AUDITORÍA DE SISTEMAS

AUDITORÍA DE BASE DE DATOS

INTRODUCCIÓN

- La gran difusión de los Sistemas de Gestión de Bases de Datos (SGBD), junto con la consagración de los datos como uno de los Activos fundamentales de las empresas, ha hecho que los temas relativos a su control interno y auditoría cobren, cada día, mayor interés.
- Como ya se ha comentado, normalmente la auditoría informática se aplica de dos formas distintas; por un lado, se auditan las principales áreas del departamento de informática: explotación, dirección, metodología de desarrollo, sistema operativo, telecomunicaciones, bases de datos, etc.; y, por otro, se auditan las aplicaciones (desarrolladas internamente, subcontratadas o adquiridas) que funcionan en la empresa.
- La importancia de la auditoría del entorno de bases de datos hace énfasis en que es el punto de partida para poder realizar la auditoría de las aplicaciones que utiliza esta tecnología.

AUDITORÍA A UNA BASE DE DATOS (BD)

- Es el proceso que permite medir, asegurar, demostrar, monitorear y registrar los accesos a la información almacenada en las bases de datos incluyendo la capacidad de determinar:
  - Quién accede a los datos
  - Cuándo se accedió a los datos
  - Desde qué tipo de dispositivo/aplicación
  - Desde que ubicación en la Red
  - Cuál fue la sentencia SQL ejecutada
  - Cuál fue el efecto del acceso a la base de datos

OBJETIVOS GENERALES DE LA AUDITORÍA DE BD

- Disponer de mecanismos que permitan tener trazas de auditoría completas y automáticas relacionadas con el acceso a las bases de datos incluyendo la capacidad de generar alertas con el objetivo de:
  - Monitorear y registrar el uso de los datos por los usuarios Autorizados o no.
  - Mantener trazas de uso y del acceso a bases de datos
  - Permitir investigaciones
  - Generar alertas en tiempo real
  - Mitigar los riesgos asociados con el manejo inadecuado de los datos
  - Apoyar el cumplimiento regulatorio.
  - Satisfacer los requerimientos de los auditores
  - Evitar acciones criminales
  - Evitar multas por incumplimiento

METODOLOGÍAS PARA LA AUDITORÍA DE BASES DE DATOS

- **METODOLOGÍA TRADICIONAL**: En este tipo de metodología el auditor revisa el entorno con la ayuda de una lista de control (checklist), que consta de una serie de cuestiones a verificar.
- Por ejemplo:
  - ¿Existe una metodología de Diseño de Base de Datos? S / N / NA (S es Sí, N No y NA No Aplicable), debiendo registrar el auditor el resultado de su investigación.
- Este tipo de técnica suele ser aplicada a la auditoría de productos de bases de datos, especificándose en la lista de control todos los aspectos a tener en cuenta.

METODOLOGÍA DE EVALUACIÓN DE RIESGOS

- En este tipo de metodología se deben seguir una secuencia de pasos los cuales son:
- **Objetivo de Control**
  - Fijar los objetivos de Control minimizan los riesgos potenciales a los que se somete el entorno.
- **Técnica de Control**
  - Se establece los tipos de Usuario, perfiles y permisos necesarios para controlar el acceso a la base de datos.

PRUEBA DE CUMPLIMIENTO

- **Listar los privilegios y perfiles existentes.**
  - Si se detectan inconsistencias en los controles, o si los controles no existen, se diseña otro tipo de prueba que permiten dimensionar el impacto de estas deficiencias.
- **Prueba Sustantiva**
  - Comprobar si la información presenta alteraciones, comparándola con otra fuente, revisando los documentos de entrada de datos y las transacciones que se han ejecutado.

