INTRODUCCIÓN A LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN

Indice

- Sistema de información
- Gobierno de las TI
- El rol de la auditoría de los SI
- Auditoría de los SI
- Tipos de auditoría
- Realización de una auditoría de SI
  - COBIT

Sistema de información

- Facilita el funcionamiento coordinado de una organización, ayudando en el proceso de toma de decisiones y en los procesos de control

  - **No debe ser independiente de la organización**
    - Los SI tienen una **importancia estratégica**
    - Los SI debe estar **alineados con los objetivos del negocio**
    - Los SI deben usarse de manera **responsable**

  - Es necesario un **gobierno de las tecnologías de la información**

Gobierno de las TI

- Administración y control efectivo de las TI para asegurar que el SI…
  - **…proporciona valor**
    - Coste , tiempo y funcionalidad esperados
  - **…evita incertidumbre**
    - Se mitigan los riesgos en el uso de TI
  - **…contribuye al negocio**
    - Nuevas oportunidades e innovaciones en productos, procesos y servicios

El rol de la auditoría de los SI

- Son necesarios mecanismos para **apoyar el gobierno de las TI** como la auditoría
  - Informes sobre la confianza que una organización puede depositar en su SI, identificando los riesgos
  - Asegurar no sólo un uso correcto de las TI sino un uso acorde al plan de negocios de la organización en función del alcance de sus objetivos

Auditoría de los SI

Inicialmente

- Surge como apoyo a la auditoría financiera
  - Proceso **sistemático** de **obtención y evaluación** objetiva acerca de **aseveraciones** efectuadas por terceros referentes a hechos y eventos de naturaleza **económica**, para testimoniar el grado de correspondencia entre tales afirmaciones y un conjunto de **criterios convencionales**, comunicando los resultados obtenidos a los destinatarios y usuarios interesados
  - Auditoría **"con"** el ordenador
    - El auditor financiero utiliza el ordenador como herramienta

Auditoría de los SI

Posteriormente

- Surgen nuevas funciones
  - Aumento de la complejidad de los SI y de dependencia de las organizaciones respecto a los SI
  - Nuevas normativas aplicables directamente a los SI
    - Por ejemplo, leyes de protección de datos
  - Sistemas de comercio electrónico entre organizaciones (B2B) u orientadas a clientes finales (B2C)
    - Impulsan la mejora de los procesos de comercialización de productos pero han abierto la puerta a nuevos riesgos derivados de "abrir" los SI de las organizaciones a terceros

- Se propone una auditoría **"del"** ordenador
  - Verificar el funcionamiento correcto, eficaz y eficiente de las tecnologías de la información y los sistemas de información
  - Análisis de los riesgos a los que puede someterse la empresa con el uso de las TI

Auditoría de los SI

Definición

Proceso de **recoger, agrupar y evaluar evidencias** para determinar si un sistema informatizado…

