datos de la evaluación.

Calidad de los Datos

Conceptos:

- 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.

Calidad de Datos ISO/IEC 25012

La norma entiende por calidad de datos:

La capacidad de las características de los datos de satisfacer necesidades explícitas e implícitas bajo determinadas condiciones de uso.

Los clasifica estas características de calidad considerando dos puntos de vista:

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.

Dependiente 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.

Inherente:

- 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.

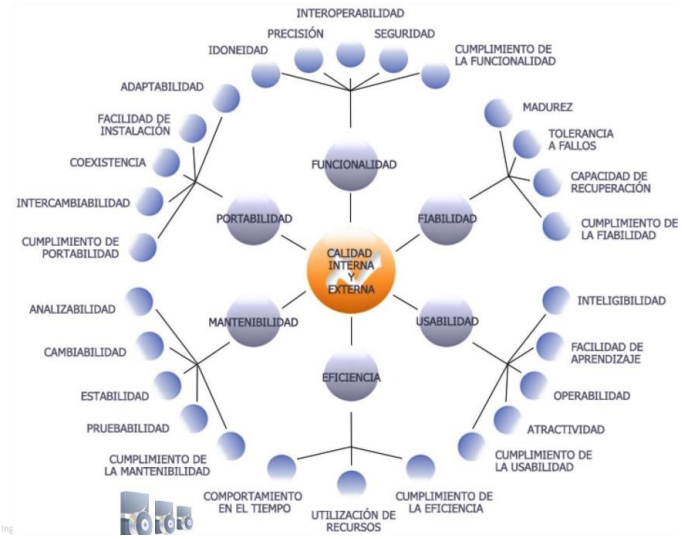
Dependientes del sistema:

- 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 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.

Calidad de Producto IRAM-NM- ISO/IEC 9126



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

- Idoneidad: Capacidad del conjunto apropiado de funciones para tareas y objetivos de usuario especificados.
- Precisión: Capacidad para proporcionar los resultados o efectos correctos o acordados, con el grado necesario de precisión.

- Interoperabilidad: Capacidad para interactuar con uno o más sistemas especificados.
- Seguridad: Capacidad para proteger información y datos de manera que las personas o sistemas no autorizados no puedan leerlos o modificarlos, al tiempo que no se deniega el acceso a las personas o sistemas autorizados.
- Cumplimiento de la funcionalidad: Capacidad para adherirse a normas, convenciones o regulaciones en leyes y prescripciones similares relacionadas con funcionalidad.

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

- Madurez: Capacidad para mantener un nivel especificado de prestaciones en caso de fallos software o de infringir sus interfaces especificados.
- Tolerancia a fallos: Capacidad para evitar fallar como resultado de fallos en el software.
- Capacidad de recuperación: Capacidad para restablecer un nivel de prestaciones especificado y de recuperar los datos directamente afectados en caso de fallo.
- Cumplimiento de la fiabilidad: Capacidad para adherirse a normas, convenciones o regulaciones relacionadas con la fiabilidad.

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

- Inteligibilidad: Capacidad que permite al usuario entender si el software es adecuado y cómo puede ser usado para unas tareas o condiciones de uso particulares.
- Facilidad de aprendizaje: Capacidad que permite al usuario aprender sobre su aplicación.
- Operabilidad: Capacidad del producto software que permite al usuario operarlo y controlarlo.
- Atractividad: Capacidad del producto software para ser atractivo.
- Cumplimiento de la usabilidad: Capacidad para adherirse a normas, convenciones, guías de estilo o regulaciones relacionadas con la usabilidad.

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

- Comportamiento en el tiempo: Capacidad para proporcionar tiempos de respuesta, tiempos de proceso y potencia apropiados, bajo condiciones determinadas.
- Utilización de recursos: Capacidad para usar las cantidades y tipos de recursos adecuados cuando el software lleva a cabo su función bajo condiciones determinadas.
- Cumplimiento de la eficiencia: Capacidad para adherirse a normas o convenciones relacionadas con la eficiencia.

Mantenibilidad: Capacidad del producto para ser modificado.

- Analizabilidad: Capacidad para serle diagnosticadas deficiencias o causas de los fallos en el software, o para identificar las partes que han de ser modificadas.
- Cambiabilidad: Capacidad del producto software que permite que una determinada modificación sea implementada.
- Estabilidad: Capacidad del producto software para evitar efectos inesperados debidos a modificaciones del software.
- Pruebabilidad: Capacidad del producto software que permite que el software modificado sea validado.
- Cumplimiento de la mantenibilidad: Capacidad del producto software para adherirse a normas o convenciones relacionadas con la mantenibilidad.

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

- Adaptabilidad: Capacidad para ser adaptado a diferentes entornos especificados, sin aplicar acciones o mecanismos distintos de aquellos proporcionados para este propósito por el propio software considerado.
- Facilidad de instalación: Capacidad del producto software para ser instalado en un entorno especificado.
- Coexistencia: Capacidad para coexistir con otro software independiente, en un entorno común, compartiendo recursos comunes.

- Intercambiabilidad: Capacidad para ser usado en lugar de otro producto software, para el mismo propósito, en el mismo entorno.
- Cumplimiento de portabilidad: Capacidad del producto software para adherirse a normas o convenciones relacionadas con la portabilidad.

Calidad de servicio - ISO/IEC 20000

- Estándar reconocido desde el 2005 para la certificación de Gestión de Servicios de TI de las Empresas.
- La serie 20000 proviene de la adopción de la serie BS 15000 desarrollada por la entidad de normalización y certificación británica BSI (British Standard Institute).
- El estándar comprende dos partes principales:
    - Parte 1: ISO/IEC 20000 - 1 : 2011 - Especificación.
    - Parte 2: ISO/IEC 20000 - 2 : 2012 - Código de Prácticas.
- Informes Técnicos de apoyo:
    - Parte 3: ISO/IEC 20000 - 3 : 2012 - Guía en la Definición del Alcance y su Aplicabilidad (informe técnico).
    - Parte 4: ISO/IEC 20000 - 4 : 2010 - Modelo de Referencia de Procesos (informe técnico).
    - Parte 5: ISO/IEC 20000 - 5 : 2010 - Ejemplo de Implementación (informe técnico).

¿Qué es un Proceso?

- Un proceso se define como un conjunto de actividades interrelacionadas que transforman entradas en salidas.
- Define Quién está haciendo Qué, Cuándo y Cómo para alcanzar un determinado objetivo.
- Transforma insumos en valor para sus clientes internos y externos. Atravesando la estructura organizacional.
- **ISO** lo define como: “Proceso o Conjunto de procesos usados por una organización o proyecto para planificar, gestionar, ejecutar, monitorizar, controlar y mejorar sus actividades de software relacionadas”.