OBJETIVOS DE CONTROL EN EL CICLO DEVIDA DE UNA BASE DE DATOS

OBJETIVOS DE CONTROL EN EL CICLO DE VIDA DE UNA BASE DE DATOS

- Estudio Previo y Plan de Trabajo
  - Se elabora un estudio tecnológico de viabilidad en el cual se contemplen distintas alternativas para alcanzar los objetivos del proyecto acompañados de un análisis coste-beneficio para cada una de las opciones.
- Concepción de la BD y Selección del Equipo
  - En esta etapa se empieza a diseñar la base de datos. La metodología de diseño determina si es o no aceptable, y luego comprueba su correcta utilización.
- DISEÑO Y CARGA
  - Se llevan acabo los diseños lógico y Físico de la BD, el auditor tendrá que examinar si estos diseños se han realizado correctamente; determinando si la definición de los datos contempla además de su estructura, las asociaciones y las restricciones oportunas, así como las especificaciones de almacenamiento de datos y las cuestiones relativas a la seguridad.

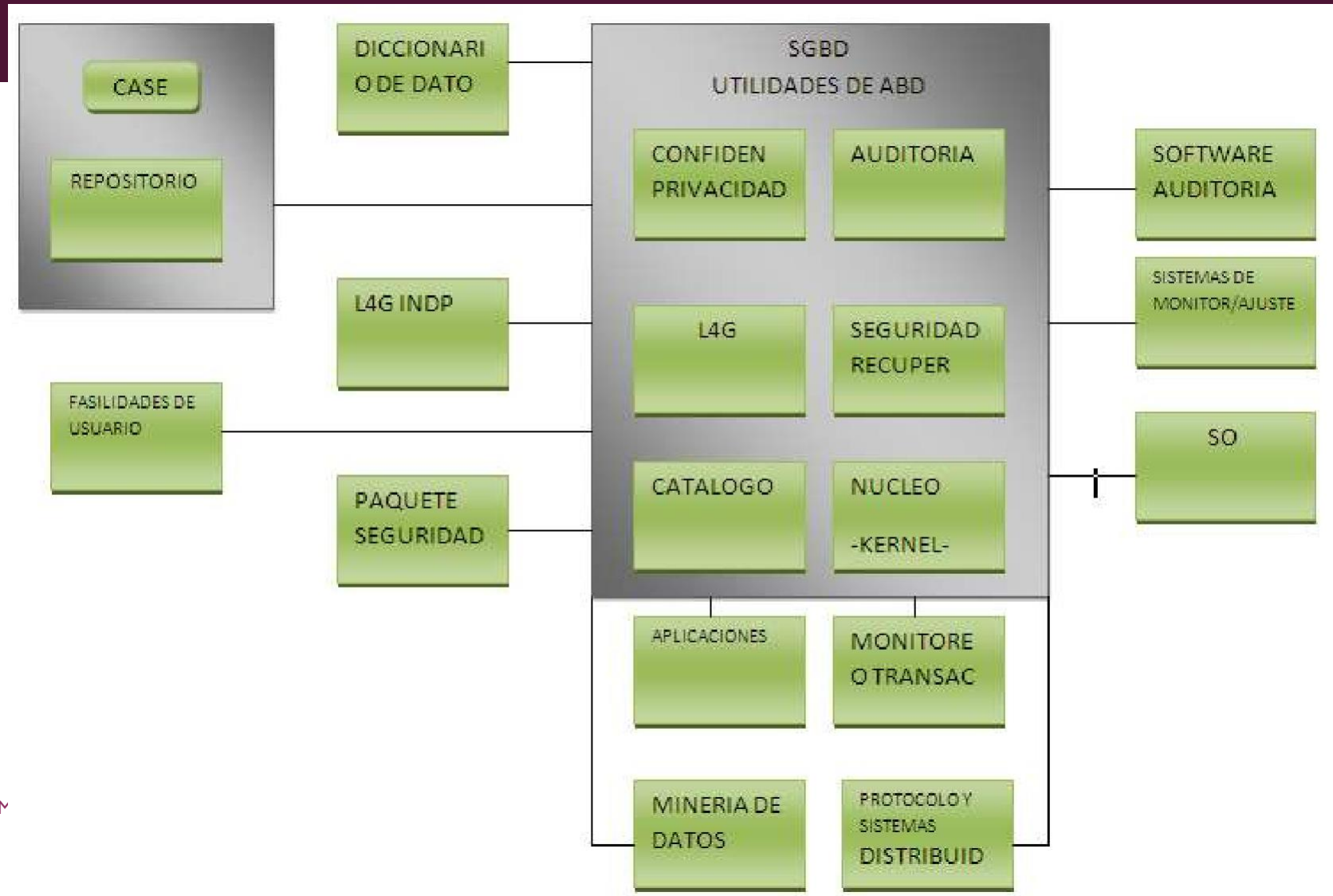
OBJETIVOS DE CONTROL EN EL CICLO DE VIDA DE UNA BASE DE DATOS

- **Explotación y Mantenimiento**
  - Se comprueba que se establezcan los procedimientos de explotación y mantenimiento que aseguren que los datos se tratan de forma congruente y exacta y que el contenido solo tendrá modificaciones mediante la autorización adecuada.
- **Revisión Post - Implantación**
  - En bastantes organizaciones omiten esta fase por falta de tiempo o recursos, pero es necesario contar con una revisión post-implantación de el sistema nuevo o modificado con el fin de evaluar:
    - Se han conseguido los resultados esperados.
    - Se satisfacen las necesidades de los usuarios.
    - Los costes y beneficios coinciden con los previstos.

AUDITORIA Y CONTROL INTERNO EN UN ENTORNO DE BASES DE DATOS

- **Sistema de Gestión de BD (SGBD)**
  - Existen diferentes componentes del SGBD como:
    - El catálogo (componente fundamental que asegura la seguridad de la BD),
    - las utilidades para el administrador (se suelen encontrar algunas para crear usuarios, conceder privilegios y resolver otras cuestiones relativas a la confidencialidad),
    - las que se encargan de la recuperación de la BD: copias de respaldo, archivos diarios, etc. entre otras.