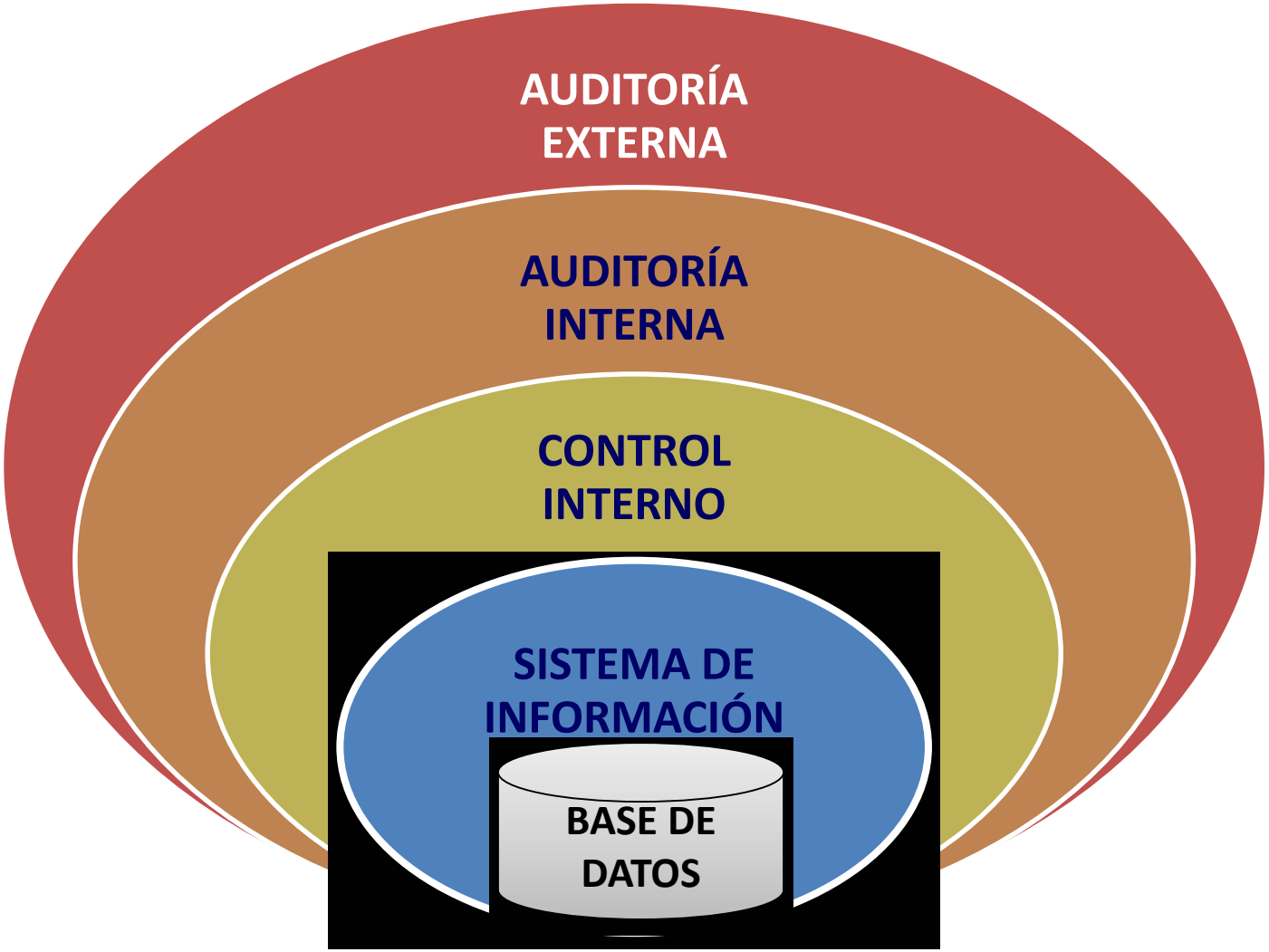
- …salvaguarda los activos
  - Protección de bienes
- …mantiene la **integridad** de los datos
  - Los datos deben ser correctos y completos
- …lleva a cabo **eficazmente** los fines de la organización
  - Ayuda a cumplir con los objetivos
- …utiliza **eficientemente** los recursos
  - Optimización en el uso de recursos

Auditoría de los SI

Funciones a realizar por un auditor informático

- Participar en las revisiones durante y después del diseño, realización, implantación y explotación de sistemas de información, así como en las fase de mantenimiento
- Revisar y juzgar los controles implantados en los sistemas informáticos para verificar su adecuación a las órdenes e instrucciones de la dirección, requisitos legales, protección de confidencialidad y cobertura de errores y fraudes
- Revisar y juzgar el nivel de eficacia, utilidad, fiabilidad y seguridad de los sistemas de información

Tipos de auditoría



Auditoría de SI externa

Se realiza por encargo a una organización externa

- Motivación concreta
  - Síntomas falta de eficiencia o eficacia de los SI
  - Requerimientos legales

Ventajas

- Total independencia de opinión
- Aporte de conocimientos técnicos externos a la empresa

Desventajas

- Poco conocimiento de la organización auditada
- Puede no existir seguimiento de las recomendaciones
- Costes elevados

Auditoría de SI interna

Se realiza internamente en la organización incluyendo todas las áreas relacionadas con TI

- Actúa de forma continua y periódica
- Planificación a corto y largo plazo

Ventajas

- Conocimiento en profundidad de la empresa
- Seguimiento de la implantación de las recomendaciones
- Evita que la empresa sufra costes elevados

Desventaja

- Poca independencia respecto a la auditoría externa

Auditoría informática NO es

Utilización de medios informáticos en la realización de una auditoría financiera

- Auditoría "con" el ordenador

Consultoría en áreas de sistemas de información

- Diferente tipo de tarea, ya que la consultoría tiene como misión asesorar sobre el desarrollo de ciertas actividades

