**Auditoria de Base de Datos**

que es AuditoriA: La palabra auditoria viene del latín *auditorius* y de esta proviene auditor, que tiene la virtud de oír y revisar [cuentas](http://www.monografias.com/trabajos5/cuentas/cuentas.shtml), pero debe estar encaminado a un objetivo específico que es el de evaluar la eficiencia y [eficacia](http://www.monografias.com/trabajos11/veref/veref.shtml) con que se está operando

QUE ES BASE DE DATOS (BD): También denominado Banco de Datos, es el conjunto de datos que se resguardan de manera masiva y ordenada los cuales pueden ser encontrados con mayor facilidad y son susceptibles de modificaciones, ya que se encuentran relacionados entres sí.

Características de una Base de Datos:

1. Independencia lógica y física de los datos.
2. Redundancia mínima.
3. Acceso concurrente por parte de múltiples usuarios.
4. Integridad de los datos.
5. Consultas complejas optimizadas.
6. Seguridad de acceso y auditoría.
7. Respaldo y recuperación.
8. Acceso a través de [lenguajes de programación](http://www.maestrosdelweb.com/principiantes/los-diferentes-lenguajes-de-programacion-para-la-web/) estándar.

QUE ES UNA AUDITORIA DE BASE DE DATOS: 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:

1. Quién accede a los datos.
2. Cuándo se accedió a los datos.
3. Desde qué tipo de dispositivo/aplicación.
4. Desde que ubicación en la Red.
5. Cuál fue la sentencia SQL ejecutada.
6. Cuál fue el efecto del acceso a la base de datos.

Objetivos: Disponer de mecanismos que permitan capturar de una auditoría la relación del personal con el acceso a las bases de datos incluyendo la capacidad de generar, modificar y/o eliminara datos.

Importancia: Dentro de los aspectos de mayor 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 se utilizan, además que toda la información financiera de una compañía reside en una de estas, ya que debe existir controles adecuados y relacionados con el acceso a las mismas.

**METODOLOGÍAS DE LA AUDITORIA DE BASE DE DATOS.**

METODOLOGIA 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.

METODOLOGIA DE LA EVALUACION DE RIESGOS: Este tipo de metodología, conocida también por Risk Oriented Approach, esta inicia fijando objetivos de control que minimizan los riesgos potenciales a los que está sometido el entorno, de acuerdo a los siguientes riesgos:

1. Incremento de la "dependencia" del servicio informatico debido a la concentración de Datos
2. Mayores posibilidades de acceso en la figura del administrador de base de datos
3. Impcompatibilidad entre sistemas de seguridad de acceso propios del SGBD y el general de la instalación.
4. Mayor impacto de los errores en datos o programas que en los sistemas tradcionales.
5. Ruptura de enlaces o cadenas por fallos del sofware o de los programas de aplicación.
6. Mayor impaco de accesos no autorizados al diccionario de la base de datos que a un fichero tradicional.
7. Mayor dependencia del nivel de conocimientos técnicos del personal que realice tareas relacionadas conel software de base de datos.

**OBJETIVO DE CONTROL EN EL CICLO DE VIDA DE UNA BD**

ESTUDIO PREVIO Y PLAN DE TRABAJO: Primera etapa del ciclo de vida, se un estudio tecnológico el cual contempla las alternativas para alcanzar los objetivos del proyecto, mediante un análisis que involucrará los beneficios vrs. costo de las todas las opciones. Además que debe considerarse las alternativas, es decir la posibilidad de no llevar a cabo el proyecto (ya que no siempre hay una justificación para implementar una BD), así como la alternativa entre desarrollar y/o comprar una sistema que adecúese la BD a las necesidades de la compañía. Otro aspecto de importancia en esta fase es la aprobación de la estructura orgánica del proyecto, sino como también de la unidad que tendrá la responsabilidad de la gestión y control de la base de datos.

CONCEPCION DE LA BASE DE DATOS Y SELECCIÓN DEL EQUIPO: En esta fase se diseña la base de datos. La metodología de diseño deberá emplearse para especifirar los documentos fuentes, así como los mecanismos de control, los métodos de seguridad y las pistas de auditoria que se incluirá en el sistema. El auditor debe analizar la metodología del diseño para determinar si es correcto o no, y si será funcional para cubrir todas la necesidades de utilización. El requisito mínimo para el diseño de la BD deberá completar dos fases de diseño: Lógico y Físico, aunque en la mayoría de los casos se incluye una tercera fase, el Diseño Conceptual.

DISEÑO Y CARGA: En esta fase se llevarán a cabo los diseños lógico y físico de la base de datos, por lo que el auditor tendrá que examinar si estos diseños se han realizado correctamente; determinando si la definición de datos contemplan 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.