Gestión por Procesos

Gestionar sus actividades con un enfoque basado en procesos proporciona a las organizaciones múltiples ventajas:

- Facilita la orientación al cliente.
- Mejora la eficacia y la eficiencia de las actividades.
- Ayuda a estructurar las actividades de la organización.
- Permite mejorar el seguimiento y el control de los resultados obtenidos.
- Facilita la planificación, el establecimiento de objetivos de mejora y la consecución de los mismos.

Proceso de software

Es importante diferenciar entre procesos organizativos, proceso de software y ciclo de vida.

- Ciclo de vida de software es un marco de referencia que contiene los procesos, las actividades y las tareas involucradas en el desarrollo, explotación y mantenimiento de un producto de software, abarcando la vida del sistema.
- El proceso de software es un concepto más amplio, basado en el ciclo de vida y cubre todos los elementos necesarios como tecnología, personal, artefactos, etc.
- Procesos organizativos incluye al contexto en el que funciona la organización el proceso de software.

Orientar la gestión de la organización mediante un enfoque por procesos requiere en primer lugar identificar cuáles son sus procesos y las relaciones existentes entre ellos.
Una organización puede describirse como un conjunto de procesos interconectados, que pueden plasmarse por escrito en un diagrama denominado Mapa de Procesos.

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, esto se debe a que estos modelos están pensados para que cada organización pueda adaptarlos según sus objetivos de negocio y las metodologías que utilice.

Principios de Gestión de la Calidad - SGC – IRAM – ISO 9001:2015

ENFOQUE EN EL CLIENTE

El objetivo principal de la Gestión de la Calidad es satisfacer las necesidades de los clientes y esforzarse por superar sus expectativas. El éxito sostenido se logra cuando una organización atrae y conserva la confianza de sus clientes y otras partes interesadas. Cada aspecto de la interacción con el cliente proporciona una oportunidad para crear más valor. Comprender las necesidades actuales y futuras de los clientes y las partes interesadas contribuye al éxito sostenido de la organización.

LIDERAZGO

Los líderes de las organizaciones, sea cual sea su nivel, deben crear las condiciones necesarias para generar la implicación del personal y lograr los objetivos marcados en el Sistema de Gestión de la Calidad. El liderazgo permite a la organización alinear sus estrategias, políticas, procesos y recursos para lograr los objetivos marcados.

COMPROMISO DEL PERSONAL

Contar con un personal comprometido es esencial para mejorar la organización, para así crear y ofrecer valor en toda la organización. Para administrar una organización con eficacia y eficiencia, es importante involucrar a todo el personal, en todos los niveles organizativos. El reconocimiento y la mejora de la competencia del personal facilita la participación de las personas en la consecución de los objetivos de Calidad.

ENFOQUE BASADO EN PROCESOS

Se logran resultados consistentes y predecibles de manera más efectiva y eficiente cuando las actividades se entienden y se gestionan como procesos interrelacionados que funcionan bajo un sistema coherente.

El Sistema de Gestión de la Calidad funciona a partir de procesos interrelacionados. Comprender cómo se producen los resultados de este sistema, permite a una organización optimizar el sistema y su rendimiento.

MEJORA

Las organizaciones exitosas tienen un enfoque basado en la mejora continua. La mejora es esencial para que una organización mantenga los niveles actuales de rendimiento, reaccione a los cambios en sus condiciones internas y externas y, cree nuevas oportunidades.

TOMA DE DECISIONES BASADA EN LA EVIDENCIA

Es más probable que la toma de decisiones fundamentadas en el análisis y la evaluación produzcan los resultados deseados. La toma de decisiones puede ser un proceso complejo, y siempre implica cierta incertidumbre. A menudo implica el estudio de mucha información, así como su interpretación, que en algunos casos puede ser subjetiva. Es importante entender las relaciones de causa - efecto y las posibles consecuencias no deseadas. Los hechos, la evidencia y el análisis de datos conducen a una mayor objetividad y confianza en la toma de decisiones.

GESTIÓN DE LAS RELACIONES

Para un éxito sostenido, las organizaciones deben gestionar eficazmente sus relaciones con todas las partes interesadas. Las partes interesadas tienen una gran influencia en el desempeño de una organización. El éxito se logra cuando la organización gestiona las relaciones con todas sus partes interesadas para optimizar su impacto en su rendimiento.

Auditoría de sistemas

Razones para controlar

Costos por pérdidas de datos:

- Los datos proveen a la organización de una imagen de sí misma, de su entorno, de su historia, y su futuro. [Everest,1985].
- Si la imagen es exacta, la organización aumenta las posibilidades de adaptarse y sobrevivir a un entorno cambiante.
- Si la imagen es inexacta, se puede incurrir en pérdidas sustanciales.
- Ejemplo: pérdida de cuentas corrientes, pérdida de los datos de los alumnos.

Costos por decisiones incorrectas:

- La alta calidad en la toma de decisiones depende, en parte, de:
  - la calidad de los datos,
  - la calidad de las reglas de decisión.
- La importancia de datos exactos depende del tipo de decisiones hechas por personas que tienen algún interés en la organización.
- Alta Gerencia -> decisiones de planeamiento estratégico -> probablemente acepten algunos errores en los datos.
- Gerencia Media -> decisiones de control administrativo y de control operativo -> requieren datos más exactos.
- Las decisiones para que los datos sean correctos involucran: detección, investigación y corrección.
- El tener reglas de decisión exactas en un sistema de información (SI) depende del tipo de decisiones hechas por personas que tienen algún interés en la organización.
- Una regla de decisión incorrecta puede tener un impacto menor. Ejemplo: cálculo de amortización erróneo en un bien de poco valor.

Costos por abuso computacional:

- un abuso computacional es un incidente asociado con tecnología informática, en el cual una víctima sufre o podría haber sufrido pérdida, y un perpetrador con intención logra o podría lograr ganancia.

- El promedio de pérdidas por abusos computacionales pareciera ser sustancialmente mayor que las pérdidas producidas por fraudes convencionales.
- Tipos de abusos: hacking, virus, acceso físico ilegal, abuso de privilegios.

Costos por errores de computación:

- Los costos por un error de computación pueden ser altos, en términos de:
  - pérdida de vida humana,
  - privación de libertad,
  - daño al medio ambiente.
- ¿Por qué? Los sistemas controlan:
  - monitoreo de pacientes,
  - cirugías,
  - vuelo de misiles,
  - un reactor nuclear.