Peritaje

- Mismo tipo de tarea pero distinta finalidad, ya que los peritos trabajan por encargo de un juez

Control interno

- Realizado a diferente nivel, sin independencia

Auditoría informática implica…

- …evaluación y emisión de una **opinión objetiva e independiente** sobre la fiabilidad de un SI

Control interno informático

Depende del departamento de informática

Supervisión diaria de que las actividades cumplen con…

- …las políticas
- …los procedimientos
- …estándares y normas
- …requerimientos legales

Aseguramiento de que los sucesos no deseados serán detectados, prevenidos y corregidos

- Mecanismos para **evitar riesgos**
  - **Probabilidad de que se produzca un error, falle un proceso o tenga lugar un hecho negativo para la empresa**

Control interno informático

Supervisión de las diferentes actividades operativas sobre los sistemas informáticos (centrales, departamentales, etc.) y sus entornos (desarrollo, pruebas o producción)

- Vigilancia sobre el control de cambios y la versiones del software
- Supervisión de la producción diaria
- Controles sobre la calidad y eficiencia del desarrollo y mantenimiento del software y del mantenimiento informático
- Controles en las redes de comunicaciones
- Controles en los sistemas microinformáticos
- Seguridad informática
  - Usuarios y perfiles de uso de archivos y bases de datos
  - Normas de seguridad
  - Control de información clasificada
- Licencias y relaciones contractuales con terceros
- Asesorar y transmitir cultura sobre el riesgo informático
- Etc.

Tipos de control interno informático

- Controles **preventivos**
  - Mecanismos para tratar de evitar un riesgo
  - Por ejemplo, un software de seguridad que impida los accesos no autorizados al sistema
- Controles **detectivos**
  - Mecanismos para tratar de conocer cuanto antes un hecho negativo que se ha producido
  - Se ponen en marcha cuando fallan los controles preventivos
  - Por ejemplo, un registro de accesos al sistema para detectar accesos no autorizados
- Controles **correctivos**
  - Mecanismos para facilitar la vuelta a la normalidad cuando se han producido incidencias
  - Por ejemplo, la recuperación de un fichero dañado a partir de las copias de seguridad

Realización de una auditoría de SI

- **Objetivos de la auditoría**
  - Verificar que **existen controles internos** para minimizar riesgos de negocio
  - Comprobar que los **controles internos funcionan** tal y como se espera

- Determinar los objetivos de auditoría incluye **determinar los objetivos de control**
  - COBIT (Control OBjectives for Information and related Technologies)