EXPLOTACIÒN Y MANTENIMIENTO: Una vez que se han realizado las pruebas de aceptación, con la participación de los usuarios, el sistema se pondrá (tras las correspondientes autorizaciones y siguiendo los procedimientos establecidos para ello) en explotación. Deben verificarse que se establecen los procedimientos de explotación y mantenimiento que aseguren que los datos se tratan de forma congruente y exacta.

REVISIÒN POST-IMPLANTACIÓNE: Establecer el desarrollo de un plan para efectuar una revisión post-implantaciónde todo sistema nuevo o modificado con el fin de evaluar si cumple con las necesidad de la empresa, mediantes las siguientes interrogantes:

* Se han conseguido los resultados esperados.
* Se satisfacen las necesidades de los usuarios.
* Los costes y beneficios coinciden con lo previsto

OTROS PROCESOS AUXILIARES: A lo largo de todo el ciclo de vida de la base de datos se deberá controlar la formación que precisan tanto los usuarios informático como los no informáticos; ya que la formación es una de las claves para minimizar el riesgo en la implantación de una base de datos.

**AUDITORIA Y CONTROL INTERNO EN UN ENTORNO DE BASE DE DATOS**

Cuando el auditor, se encuentra en explotación de la informaciòn, debera estudiar el SGBD y el entorno. El desarrollo y manteniminto de sistemas informativos entornos de BD, deberían considerarse el control, la integridad y la seguridad de los datos compartidos por multiples usuario, por tal razon deben abarcase todos los componentes de la BD, pero cabe resaltar que el entorno es cada vez mas complejo y no puede limitarse al propio de una SGBD.

SISTEMA DE GESTION DE BASE DE DATOS (SGBD)

Entre sus componentes puede destacarse:

1. El núcleo (Kernel)
2. El catálogo, componente para asegurad la seguridad de la BD
3. Las utilidades del administrador de la BD, entre las que se pueden crear usuaciros, conceder privilegios y resolver otras asuntos relatives a la confiencialidad.
4. Las que se encargan de la recuperacion de BD
5. Rearranque, copias de respaldo, archives diarios
6. Funciones de auditoria
7. Lenguaje de cuarta generaciòn (LG4) que incorpora el propio SGBD

SOFTWARE DE AUDITORIA: Son paquetes que pueden emplearse a facilitar la labor del auditor, es decir para la extracciòn de base de datos, seguimiento de transacciones, datos de prueba, etc. Hay productos muy interesantes que premiten cuadrar datos de diferentes entornos permitiendo realizar una verdadera AUDITORIA DE BASE DE DATOS.

SISTEMA DE MONITORIZACIÓN Y AJUSTE (TUNING): Este tipo de sistema complementan las facilidades ofrecidas por el propio SGBD, ofreciendo mayor información para optimizar el sistema, llegando a ser en determinadas ocasiones verdaderos sistemas expertos que proporcionan la estructura óptima de la base de datos y de ciertos parámetros del SGBD y del SO.

SISTEMA OPERATIVO (SO): Un sistema operativo (SO, siglas en inglés Operating System) es un [programa](http://es.wikipedia.org/wiki/Programa_inform%C3%A1tico) o conjunto de programas que en un sistema informático gestiona los recursos de [hardware](http://es.wikipedia.org/wiki/Hardware) y provee servicios a los [programas de aplicación](http://es.wikipedia.org/wiki/Aplicaci%C3%B3n_inform%C3%A1tica), ejecutándose en modo privilegiado respecto de los restantes y anteriores próximos y viceversa.[ Ademas que es una pieza clave del entorno puesto que el SGBD se apoyara en mayor medida de los servicios que le ofrezca el SO en cuanto control, memoria, gestion de almacenamiento, manejo de errores, control de confidencialidad, mecanismos de bloqueo, etc.

MONITOR DE TRANSACCIONES: Un sistema de procesamiento de transacciones (TPS por sus siglas en inglés) es un tipo de sistema de información que recolecta, almacena, modifica y recupera toda la información generada por las transacciones producidas en una organización. Una transacción es un evento que genera o modifica los datos que se encuentran eventualmente almacenados en un sistema de información.

PROTOCOLOS Y SISTEMAS DISTRIBUIDOS: Protocolos: Es un conjunto bien conocido de reglas y formatos que se utilizan para la comunicación entre procesos que realizan una determinada tarea. Un protocolo permite que componentes heterogéneos de sistemas distribuidos puedan desarrollarse independientemente.