Valor de hardware, software y personal:

- Recursos críticos en las organizaciones:
  - Datos - ¿qué pasa si la competencia obtiene información confidencial?
  - Hardware - ¿qué pasa si un componente crítico deja de funcionar?
  - Software - ¿qué pasa si se destruye?
  - Personal - ¿qué pasa si un profesional calificado deja la empresa?

Mantenimiento de privacidad:

- Muchos datos se recolectan sobre los individuos: impuestos, obras sociales, trabajo, residencia.
- Con sistemas automatizados se puede integrar y buscar información.
- ¿Qué pasa con la privacidad?
  - Se podrían utilizar datos de genética humana para obtener información detallada sobre una persona y usarla en su contra.

Evolución controlada del uso:

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

Auditoría de sistemas de información

Definición:

La auditoría de sistemas de información es el proceso de **recolectar** y **evaluar evidencia** para determinar si:

1. el sistema automático **preserva los activos**,
2. mantiene la **integridad de los datos**,
3. permite que los objetivos organizacionales se alcancen con **eficacia**,
4. usa los recursos con **eficiencia**.

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 cual los datos poseen ciertos atributos:

- completitud
- consistencia
- veracidad
- correctitud

Si la integridad de los datos de una organización no es mantenida, no posee representación de sí misma o de los eventos.

Sin integridad de datos se pueden producir pérdidas de ventajas competitivas.

El valor de 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]
2. el grado en el cual el ítem de dato es compartido entre los tomadores de decisiones
3. 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.

Generalmente, la eficiencia se estudia cuando se agotan los recursos.

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

Sistema de control interno

Un sistema de control interno incluye:

1. separación de obligaciones,

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

Sistema de control interno - implementación

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

1) SEPARACIÓN DE OBLIGACIONES

En un sistema manual, personas diferentes deben realizar las tareas de:

1. iniciar la transacción
2. registrar la transacción
3. prevenir errores o detectar irregularidades

En un sistema automatizado, es el mismo programa el que realiza todas las funciones.

En los sistemas automatizados, la separación de obligaciones se aplica distinto: se tiene que separar la capacidad de ejecutar el programa, de la capacidad de modificar el programa.

2) DELEGACIÓN

Una delegación clara de autoridad y responsabilidad es esencial tanto en sistemas manuales como automatizados.

En un sistema automatizado, hacer esto de una manera no ambigua puede ser dificultoso.

Ejemplo: cuando múltiples usuarios tienen acceso a los mismos datos y la integridad es violada de alguna manera, no es fácil ubicar quién es el responsable, para identificar y corregir el error.

3) PERSONAL COMPETENTE Y CONFIABLE

A las personas responsables de desarrollar, implementar y operar los sistemas de información se les delega mucho poder.

El personal responsable de los sistemas automatizados tiene delegado mayor poder que los empleados que realizan tareas manuales

4) SISTEMA DE AUTORIZACIONES

La gerencia debe establecer dos tipos de autorizaciones:

1. autorizaciones generales: establecen las políticas que la organización debe seguir. Ejemplo: lista de precios.
2. autorizaciones específicas: aplicables a transacciones individuales. Ejemplo: compra de activos de alto valor.

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, por ejemplo:

1. un pedido telefónico,
2. un sistema de reposición automático de stock.

En un sistema bien diseñado debería haber mayores registros de auditoría que en un sistema manual.

Se deben prever controles de acceso y facilidades de acceso (login) para asegurar que los rastros de auditoría sean exactos y completos.

6) CONTROL DE ACCESO FÍSICO

El control de acceso físico a los activos y a los registros es crucial, tanto en sistemas manuales como automáticos.

Diferencia:

- sistema manual: puede tener que acceder a varios sitios
- sistema automatizado: todos los registros necesarios se pueden mantener en un sólo lugar.

La concentración de información aumenta la posibilidad de pérdida que puede surgir por abuso o desastre.

Supervisión general adecuada:

En sistemas manuales se facilita, ya que empleados y supervisores, generalmente, comparten el lugar físico.

En sistemas automatizados, las comunicaciones permiten que los empleados estén cerca de los clientes. La supervisión se debe llevar a cabo en forma remota.

Los controles para supervisión deben estar construidos dentro del sistema.

El gerente debe acceder a los registros de auditoría para evaluar la gestión de los empleados.

7) CHEQUEOS DE PERFORMANCE

En sistemas manuales, los chequeos realizados por otra persona ayudan a detectar errores o irregularidades.

En sistemas automatizados, los programas siempre ejecutan el mismo algoritmo, a excepción de una falla de hardware o de software.

Los auditores deben evaluar los controles establecidos para desarrollar, modificar, operar y mantener programas.

8) COMPARACIÓN PERIÓDICA

Periódicamente, se deben controlar los datos que representan los activos con los activos reales, a fin de determinar falta de completitud o inexactitud de los datos.

En sistemas automatizados se deben preparar programas para que hagan esto. Ejemplo: control de inventarios.

Nuevamente, son importantes la implementación de estos controles durante el desarrollo de sistemas.

La computación en auditoría

En sistemas automatizados es más complicado recolectar evidencia.

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

Los errores en los sistemas manuales tienden a ser estocásticos. Ejemplo: periódicamente el empleado se equivoca al actualizar un precio.

Los errores en los sistemas automáticos:

1. tienden a ser determinísticos
2. se generan a mayor velocidad
3. es más costoso arreglarlos

Los controles internos que aseguran la alta calidad en el diseño, implementación, operación y mantenimiento de los sistemas, son críticos.

Fundamentos de la auditoría

Auditoría tradicional:

Aporta conocimientos y experiencia sobre técnicas de control interno.

Aporta la filosofía de los controles. Ejemplo: los programas deben asegurar que todas las transacciones fueron procesadas correctamente.

Involucra examinar los SI con una mente crítica, siempre con una visión cuestionadora sobre la capacidad de los SI para:

1. salvaguardar activos,
2. mantener integridad de datos,

3. lograr objetivos eficiente y eficazmente.

Administración de Sistemas de Información:

Aporta:

1. técnicas de administración de proyectos.
2. documentación, estándares, presupuestos.

A raíz de los fracasos al comienzo, ahora aporta nuevos métodos para mejorar el desarrollo y la implementación de sistemas.

Ejemplo: metodologías de desarrollo de sistemas.

Ciencias del Comportamiento:

Una resistencia de comportamiento para con el sistema pone en peligro los objetivos de la auditoría.