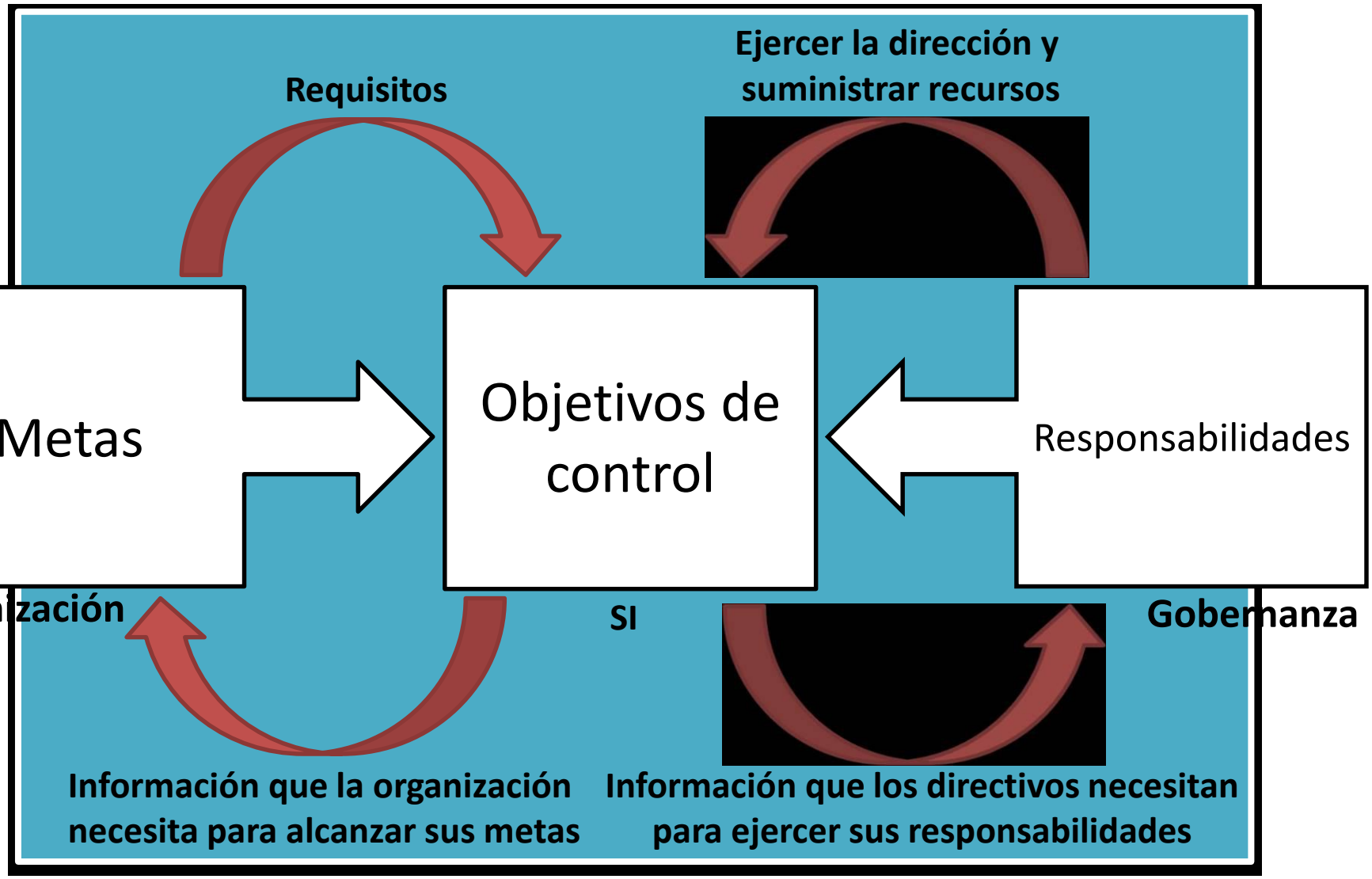
CobiT

Control **OB**jectives for **I**nformation and related **T**echnologies

- Definido por el ITGS (Information Technology Governance Institute) – www.itgi.org
- Marco de referencia para facilitar el gobierno de las TI a través de un conjunto estructurado de buenas prácticas y metodologías
  - ¿Está la TI alineada con el negocio contribuyendo a la maximización del beneficio?
  - ¿Son utilizados los recursos de TI (humanos y técnicos) de manera responsable?
  - ¿Son gestionados los riesgos de TI adecuadamente?
- Enfatiza el cumplimiento de normas y legislación