Sistemas Distribuidos: Sistemas cuyos componentes hardware y software, que están en ordenadores conectados en red, se comunican y coordinan sus acciones mediante el paso de mensajes, para el logro de un objetivo. Se establece la comunicación mediante un protocolo prefijado por un esquema cliente-servidor.

PAQUETES DE SEGURIDAD: Son programas de software y servicios que ayuda a proteger tu computadora de hackers, virus, spyware y otras amenazas. Paquete de seguridad de se actualizan automáticamente para mantener al usuario protegido de nuevas amenazas por internet.

DICCIONARIO DE DATOS: Un diccionario de datos es un conjunto de metadatos que contiene las características lógicas y puntuales de los datos que se van a utilizar en el sistema que se programa, incluyendo nombre, descripción, alias, contenido y organización. Identifica los procesos donde se emplean durante el análisis de flujo de datos y auxilia a los analistas que participan en la determinación de los requerimientos del sistema, su contenido también se emplea durante el diseño.

HERRAMIENTAS CASE: Son un conjunto de herramientas y métodos asociados que proporcionan asistencia automatizada en el proceso de desarrollo del software a lo largo de su ciclo de vida. Fueron desarrolladas para automatizar esos procesos y facilitar las tareas de coordinación de los eventos que necesitan ser mejorados en el ciclo de desarrollo de software.

LENGUAJES DE CUARTA DIMENSIÓN: Los 4GL son entornos de desarrollo de aplicaciones constituidos por un conjunto de herramientas integradas. Se centran principalmente en las fases de Construcción e Implantación del ciclo de vida del desarrollo de software. Los lenguajes de cuarta generación contemplan un gran grado de abstracción que viene a crear una verdadera caja negra pues el programador no dice como se realizaran las aplicaciones que se desee crear, nada más dará una serie de parámetros que aunque dependen del programa que se quiera crear siempre van a estar muy alejados de la máquina o hardware, esta ha sido la tendencia a seguir con cada generación de los lenguajes de programación.

FACILIDADES DE USUARIO DE BASES DE DATOS: demuestran facilidades para dotar el usuario final de las más modernas y completas facilidades resultantes de la utilización de base de datos y de los ambientes que ofrecen los lenguajes de cuarta generación.

HERRAMIENTAS DE MINERIA DE DATOS: La minería de datos o exploración de datos, es un campo de las ciencias de la computación referido al proceso que intenta descubrir patrones en grandes volúmenes de conjuntos de datos. Utiliza los métodos de la inteligencia artificial, aprendizaje automático, estadística y sistemas de bases de datos. El objetivo general del proceso de minería de datos consiste en extraer información de un conjunto de datos y transformarla en una estructura comprensible para su uso posterior.

APLICACIONES: es un programa diseñado como herramienta que permite al usuario realizar uno o diversos trabajos, especialmente como una solución informática para la automatización de ciertas tareas complicadas como la contabilidad, la redacción de múltiples documentos, el control de gestión de un almacén o la ejecución presupuestaria de una entidad, siendo estas: los procesadores de texto, hojas de cálculo y bases de datos. Ciertas aplicaciones desarrolladas suelen ofrecer una gran potencia ya que están exclusivamente diseñadas para resolver un problema en específico.

**TENICAS PARA EL CONTROL DE BASES DE DATOS**

La Dirección de la empresa tiene responsabilidad en lo que se refiere a la coordinación de los distintos elementos del entorno de la Base de Datosy a la aplicación correcta y coherente de los controles de seguridad. Hay que fijar responsables y procedimientos y, en la medida de lo posible, que estos faciliten una auditoría posterior.

1. Técnica de Matrices de Control
* Es la técnica básica de toda la vida
* Matriz que por un lado lleva un elemento a controlar, y por otro, los tipos de controles de seguridad (preventivos, detectivos, correctivos) que se han diseñado para ello. En su cruce llevará la enumeración de dichos controles y la opinión del auditor sobre su funcionamiento
1. Técnica de los Caminos de Acceso
* Se documentan todas las fases (flujos) por las que pasa un dato desde su introducción por un ente (usuario / máquina) hasta que se almacena en la Base de Datos, identificando los componentes por los que pasa y los controles asociados (definidos por la entidad).
* Esto mismo se hace con los datos que se obtienen del proceso de otros (por qué componentes pasa – programa, cadenas, almacenamientos transitorios – y a qué controles es sometido.
* Esta técnica permite detectar debilidades del sistema que pongan a las datos que pongan en riesgo a nivel de: Integridad, confidencialidad y seguridad.
* Hay que poner especial cuidado en el análisis de los interfaces entre los componentes y los almacenamientos transitorios (debilidades de seguridad).