COMPONENTES DE UN SGBD



COMPONENTES DE UN SGBD

- SOFTWARE DE AUDITORÍA
  - Paquetes que facilitan la labor del auditor, en cuanto a la extracción de datos de la BD, el seguimiento de la transacciones, datos de prueba, etc.
- SISTEMA DE MONITORIZACIÓN Y AJUSTE
  - Complementa las facilidades ofrecidas por el SGBD, ofreciendo mayor información para optimizar el sistema, llegando a ser en determinadas ocasiones verdaderos sistemas expertos.
- SISTEMA OPERATIVO (SO)
  - Es una pieza clave del entorno, en cuanto a control de memoria, gestión de área de almacenamiento intermedio, manejo de errores, control de confidencialidad, mecanismos de ínter bloqueo, etc.
- MONITOR DE TRANSACCIONES
  - Se considera un elemento mas del entorno con responsabilidades de confidencialidad y rendimiento.

COMPONENTES DE UN SGBD

- PAQUETE DE SEGURIDAD
  - Existe una gran variedad de productos que permiten la implantación de una política de seguridad, puesto que centralizan el control de accesos, la definición de privilegios, perfiles de usuario, etc.
- DICCIONARIO DE DATOS
  - Conjunto de metadatos que contiene las características lógicas y puntuales de los datos que se van a utilizar en el sistema incluyendo nombre, descripción, alias, contenido y organización.
- HERRAMIENTAS CASE
  - Permite al auditor revisar el diseño de la base de datos, comprobar si se ha empleado correctamente la metodología y asegurar un nivel mínimo de calidad.

COMPONENTES DE UN SGBD

- LENGUAJES DE 4 GENERACIÓN
  - Se utilizan en la actualidad para desarrollar prototipos que facilitan a los usuarios la exposición de necesidades.
- FACILIDADES DEL USUARIO
  - Con la aparición de interfaces graficas fáciles de usar (con menús, ratón, ventanas, etc.) se ha desarrollado toda una serie de herramientas que permiten al usuario final acceder a los datos sin tener que conocer la sintaxis de los lenguajes del SGBD.
  - El auditor debe investigar las medidas de seguridad que ofrecen estas herramientas y bajo que condiciones han sido instaladas; las herramientas de este tipo deberán " proteger al usuario de sus propios errores".
- HERRAMIENTAS DE MINERÍA DE DATOS
  - Ofrecen el soporte a la toma de decisiones sobre los datos de calidad integrados en le almacén de datos.