CobiT

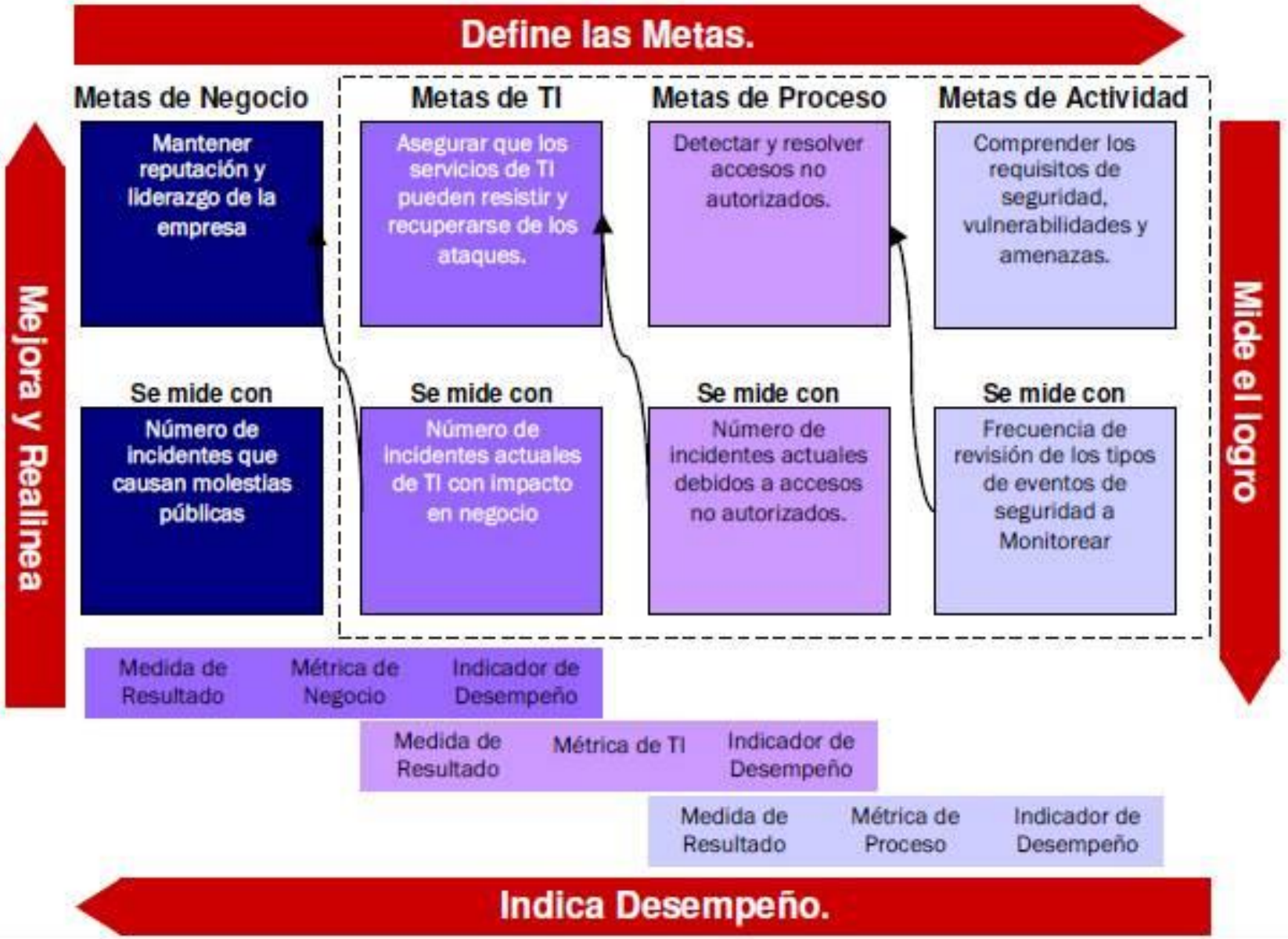
Control **OB**jectives for **I**nformation and related **T**echnologies



COBIT

Control **OB**jectives for **I**nformation and related **T**echnologies

- Definición de una serie de metas
  - Metas de la actividad
  - Metas del proceso
  - Metas de TI
  - Metas del negocio
- Metas medibles por medio de métricas
  - Con el fin de conocer si existen ciertos controles y su grado de cumplimiento
- Ejemplo: relaciones entre metas y métricas en un objetivo de control de COBIT
  - DS5: asegurar la seguridad del sistema


Define las Metas.
Metas de Negocio
Metas de TI
Metas de Proceso
Metas de Actividad
Mantener reputación y liderazgo de la empresa
Asegurar que los servicios de TI pueden resistir y recuperarse de los ataques.
Detectar y resolver accesos no autorizados.
Comprender los requisitos de seguridad, vulnerabilidades y amenazas.
Se mide con
Número de incidentes que causan molestias públicas
Se mide con
Número de incidentes actuales de TI con impacto en negocio
Se mide con
Número de incidentes actuales debidos a accesos no autorizados.
Se mide con
Frecuencia de revisión de los tipos de eventos de seguridad a Monitorear
Mejora y Realinea
Mide el logro
Medida de Resultado
Métrica de Negocio
Indicador de Desempeño
Medida de Resultado
Métrica de TI
Indicador de Desempeño
Medida de Resultado
Métrica de Proceso
Indicador de Desempeño
Indica Desempeño.

Auditoría de bases de datos

- Metodología
  - Determinar los objetivos de control que minimicen los riesgos potenciales a los que está sometido el entorno de bases de datos

Auditoría de bases de datos

- Ejemplo
  - Objetivo de control
    - SGBD preservará la confidencialidad de la base de datos
  - Técnica de control
    - Preventivas
      - Establecer los tipos de usuarios, perfiles y privilegios necesarios para controlar el acceso a la base de datos
    - Detectivas
      - Monitorizar los accesos a la base de datos
    - Correctivas
      - Realizar una copia de respaldo