Usuarios descontentos pueden intentar sabotaje o circunscribir controles.

Lo mismo sucede con diseñadores, y entre estos y los usuarios.

Los auditores deben comprender las situaciones que dan lugar a conflictos de comportamiento y como resultado posible, el fracaso del sistema.

Los Ingenieros de Software deben colaborar con los objetivos de la auditoría.

Ejemplo: investigar sobre cómo probar la correctitud de un programa formalmente.

El conocimiento técnico en profundidad desarrollado por esta disciplina causa problemas y beneficios a los auditores.

- beneficios: se pueden preocupar menos por la confiabilidad de algunas componentes.
- problemas: pueden tener dificultades para determinar abusos.

Controles

Definición: Un control es un sistema que previene, detecta, o corrige eventos ilegales.
Hay tres aspectos claves en esta definición:

1. un control es un sistema
2. eventos ilegales
3. los controles son usados para prevenir, detectar o corregir eventos ilegales.

Una password, ¿es un control ?
Habitualmente, tendemos a nombrar los controles, teniendo en cuenta sólo un aspecto del control.
Una password se convierte en control, sólo en el contexto de un sistema que asegure:

1. seguridad para elegir passwords,
2. correcta validación de passwords,
3. almacenamiento seguro de las passwords,seguimiento en el uso indebido de passwords
4. etc

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:

1. controles preventivos: reducen la probabilidad que estos eventos ocurran.
2. controles detectivos y correctivos: reducen la cantidad de pérdidas cuando los eventos ilegales ocurren.

La tarea del auditor es determinar si los controles están ubicados y funcionan para prevenir los eventos ilegales.

¿CÓMO ADMINISTRAR LA COMPLEJIDAD?

Para administrar la complejidad, se sugiere:

1. factorizar el sistema en subsistemas
2. determinar la confiabilidad de cada subsistema, y las implicancias de cada uno de ellos en el nivel de confiabilidad general del sistema.

Factorización

El primer paso para comprender un sistema complejo es particionarlo en subsistemas.

Un subsistema es un componente de un sistema que:

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

Los subsistemas son componentes lógicas y no físicas.

El proceso de particionar en subsistemas se denomina factorización.

¿Cómo?

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.

Otro criterio de factorización

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 factorizar

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”.

En base a las funciones gerenciales

Subsistema Gerencial	**Descripción**
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.

En base a las funciones de aplicación

Los sistemas de información que soportan una organización, se dividen en ciclos
Los ciclos varían de acuerdo al tipo de organización: industria, entidad financiera, etc.
En general incluyen:

1. ventas y cobranzas,
2. administración de personal, sueldos y jornales,
3. compras y pagos,
4. producción, inventario y almacenaje,
5. tesorería (contabilidad).

Cada ciclo es factorizado en uno o más sistemas de aplicación.
Ejemplo: Ventas puede subdividirse en:

1. administración de clientes
2. captura de pedidos
3. facturación

El conjunto de subsistemas de aplicación incluyen lo siguiente:

Subsistema de Aplicación	**Descripción**
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 subsistemas

Primero - determinar el menor nivel de los subsistemas

Segundo - evaluar la confiabilidad de los controles en cada subsistema.

Confiabilidad de controles

Para evaluar la confiabilidad de los controles:

1. se deben identificar todos los posibles tipos de eventos que pueden ocurrir en el subsistema.
2. se deben considerar todos los eventos válidos o ilegales.

Para identificar los eventos, hay que considerar las principales funciones que realiza el subsistema.

Considerar las principales funciones

Para cada función:

1. analizar cómo debería realizarse
2. evaluar cómo el subsistema cumple con esa visión normativa.

Para determinar si un evento es legal o ilegal se deben considerar las transacciones que pueden ocurrir como input al subsistema.

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

Eventos y transacciones

Cuando un evento ocurre, el sistema recibe una transacción de input

Cuando la transacción se recibe como input el sistema cambia de estado.

Otros cambios de estado ocurren a medida que el sistema procesa la transacción.

Para identificar todos los eventos que pueden ocurrir en un sistema como resultado de la transacción, se debe entender cómo el sistema procesa la transacción.

Procesamiento de transacciones

Generalmente los auditores aplican técnicas de walk-through:

1. se considera una transacción particular,
2. se identifican todos los componentes del sistema que procesan la transacción
3. se trata de entender cada paso de procesamiento que ejecuta cada componente
4. se considera cualquier error o irregularidad (evento ilegal) que pueda ocurrir en el camino.

Clases de transacciones

Generalmente es muy costoso realizar este proceso para todas las transacciones.

Por eso, se trabaja con clases de transacciones:

1. se agrupan transacciones que tengan un procesamiento similar,
2. se trata de entender esas transacciones, y los eventos que puedan surgir como resultado de esas transacciones como grupo,
3. se tratan sólo aquellas transacciones que se consideran importantes para los objetivos de la auditoría.

¿Qué eventos?

Usando esta técnica, no se identifican todos los eventos que puedan surgir en un sistema.

A pesar de esto, los auditores deberían examinar todas aquellas transacciones y eventos que consideren importantes.

Una vez que se han identificado los eventos que pueden ocurrir, los auditores deben evaluar:

1. si los controles están correctamente ubicados, y
2. si funcionan para detectar eventos ilegales.

Confiabilidad de los controles

Los auditores deben recolectar evidencias sobre la existencia y confiabilidad de los controles, para determinar si las pérdidas por los eventos ilegales se reducen a niveles aceptables.

Para cada evento ilegal, se debe considerar:

1. cómo los controles cubren a ese tipo de evento,
2. cuánto de confiable son los controles,
3. si puede ocurrir un error material o una irregularidad.

Se publican listas que ayudan a realizar esta tarea.
Estas listas muestran por ejemplo:

1. las caídas en los sistemas de información,
2. errores e irregularidades que ocurren en diferentes tipos de transacciones.

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

Estimar la confiabilidad

La evaluación de la confiabilidad procede de abajo hacia arriba en el nivel de estructura de los sistemas.

Los subsistemas de menor nivel son componentes de los de mayor nivel.

Cuando se haya evaluado la confiabilidad de los subsistemas de menor nivel, se puede analizar:

1. el impacto
2. la naturaleza, y
3. la frecuencia de los eventos ilegales

en los sistemas de mayor nivel.