PASOS PARA ELABORAR UN INFORME DE AUDITORÍA

- Se requieren varios pasos para realizar una auditoría.
- El auditor de sistemas debe evaluar los riesgos globales y luego desarrollar un programa de auditoria que consta de objetivos de control y procedimientos de auditoria que deben satisfacer esos objetivos.
- El proceso de auditoria exige que el auditor de sistemas reúna evidencia, evalúe fortalezas y debilidades de los controles existentes basado en la evidencia recopilada, y que prepare un informe de auditoria que presente esos temas en forma objetiva a la gerencia.
- Asimismo, la gerencia de auditoría debe garantizar una disponibilidad y asignación adecuada de recursos para realizar el trabajo de auditoria además de las revisiones de seguimiento sobre las acciones correctivas emprendidas por la gerencia.
- La importancia de la auditoría del entorno de bases de datos radica en que es el punto de partida para poder realizar la auditoría de las aplicaciones que utiliza esta tecnología.

LA AUDITORÍA DE BD ES IMPORTANTE PORQUE:

- Toda la información financiera de la organización reside en bases de datos y deben existir controles relacionados con el acceso a las mismas.
- Se debe poder demostrar la integridad de la información almacenada en las bases de datos.
- Las organizaciones deben mitigar los riesgos asociados a la pérdida de datos y a la fuga de información.
- La información confidencial de los clientes, son responsabilidad de las organizaciones.
- Los datos convertidos en información a través de bases de datos y procesos de negocios representan el negocio.
- Las organizaciones deben tomar medidas mucho más allá de asegurar sus datos. Deben monitorearse perfectamente a fin de conocer quién o qué les hizo exactamente qué, cuándo y cómo.

PLANIFICACIÓN DE LA AUDITORIA DE BD

1. Identificar todas las bases de datos de la organización
2. Clasificar los niveles de riesgo de los datos en las bases de datos
3. Analizar los permisos de acceso
4. Analizar los controles existentes de acceso a las bases de datos
5. Establecer los modelos de auditoría de BD a utilizar
6. Establecer las pruebas a realizar para cada BD, aplicación y/o usuario

CONSIDERANDO LOS RIESGOS DE:

- Dependencia por la concentración de Datos
- Accesos no restringidos en la figura del DBA
- Incompatibilidades entre el sistema de seguridad de accesos del SGBD y el general de instalación
- Impactos de los errores en Datos y programas
- Rupturas de enlaces o cadenas por fallos del software.
- Impactos por accesos no autorizados
- Dependencias de las personas con alto conocimiento técnico

SE PUEDEN DEFINIR LOS SIGUIENTES CONTROLES:

- **Objetivo de control**: el SGBD deberá preservar la confidencialidad de la BD.
- **Técnicas de Control:** se establecen niveles y tipos de usuarios, privilegios para el control de Acceso a la base datos.

TAREA:

- Investigar sobre diferentes herramientas de software para Auditoría y Ajuste (tuning) de Base de Datos
- Elejir una alternativa de las evaluadas y justificar el por qué de su elección.
- Elaborar un listado de ventajas y desventajas de la misma.
- Elabore un informe sobre la prueba y utilización de esta aplicación.
- Incluya sus conclusiones y recomendaciones.
- Tarea grupal.

AUDITORÍA DE SISTEMAS

AUDITORÍA DE MANTENIMIENTO DE SOFTWARE

QUÉ ES AUDITORÍA DE MANTENIMIENTO DE SOFTWARE?

- Es la revisión y evaluación del mantenimiento, la documentación de los cambios y las pruebas realizadas al software de una organización,

IMPORTANCIA DE LA ETAPA DE MANTENIMIENTO

- Consume la mayor parte de los recursos empleados en un proyecto de software (más del 60% de los recursos empleados en todo el proyecto).
- Debe ser especialmente considerada en los estudios de Productividad y de la Auditoría Informática.
- Los esfuerzos de Auditoría en la etapa de mantenimiento se plasman en las primeras etapas de desarrollo de software.
- En las especificaciones del software y en la definición de requerimientos, se encuentran los primeros pasos que van a determinar el esfuerzo o dificultad de mantenimiento del software.