Auditoría de bases de datos

- Si los controles existen, se definen pruebas de cumplimiento para verificar su consistencia
  - Prueba de cumplimiento
    - Listar los privilegios y perfiles existentes en el SGBD
- Si las pruebas detectan inconsistencias en los controles o si los controles no existen se pasa a diseñar pruebas para dimensionar el impacto de estas deficiencias
  - Prueba sustantiva
    - Comprobar si la información ha sido corrompida comparándola con otra fuente o revisando los documentos de entrada de datos y las transacciones ejecutadas

Auditoría de bases de datos

- Una vez valorados los resultados se obtienen unas conclusiones que se comentan y discuten con los responsables del área

- Auditor debe emitir
  - Descripción de la situación
  - Riesgo existente
  - Deficiencia a solucionar
  - Posible solución

COBIT y la auditoría de bases de datos

- Objetivos de control relacionados con las bases de datos
  - PO2 Definir la arquitectura de información
    - PO2.1 Modelo corporativo de arquitectura de información
    - PO2.2 Diccionario de datos corporativo y reglas de sintaxis de datos
    - PO2.3 Esquema de clasificación de datos
    - PO2.4 Gestión de integridad

COBIT y la auditoría de bases de datos

- Objetivos de control relacionados con las bases de datos
  - DS11 gestionar datos
    - DS11.1 Requisitos de negocio para la gestión de datos
    - DS11.2 Planes de almacenamiento y retención de datos
    - DS11.3 Sistema de gestión de bibliotecas de medios
    - DS11.4 Eliminación de datos
    - DS11.5 Copia de respaldo y restauración
    - DS11.6 Requisitos de seguridad para la gestión de datos

DS11: gestionar datos

- Objetivos y métricas
  - Objetivos de las tecnologías de la información
    - Optimizar la utilización de la información
    - Asegurar que la información crítica y confidencial es inaccesible para los no autorizados
    - Asegurar la conformidad de las tecnologías de la información con las leyes, regulaciones y contratos
    - Métricas
      - Número de ocurrencias de incapacidad para recuperar datos críticos para los procesos de negocio
      - Porcentaje de satisfacción del usuario con la disponibilidad de los datos
      - Número de incidentes de no conformidad con la legislación

DS11: gestionar datos

- Objetivos y métricas
  - Objetivos de los procesos
    - Mantener la integridad y accesibilidad de los datos
    - Gestionar el almacenamiento
    - Métricas
      - Porcentaje de restauraciones de datos exitosas
      - Número de caídas de sistemas o incidentes de integridad de datos causados
  - Objetivos de las actividades
    - Realizar copias de respaldo y pruebas de restauración
    - Asegurar la disposición de datos y equipos
    - Métricas
      - Frecuencia de pruebas de copias de respaldo
      - Tiempo medio de restauración de datos

DS11: gestionar datos

- Objetivos y métricas
  - Objetivos de las tecnologías de la información
    - Optimizar la utilización de la información
    - Asegurar que la información crítica y confidencial es inaccesible para los no autorizados
    - Asegurar la conformidad de las tecnologías de la información con las leyes, regulaciones y contratos
    - Métricas
      - Número de ocurrencias de incapacidad para recuperar datos críticos para los procesos de negocio
      - Porcentaje de satisfacción del usuario con la disponibilidad de los datos
      - Número de incidentes de no conformidad con la legislación

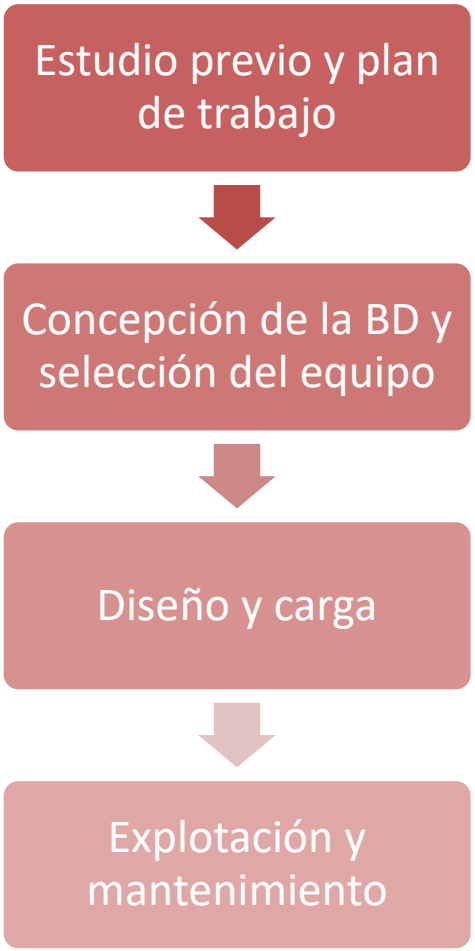
DS11: gestionar datos

- DSS11.6: requisitos de seguridad para gestión de datos
  - Información sensible asegurada y protegida apropiadamente
  - Capacidad de ver o alterar la información disponible a usuarios autorizados
  - Integridad de datos transmitidos
  - Riesgos
    - Datos sensibles mal utilizados o destruidos
    - Acceso o alteración de datos no autorizados
    - Falta de integridad en los datos transmitidos