Estimar la confiabilidad- Pasos

En cualquier nivel de la estructura, los pasos de evaluación son:

1. identificar las transacciones que ingresan al sistema
2. considerar los eventos legales e ilegales que puedan ocurrir
3. asegurar la confiabilidad de los controles que detectan los eventos ilegales

Detectar nuevos controles

A medida que se evalúan los sistemas de más alto nivel, se pueden encontrar nuevos controles debido a:

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

Riesgos

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

RDA = RI * RC * RD

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

Tipos de riesgo

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

1)Riesgo Deseado para una Auditoría

Primero los auditores eligen el nivel de **RDA.**

Evalúan las consecuencias de fracasar en detectar las pérdidas materiales reales o potenciales.

2)Riesgo Inherente de Sistemas

Luego, se considera el nivel de **RI**.

Los auditores consideran factores generales tales como:

1. a naturaleza de la organización (la posición en el mercado),
2. la industria en la que opera (¿la industria está sujeta a cambios rápidos?)
3. las características del gerenciamiento (¿es agresivo y autocrático?)
4. intereses contables y de auditoría (¿se usan técnicas?)

Se consideran luego los RI asociados con diferentes segmentos de la auditoría (ciclos, sistemas de aplicación, ...).

Para cada segmento, se consideran factores tales como:

1. sistemas financieros
2. sistemas estratégicos
3. sistemas de operación crítica
4. sistemas de tecnología avanzada

3)Riesgo 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.

4) Riesgo 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:

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

Procedimientos

Procedimientos de una auditoría:

Existen diferentes procedimientos de auditoría, dependiendo de lo que se 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
2. testeo de controles
3. testeos substantivos de detalle de transacciones
4. testeos substantivos de detalle de balances contables
5. procedimientos de revisión analítica

procedimientos para comprender los controles

Los procedimientos incluyen:

1. cuestionarios,
2. inspecciones,
3. observaciones

Para determinar:

1. si los controles existen,
2. analizar cómo están diseñados,
3. si funcionan.

testeo de controles

Son para evaluar si los controles están actuando efectivamente.

Ejemplos:

1. cuestionarios
2. inspecciones
3. observaciones
4. reprocesos

detalle de transacciones

Los testeos substantivos de detalle de transacciones están diseñados para detectar:

1. errores monetarios o
2. irregularidades

en transacciones que afectan los estados financieros.

detalle de balances contables

Los tests substantivos de detalle de balances contables se focalizan en los registros contables finales, en el balance.

Ejemplo: se puede circularizar a una muestra de clientes para controlar que los saldos registrados sean correctos.

procedimientos de revisión analítica

Los procedimientos de revisión analítica se focalizan en las relaciones entre los ítems de datos.

El objetivo es identificar áreas que requieran un trabajo de auditoría posterior.

Eficacia y Eficiencia

Para 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. Ejemplo: testeos de performance.
5. procedimientos de revisión analítica. Ejemplo: modelos de simulación.

Orden de los testeos

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

1. procedimientos de revisión analítica

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

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

Tareas

Planificación de una auditoría

La primera etapa es la planificación.

Las tareas que se realizan en la etapa de planificación varían dependiendo si es una:

1. auditoría interna.
2. auditoría externa.

Auditoría interna

La etapa de planificación incluye:

1. asignar personal adecuado a las auditorías
2. obtener información del cliente
3. realizar procedimientos de revisión analíticos para comprender el negocio del cliente
4. identificar áreas de riesgo

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

Auditoría externa

La etapa de planificación incluye:

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

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

Tareas de planificación

1. determinar el alcance de la auditoría,
2. emitir una opinión sobre el RDA,
3. emitir una opinión sobre el RI,
4. emitir una opinión sobre el RC,
5. calcular el RD que se debe lograr para cumplir con el RDA,
6. recolectar evidencia
7. documentar evidencia

Alcance de la auditoría

Determinar qué se va a auditar:

- Un sistema
- Un conjunto de sistemas
- Un área de tecnología informática

Opinión de RDA

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

Opinión sobre RI

El RI depende del segmento a auditar.

Algunos segmentos son más susceptible a errores, irregularidades, ineficiencias, o ineficacias.

Para cada segmento evaluar los factores que conducen a RI, por ejemplo:

- sistema con manejo de efectivo: posibilidades de defraudaciones.
- sistema complejo tecnológicamente: posibilidades de mal uso de recursos.

Opinión sobre RC

La decisión más difícil está en emitir el juicio en el nivel de RC asociado con cada segmento de la auditoría.

Para esto, los auditores deben comprender los controles internos usados dentro de la organización.

Los controles internos (CI) comprenden 5 componentes relacionados:

1. controles de entorno
2. evaluación de riesgo
3. actividades de control
4. información y comunicación
5. monitoreo

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.

evaluación de riesgo: Incluye evaluar los elementos que identifican y analizan los riesgos a los cuales se enfrenta la organización y cómo son administrados.

actividades de control: Incluye evaluar los elementos que operan para asegurar que:

1. las transacciones son autorizadas,
2. las responsabilidades se separan,
3. los documentos y registros se mantienen adecuadamente, etc.

Se clasifican en:

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

información y comunicación: Incluye evaluar los elementos en los cuales se: identifica, captura e intercambia información en tiempo y forma.

Permite asignar responsabilidades del personal adecuadamente.

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

Comprender los controles

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

Los controles gerenciales varían sustancialmente de organización a organización.

ejemplo de controles:

Controles Internos	**Implementación**
Actividades de Control	Procedimiento para instalar programas en producción (control gerencial)
Controles de Entorno y Evaluación de Riesgos	Existencia de comité de seguimiento de proyectos (control gerencial)
Información y Comunicación	Procedimiento para comunicar información (control gerencial) Procedimiento para capturar, registrar y procesar transacciones (control de aplicación)
Monitoreo	Procedimiento para medir la productividad del personal (control gerencial)

Recolectar evidencias

Existen distintas técnicas para recolectar evidencia:

1. revisión de papeles de trabajo de auditorías previas
2. entrevistas con alta gerencia y personal superior
3. observación de cómo se desarrollan las actividades
4. revisión de documentación de sistemas

Documentar evidencias

La evidencia se documenta:

1. completando cuestionarios.
2. construyendo diagramas de flujo de alto nivel.
3. construyendo tablas de decisión.
4. redactando descripciones narrativas.
5. utilizando herramientas CASE .

No invertir demasiado tiempo en esta etapa. El necesario para comprender los controles internos y decidir cómo proseguir con la auditoría.

Evaluación de Riesgo de Control

Si se evalúa que el RC < el nivel máximo =>

1. identificar los controles materiales que se relacionan con la evaluación
2. testear los controles para determinar si operan efectivamente.