PRODUCTIVIDAD EN LA ETAPA DE MANTENIMIENTO

- Es frecuente que las empresas de software busquen la máxima productividad en el desarrollo de sus productos, dejando en un segundo lugar a la etapa de mantenimiento de software.

POSIBLES CONSECUENCIAS DE PRODUCTIVIDAD BAJA EN LA ETAPA DE MANTENIMIENTO:

- Implicaciones económicas
- El equipo humano que desarrolló un producto tenga que dedicarse a tiempo completo a su mantenimiento.
- Inclusión de un nuevo equipo de desarrollo para nuevos proyectos, aumentando el costo de la planilla y disminuyendo otros presupuestos.
- Desaprovechamiento al menos parcial de la experiencia adquirida por el equipo de desarrollo anterior.
- Se requiere invertir recursos en capacitación y formación del nuevo equipo hasta adquirir el conocimiento sobre los métodos y herramientas utilizadas.

MANTENIBILIDAD

- Representa la capacidad del producto software para ser modificado efectiva y eficientemente, debido a necesidades evolutivas, correctivas o mejoras.
- Es un factor crítico y fundamental cuando se realiza una auditoría de mantenimiento.
- Engloba todas aquellas características del software destinadas a hacer que el producto sea más fácilmente mantenible y en consecuencia a conseguir una mayor productividad durante la etapa de mantenimiento.

CARACTERÍSTICAS DE LA MANTENIBILIDAD

- **Modularidad**: capacidad de un sistema o software que permite que un cambio en un componente tenga un impacto mínimo en los demás.
- **Reusabilidad**: capacidad de un componente que permite que sea utilizado en más de un sistema software o en la construcción de otros componentes.
- **Capacidad para ser analizado**: facilidad con la que se puede evaluar el impacto de un determinado cambio sobre el resto del software, diagnosticar las deficiencias o causas de fallos en el software, o identificar las partes a modificar.

CARACTERÍSTICAS DE LA MANTENIBILIDAD …

- **Capacidad para ser modificado**: capacidad del producto que permite que sea modificado de forma efectiva y eficiente sin introducir defectos o degradar el desempeño.
- **Capacidad para ser probado**: facilidad con la que se pueden establecer criterios de prueba para un sistema o componente y con la que se pueden llevar a cabo las pruebas para determinar si se cumplen dichos criterios.

IMPORTANCIA DE LA MANTENIBILIDAD

- Es el factor de calidad del software con mayor influencia en la etapa de mantenimiento.
- Elemento decisivo en los estudios de Auditoría Informática del Mantenimiento.
- Las métricas de mantenibilidad se encuentran en primer lugar de utilización de métricas de calidad.
- Existe una relación de dependencia entre las características de mantenibilidad del software desarrollado y el esfuerzo de mantenimiento.

LISTAS DE COMPROBACIÓN EN AUDITORIA INFORMÁTICA DEL MANTENIMIENTO

- Podríamos resaltar 5 grandes bloques o enfoques hacia los cuales poder orientar las preguntas:
  - ¿Se han tenido en cuenta las implicaciones laterales asociadas con el cambio?
  - ¿Se han tenido en cuenta los aspectos documentales en cuanto a evaluar y aprobar la petición de cambios?
  - ¿Se ha documentado el cambio, una vez realizado y procediéndose a dar información a todos los que se ven implicados en el proceso?
  - En cuanto a las revisiones técnicas formales. ¿se han realizado las adecuadas?
  - ¿Se ha hecho una revisión de aceptación final para asegurar que toda la arquitectura software, fue actualizada y probada y se procedió a los cambios adecuadamente?