DS11: gestionar datos

- DSS11.6: requisitos de seguridad para gestión de datos
  - Pruebas de diseño del control
    - ¿Se dispone de un proceso que identifica datos sensibles y garantiza la confidencialidad de los datos y su conformidad a la legislación?
    - ¿Se define e implementan mecanismos para transmitir y acceder a los datos de forma protegida: cifrado, autenticación, etc.?
    - ¿Se han establecido procedimientos para el acceso a las salidas de los datos y para la gestión y realización d e copias de respaldo de datos sensibles?

Objetivos de control en el ciclo de vida de una base de datos



Estudio previo y plan de trabajo

¿Existe un estudio de viabilidad?

- Diferentes alternativas para alcanzar los objetivos del proyecto
- Análisis coste/beneficio
- Valorar el desarrollo o la compra

¿El estudio de viabilidad es revisado por la alta dirección?

- Determinar si hay un apoyo explícito de la alta dirección

¿Existe un plan director para el seguimiento y gestión del proyecto acorde a los procedimientos de la organización?

Estudio previo y plan de trabajo

- ¿Existe una estructura adecuada para llevar a delante el proyecto y para gestionar la base de datos a crear?
- ¿Existe una separación de funciones clara?
  - Entre el personal de desarrollo de sistemas y el de explotación
  - Entre la explotación y el control de datos
  - Entre la administración de bases de datos y el desarrollo
- Si la separación de funciones no es total (mismas persona con diferentes funciones) se deben establecer controles compensatorios
  - Por ejemplo, mayor atención de la dirección

Concepción de la base de datos y selección del equipo

- ¿Son aceptables los modelos y técnicas de diseño de bases de datos empleados?
- ¿Se utilizan correctamente?
- ¿Cómo se ha seleccionado el equipo?
  - Necesidades de la empresa
  - Prestaciones de diferentes SGBD

Diseño y carga

- ¿Se han realizado correctamente los diseños lógico y físico?
  - Definición de datos, estructura, asociaciones, restricciones, etc.
  - Muestreo de ciertos elementos
    - Tablas, vistas, índices, etc.
    - ¿Aprobados por el usuario?
    - ¿Participó el administrador en su establecimiento?

Diseño y carga

- ¿Se planificó convenientemente la carga de datos?
  - Migración
    - Evitar pérdida de información y transmisión de datos erróneos
  - Entrada manual de datos
    - Controles para asegurar la integridad de los datos introducidos

Diseño y carga

- ¿Se hace un tratamiento adecuado de los datos de entrada erróneos?
  - Validar los datos lo más cerca al punto de origen como sea posible
- ¿Los programas implementan de forma apropiada la integridad que no se puede manejar en la base de datos?

Explotación y mantenimiento

- ¿Se han realizado pruebas de aceptación?
- ¿Se establecen los procedimientos de explotación y mantenimiento que aseguren que los datos se tratan de forma congruente y exacta y que el contenido de la base de datos sólo se modifica mediante la autorización adecuada?
- ¿Se ha llevado a cabo un proceso adecuado de ajuste y optimización de la base de datos?

Revisión post-implantación

- ¿Se ha establecido un plan para llevar a cabo una revisión de la base de datos una vez implantada?
  - ¿Se han conseguido los resultados esperados?
  - ¿Se satisfacen las necesidades de los usuarios?
  - ¿Los costes y beneficios coinciden con los previstos?

Otros procesos auxiliares

- ¿Se ha llevado a cabo una correcta formación de lo usuarios?
- ¿La documentación generada a lo largo de todo el proceso es suficiente y se ajusta a los estándares aprobados por la empresa?

Bibliografía

- Auditoría de tecnologías y sistemas de información. Mario Piattini Velthuis, Emilio del Peso Navarro, Mar del Peso
- La auditoría informática : métodos, reglas, normas. Marc Thorin