Premisa: los testeos de controles probarán, que si los controles funcionan correctamente, se puede reducir la necesidad de un testeo sustantivo.

Si se evalúa que el RC es de nivel máximo => no se testean los controles.

Se podría concluir que los controles internos no son efectivos.

Se debería realizar un testeo amplio.

Testeo de Controles

El testeo de controles evalúa 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.

Controles Gerenciales - Testeo

Si los controles gerenciales, demuestran contrariamente a lo supuesto, que no operan eficientemente => no tiene sentido testear los controles de aplicación.

Controles de Aplicación - Testeo

Si los controles gerenciales funcionan efectivamente, se procede a evaluar los controles de la aplicación.

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

Testeo de Controles - Conclusión

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

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

Si los controles son más débiles, se pueden ampliar los testeos.

Actitud del auditor

Durante esta etapa los auditores externos e internos pueden tener distintas actitudes.

Situación: se detecta que los controles son débiles

1. auditor interno: puede expandir sus investigaciones para lograr una mejor comprensión a cerca de la naturaleza e implicancias de estas debilidades.
2. auditor externo: puede cortar sus investigaciones (sobre causas) y realizar testeos más amplios.

Testeo de transacciones

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

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

Testeo de resultados generales

Se realizan con el fin de obtener evidencia suficiente para realizar un juicio final sobre el grado de pérdidas que podrían ocurrir cuando el sistema falla en: salvaguardar activos, mantener la integridad de los datos y lograr efectividad y eficiencia.

En general, este tipo de testeos, son los más caros de las auditorías.

Testeo de resultados

Si los auditores confían en que los controles son confiables, pueden limitar el número y alcance de estos testeos.

Si es a la inversa, aumentarán el grado de control para estimar mejor las pérdidas.

Evaluar efectividad y eficiencia

Evaluar efectividad y eficiencia es más complejo.

Se puede trabajar con los usuarios estimando las pérdidas por no haber tomado una decisión por no contar con la información en tiempo y forma.

Completar la auditoría

En la etapa final, se realizan testeos adicionales para cerrar la evidencia.

Finalmente, se formula la opinión sobre cómo ocurrieron las pérdidas materiales o registros incorrectos en un informe.

Opiniones de auditoría

Los estándares en varios países requieren que la opinión sea:

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

Gobernanza de TI

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

- trata con la relación entre el enfoque empresarial y la gestión de TI
- destaca la importancia de las cuestiones de TI
- promueve que las decisiones estratégicas de TI deben ser tomadas por una junta directiva corporativa

Definiciones:

Son estructuras y procesos de liderazgo y organizativos que aseguran que las TI de la organización sostienen y extienden las estrategias y los objetivos de la organización.

Se trata de especificar los derechos de decisión y el marco de rendición de cuentas para fomentar el comportamiento deseable en el uso de TI.

Es el sistema por el cual se dirige y controla el uso actual y futuro de las TIC. Implica evaluar y dirigir los planes para el uso de las TIC para apoyar a la organización y monitorear este uso para alcanzar los planes. Incluye la estrategia y las políticas para el uso de las TIC dentro de una organización

Administración de TI: se trata de tomar e implementar decisiones de TI
Gobernanza de TI: se trata de quién toma las decisiones de TI

- quién tiene autoridad para tomar las decisiones importantes

- quién tiene información para tomar las decisiones importantes
- quién es responsable por implementar las decisiones importantes

Áreas de enfoque

1. Entrega de valor
2. Manejo de riesgos
3. Alineamiento estratégico
4. Manejo de recursos
5. Mediciones de desempeño

Preguntas clave

Pregunta estratégica: ¿Estamos haciendo las cosas correctas?
Pregunta de arquitectura: ¿Las estamos haciendo de forma correcta?
Pregunta de entrega: ¿Las estamos haciendo bien?
Pregunta de valor: ¿Estamos obteniendo beneficios?

Ejemplos de pregunta estratégica:

La inversión en TI…

- está alineada con la visión?
- es consistente con los principios de negocio?
- está contribuyendo a los objetivos estratégicos?
- está proporcionando un valor óptimo, a un costo accesible y un nivel de riesgo aceptable?

Ejemplos de pregunta de arquitectura:

La inversión en TI…

- está alineada con la arquitectura de la agencia?
- es consistente con los principios arquitectónicos de la agencia?
- está contribuyendo a la población de nuestra arquitectura?
- está en línea con otras iniciativas?

Ejemplos de pregunta de entrega:

Tenemos…

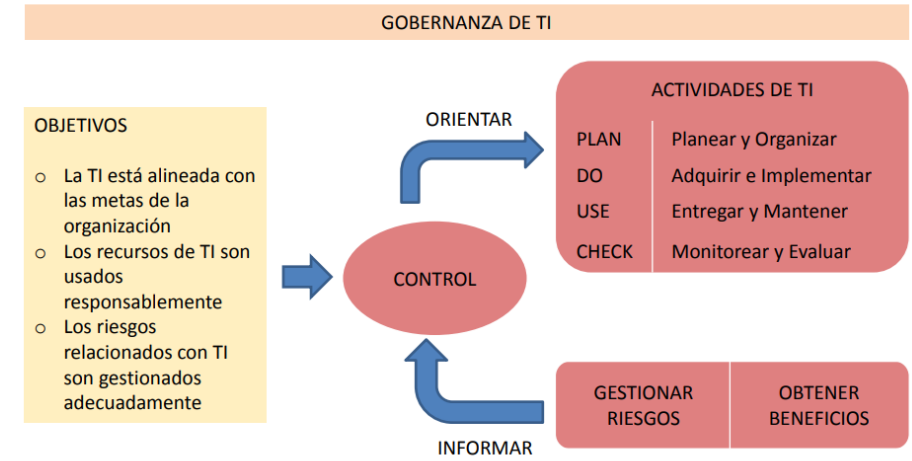
- procesos efectivos y disciplinados de administración, entrega y gestión de cambios?
- recursos técnicos y gubernamentales competentes y disponibles para entregar:
    - las prestaciones requeridas?
    - Los cambios organizacionales necesarios para aprovechar las prestaciones?

Ejemplos de pregunta de valor:

Tenemos…

- una comprensión clara y compartida de los beneficios esperados?
- una clara responsabilidad para la obtención de los beneficios?
- métricas relevantes para la medición de los beneficios?
- un proceso efectivo de realización de beneficios?