LISTAS DE COMPROBACIÓN EN AUDITORIA INFORMÁTICA DEL MANTENIMIENTO …

- La utilización de grandes bloques como los mencionados nos va a permitir centrar nuestro esfuerzo de auditoria informática, permitiendo así conseguir la mayor cantidad de información que sea posible.
- Surge así la necesidad de centrar el esfuerzo de auditoria en un factor que pueda ser determinante, tal como es la Mantenibilidad en la etapa de mantenimiento del software.

MODELIZACIÓN EN LA ETAPA DE MANTENIMIENTO

- **Modelo COCOMO (COnstructive COst MOdel)**
  - Es un modelo de estimación de costes de proyectos software.
  - El importante número de proyectos tratados y la esmerada elaboración del modelo hacen que su validez perdure hasta la actualidad.
  - Este modelo ofrece formulas empíricas de estimación de costes o esfuerzos software.

MODELIZACIÓN EN LA ETAPA DE MANTENIMIENTO

- Tras aplicar la versión inicial del modelo a una amplia variedad de entornos se comprobó que no bastaba con un único modo de desarrollo, por lo que se plantaron 3 modos:
  - básico,
  - intermedio y
  - detallado
- En función de varias características como:
  - tamaño,
  - necesidades de comunicación,
  - experiencia en proyectos similares, entre otros.

MODELIZACIÓN EN LA ETAPA DE MANTENIMIENTO …

- **El básico** es adecuado para estimaciones rápidas, aunque sin una gran precisión.
- **El intermedio** considera 15 atributos del proyecto (fiabilidad requerida, tamaño de la base de datos, restricciones de memoria, tiempo de respuesta requerido, entre otros) cuya valoración actúa como factor multiplicador en el modelo.
- **La versión detallada** considera las estimaciones en cada una de las etapas del ciclo de vida del proyecto.

MODELIZACIÓN EN LA ETAPA DE MANTENIMIENTO …

- El Trafico de Cambio Anual (TCA), consiste en la proporción de instrucciones fuente que sufren algún cambio durante un año, bien sea por adicción o por modificación.
- Así, el esfuerzo en la etapa de mantenimiento, según el modelo COCOMO, viene dado como producto del esfuerzo de desarrollo y el tráfico de cambio anual.
- Toda la información necesaria para la aplicación del modelo, puede incluirse en una tabla que se denomina Tabla Histórica (TH).
- Haciendo un sencillo análisis de regresión sobre este conjunto de puntos se puede obtener la curva que mejor se ajusta.

MODELO DE ESTIMACIÓN EN EL MANTENIMIENTO

- Elementos de la mantenibilidad
- Una acción de mantenimiento puede estar compuesta por tres actividades:
  - Comprensión del cambio a realizar.
  - Modificación o realización del cambio.
  - Prueba del cambio realizado.
- El esfuerzo de mantenimiento está determinado por el esfuerzo en las tres actividades mencionadas.

MÉTRICAS DE MANTENIBILIDAD

- Se tienen 3 características que afectan de manera directa a un componente de la mantenibilidad:
  - **Métrica de comprensibilidad:** número de líneas de comentario por cada 100 líneas de código. La estrecha relación entre la documentación interna del código y el esfuerzo de comprensión es evidente,
  - **Métrica de modificabilidad**: número de líneas sin datos constantes por cada 100 líneas de código. La existencia de un gran número de datos constantes en el código implica un mayor esfuerzo para la modificación.
  - **Métrica de testeabilidad**: número de líneas de tratamiento de errores por cada 100 líneas de código. La depuración o testing del código va a ser más fácil si existen procedimientos de detección y manejo de errores.

FUNCIONES DE MANTENIBILIDAD

- Para la obtención de estas funciones se utiliza la información histórica (TH), ya que la experiencia adquirida en proyectos anteriores adquiere un gran valor al emprender proyectos nuevos. Con estas se pueden obtener valores como los índices de mantenibilidad:
- **Del producto desarrollado**
  - **XC**: Métrica de comprensibilidad
  - **XM**: Métrica de modificabilidad
  - **XT**: Métrica de testeabilidad
- **Del proceso de mantenimiento**
  - **MMC**: Esfuerzo de comprensión
  - **MMM**: Esfuerzo de modificación
  - **MMT**: Esfuerzo de prueba