CICLO DE VIDA



Enfoques

1. OBJETIVOS DE CONTROL PARA INFOrMACIÓN Y TECNOLOGÍA RELACIONADA (COBIT) Enfoque para estandarizar buenas practices de TI y control. Provee herramientas para acceder y medir el desempeño de los procesos de gobernanza y administración de TI de una organización. Desarrollado y mantenido por el Instituto de Gobernanza de TI.
2. BIBLIOTECA DE INFRAESTRUCTURA DE TI (ITIL) Marco detallado con información sobre cómo lograr una gobernanza de TI exitosa. Desarrollado y mantenido por la Oficina de Comercio Gubernamental del Reino Unido.
3. ISO 27001 Conjunto de buenas prácticas a seguir para las organizaciones cuando se implementa y mantiene un programa de seguridad.
4. MODELO DE MADUREZ DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (ISM3) Proceso basado en el modelo de madurez de gestión de la seguridad de la información -
5. AS8015-2005 Estándar Australiano para el Gobierno Corporativo de las Tecnologías de Información y Comunicación.

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.

Fue creado por la Asociación de Auditoría y Control de Sistemas de Información (ISACA, www.isaca.org) y el Instituto de Gobernanza de TI en 1992.

COBIT 5 consolida COBIT 4.1, Val IT y Risk IT en un marco y se ha actualizado para alinearse con las mejores prácticas actuales, por ejemplo ITIL V3 2011, TOGAF (El Marco de Arquitectura de Grupo Abierto).

Principios de COBIT

1. Satisfacer las necesidades de las partes interesadas:
    - Garantizar que las empresas aporten valor a sus partes interesadas mediante la obtención de beneficios, la optimización del uso de los recursos y la gestión de riesgos.
2. Cubrir la empresa de extremo a extremo:
    - Tener en cuenta todos los sistemas de gobernanza y administración relacionados con TI para que sean integrales y de extremo a extremo – incluyendo tanto sistemas internos como externos.

3. Aplicar un marco integrado:
    - Alinearse con otros estándares y buenas prácticas relacionadas con TI, sirviendo de marco general para la gobernanza y administración de TI empresarial.
4. Habilitar un enfoque holístico:
    - Tener en cuenta los elementos que interactúan, especificar un conjunto de habilitadores para definir un sistema integral de gobernanza y administración de TI empresarial.
5. Separar las funciones principales:
    - Establecer una distinción clara entre las funciones de gobernanza y administración.

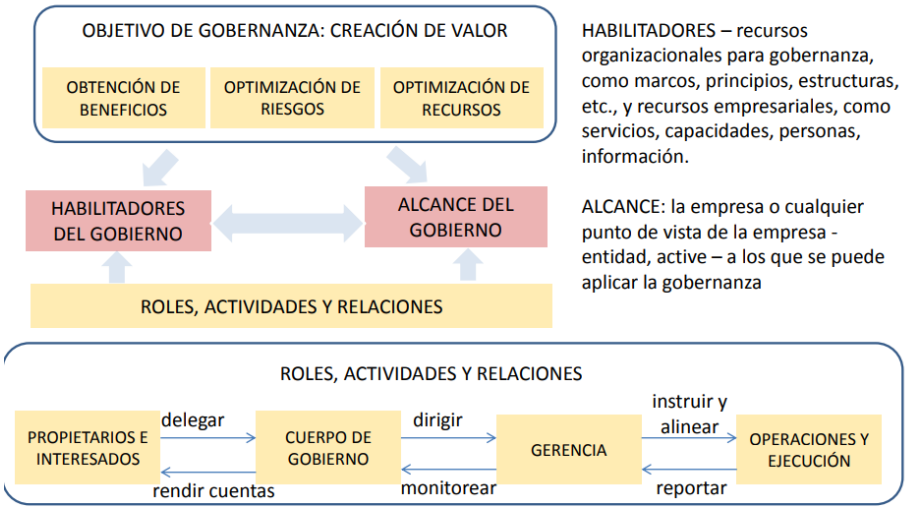
Satisfacer las necesidades de las partes interesadas

Todas las empresas deben aportar valor a sus partes interesadas. Por lo tanto, la creación de valor es un objetivo de gobernanza de toda organización.

El valor puede ser creado mediante la obtención de beneficios a un costo óptimo de recursos mientras se optimizan los riesgos.

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

Cubrir la empresa de extremo a extremo



<Literal no encontré forma de descomponer este cuadro a palabras>

Aplicar un marco integrado

COBIT 5:

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

Habilitar un enfoque holístico

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

COBIT define siete categorías de habilitadores:

Separar las funciones principales

Gobernanza asegura:

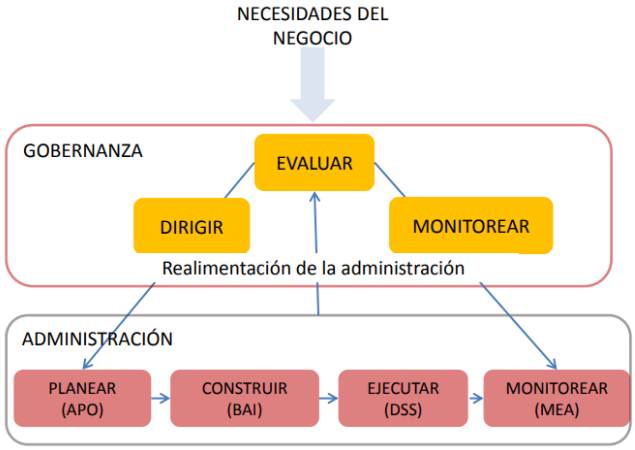
- que las necesidades, condiciones y opciones de las partes interesadas son evaluadas para determinar objetivos empresariales a alcanzar equilibrados y acordados
- establecer la dirección a través de la priorización y la toma de decisiones
- supervisando el desempeño y cumplimiento contra la dirección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

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

Modelo de referencia del Proceso

COBIT 5.0 divide los procesos en 2 dominios:

1. GOBERNANZA – incluye 5 procesos, dentro de cada uno de ellos se definen prácticas de Evaluar, Dirigir y Monitorear
2. ADMINISTRACIÓN – incluye 32 procesos clasificados en 4 dominios – APO, BAI, DSS y MEA.



características principales:

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

audiencia:

- Gerentes: les ayuda a equilibrar el riesgo y control de la inversión en un ambiente de TI a menudo impredecible
- Usuarios: les garantiza seguridad y control de los servicios de TI internos o proporcionados por terceros

- Auditores: les ayuda a definir el nivel de seguridad sobre el objeto particular a auditar. Los asesora sobre la gestión de los controles internos

Procesos de administración de COBIT

COBIT clasifica la Administración de TI en 4 dominios:

- **Alinear, Planear y Organizar (APO)**: proporciona direcciones a la entrega de soluciones y servicios. Se interesa en
  - la comprensión de la visión a planificar, comunicar y gestionar.
  - una organización e infraestructura adecuadas para su puesta en marcha.
- **Construir, Adquirir e Implementar (BAI)**: provee soluciones a DSS para la entrega de servicios. Se enfoca en:
  - los cambios en las soluciones de TI existentes.
  - el mantenimiento de sistemas existentes.
  - asegurar que las soluciones continúan cumpliendo con las metas empresariales.
- **Entrega, Servicio y Soporte (DSS)**: recibe soluciones y las hace utilizables para los usuarios finales. Se enfoca en:
  - la gestión de seguridad y continuidad del servicio.
  - el soporte de servicios para usuarios.
  - la administración de datos.
- **Monitorear y Evaluar (MEA)**: monitorea todos los procesos para asegurar que se siga la dirección provista. Se enfoca en:
  - la gestión de desempeño.
  - el cumplimiento normativo.
  - el control interno.

Acá la teoría habla de objetivos y prácticas de control en detaller pero la verdad me da una paja tremenda esto así que salto a la próxima teoría.

WBS - WORK BREAKDOWN STRUCTURE

Es una descripción jerárquica del trabajo que se debe realizar para completar el proyecto.
Es similar a una descomposición funcional. El trabajo se divide en actividades. Las actividades se dividen en tareas.
El WBS es una herramienta para:

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.

Su confección es responsabilidad del LP (líder del proyecto). Debe definirse de tal manera que el LP pueda administrar el proyecto. Las formas de construirlo son:

1. Top-Down
   a. equipo completo
   b. sub-equipos
2. Botton-up

TOP DOWN EQUIPO COMPLETO

Todos los miembros del equipo participan de la descomposición. 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. Debido a que las actividades se definen con el suficiente nivel de detalle, las estimaciones de costo, tiempo y recursos son más exactas. Una vez que las actividades se han definido, se deben secuenciar. Se debe analizar qué actividades se pueden hacer concurrentemente.

TOP DOWN SUB-EQUIPOS

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

BOTTOM UP

Se asemeja a una lluvia de ideas. El equipo completo acuerda la partición del primer nivel. Se crean tantos sub-equipos como actividades haya en el nivel uno. Cada sub-equipo particiona una actividad (se le asigna la actividad para la cual tenga más experiencia). Cada grupo hace una lista de actividades en las cuales se descompone la actividad de nivel 1 asignada. Los integrantes presentan ideas sobre las tareas que involucra cada una de esas sub-actividades. El grupo clasifica las actividades que parecieran relacionarse. Se reúnen todos los grupos y cada grupo presenta sus resultados. Se discute en conjunto. La desventaja de este enfoque es no definir las tareas con el suficiente grado de granularidad.

WBS - ¿Cómo determinar completitud?

Cada actividad debe poseer 6 características para considerarse completa:

1. **Estado medible**: en cualquier momento se debería poder determinar el estado en que se encuentra.
2. **Acotada**: debe poseer evento y fecha de comienzo como así también evento y fecha de fin.
3. **Producir un entregable**: el entregable es un signo visible de que la actividad se completó. Puede ser un producto, un documento, etc.
4. **Tiempo y costo estimable**: una actividad debe tener un tiempo y un costo medibles.
5. **Duración aceptable**: en lo posible no trabajar con tareas de más de 10 días - 2 semanas laborables.
6. **Independiente**: una vez que se comenzó una actividad se debe poder continuar razonablemente sin interrupciones y sin la necesidad de un input adicional.

WBS - Enfoques para definición de actividades

Se pueden estipular criterios para nombrar las tareas:

1. **Enfoque por sustantivos**: en función de los entregables.
2. **Enfoque por verbos**: en función de las acciones requeridas para producir el entregable.
3. **Enfoque organizacional**: en función de las unidades organizativas que trabajarán en el proyecto.

Duración

Duración es el tiempo transcurrido en días laborables para finalizar el proyecto - sin considerar feriados, fines de semana, días no laborables.

Esfuerzo de Trabajo es la labor requerida para completar una actividad. La labor se puede realizar en horas consecutivas o no.

La duración de una actividad es influenciada por la cantidad de recursos planificados para trabajar en ella. Se dice *influenciada*, ya que no es una relación lineal directa entre la cantidad de recursos asignados a la tarea y la duración de la misma.

Crash de la Actividad: agregar más recursos para mantener la duración de una actividad dentro de los límites planificados.

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

Existen distintas causas por las variaciones a la duración de una actividad:

1. **variación en los perfiles**: la estrategia es estimar la duración de la actividad basados en personas con un determinado perfil para la actividad.
2. **eventos inesperados**: demoras de proveedores, fallas de energía, etc.
3. **eficiencia del tiempo de trabajo**: cada vez que un trabajador es interrumpido, le demanda más tiempo volver al nivel de productividad previo al momento de la interrupción.
4. **errores e interpretaciones erróneas**: esto puede implicar rehacer trabajo ya hecho.

Estimación de proyectos

Existen distintas técnicas para estimar esfuerzo:

1. ***Similitud con otras actividades:*** *estimar en base a las estimaciones de actividades similares de otros proyectos. Los datos están en la memoria de las personas.*
2. ***Datos históricos:*** *similar al punto 1 pero los datos están en algún tipo de registro o base de datos.*
3. ***Juicio experto:*** *las estimaciones las realizan consultores externos o vendedores con experiencia en la metodología o en la 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. Aquellos participantes cuyas estimaciones cayeron en los cuartiles exteriores, se les pide que justifiquen su estimación. Luego de escuchar los argumentos, se les pide a los miembros que vuelvan a estimar. Se vuelve a repetir este proceso de estimar y defender sus argumentos 3 veces. El promedio de la tercera pasada se usa como estimación del grupo.*
5. ***Técnica de 3 Puntos:*** *se necesitan 3 estimaciones de la duración de la actividad:*
    a. *Estimación optimista: es la duración más corta suponiendo que todo suceda de acuerdo a la planificado.*
    b. *Estimación pesimista: : la duración de la actividad suponiendo que falle todo lo que se prevé que puede fallar.*
    c. *Estimación media: la duración normal (usual) de la actividad.*

    Luego se calcula: ***Estimación = (Optimista + 4*Media + Pesimista)/6***
6. ***Técnica 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: la optimista, la pesimista y la media. Se recopilan los resultados de la Delphi y luego la fórmula de la de 3 puntos.*