Instituto de Educación Superior Tecnológico Público

SANTIAGO ANTÚNEZ DE MAYOLO

COMPUTACIÓN E INFORMÁTICA

Manual de la Unidad Didáctica

ADMINISTRACIÓN DE BASE DE DATOS

Ing. Moisés Álvarez Huamán

2016-II

ADMINISTRACIÓN DE BASE DE DATOS

ING. MOISÉS ÁLVAREZ HUAMÁN

HUANCAYO - PERÚ
2016

ADMINISTRACIÓN DE BASE DE DATOS

AUTOR:

ÁLVAREZ HUAMÁN, MOISÉS

EDITOR:

ÁLVAREZ HUAMÁN, MOISÉS
Dirección: Jr. Amazonas Mz47 Lt8 El Tambo
Email: malvarezh@hotmail.com

Publicación.
Primera Edición, abril 2016

MÓDULO PROFESIONAL N° 02
DESARROLLO DE SOFTWARE Y GESTIÓN DE BASE DE DATOS

Competencia del Módulo

Analizar, diseñar, desarrollar |y administrar sistemas de información y sistemas de gestión de base de datos de acuerdo a los requerimientos de la organización; considerando los criterios de seguridad en la transmisión y el almacenamiento de datos

Capacidad Terminal

CAPACIDAD TERMINAL	CRITERIOS DE EVALUACIÓN
Gestionar la operatividad de la base de datos, teniendo en cuenta los estándares de calidad y seguridad.	➢ Determina las características de operatividad del servidor de base datos, de acuerdo a los requerimientos del sistema. ➢ Describe y ejecuta procedimientos de administración de la base de datos, teniendo en cuenta estándares de calidad y seguridad. ➢ Realiza tareas de gestión en el servidor, a partir de los procedimientos establecidos.

.

Actividad de Aprendizaje N° 01

Introducción a la Administración de Base de Datos

INTRODUCCIÓN.

Una Base de Datos es una colección de archivos, datos, información; ordenada, organizada, y relacionada, con la finalidad de permitir el manejo de la información para su procesamiento. Cada uno de los archivos representan una colección de registros y cada registro está compuesto de una colección de campos. Cada uno de los campos de cada registro permite llevar información de alguna característica o atributo de alguna entidad del mundo real.

El DBMS es un conjunto de programas que se encargan de manejar la creación y todos los accesos a las bases de datos. Se compone de un Lenguaje de Definición de Datos (DDL: Data Definition Languaje), de un Lenguaje de Manipulación de Datos (DML: Data Manipulation Languaje), y de un Lenguaje de Consulta (SQL: Structured Query Languaje).

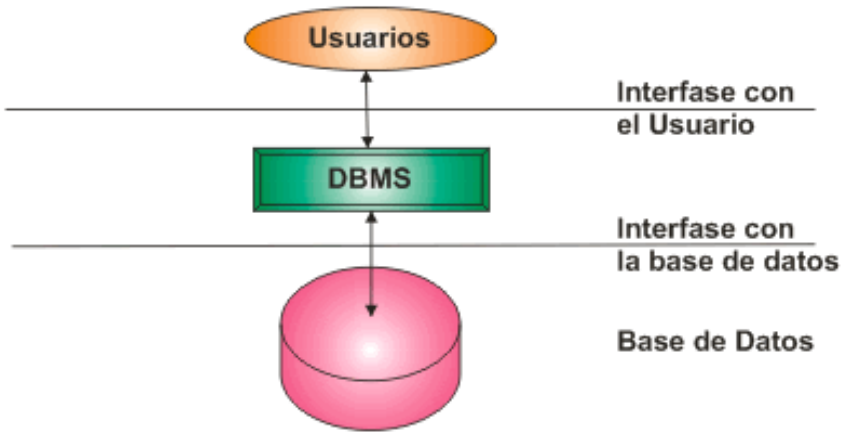
Sistema de Administración de Base de Datos (DBMS).

Es el nivel de software que provee el acceso a la información a un alto nivel de abstracción. En lugar de manipular archivos, registros, índices, el programa de aplicación opera en términos de clientes, cuentas, saldos, etc.

Acceso a la Base de Datos

La secuencia conceptual de operaciones que ocurren para accesar cierta información que contiene una base de datos es la siguiente:

- El usuario solicita cierta información contenida en la base de datos.
- l DBMS intercepta este requerimiento y lo interpreta.
- DBMS realiza las operaciones necesarias para accesar y/o actualizar la información solicitada



Proceso para Accesar Información de Bases de Datos.

Actividad de Aprendizaje N° 02

Funciones de la administración de base de datos

1. FUNCIONES DEL ADMINISTRADOR DE LA BASE DE DATOS.

1.1 Conceptos Generales.

Administrador de la Base de Datos. Es la persona encargada de definir y controlar las bases de datos corporativas, además proporciona asesoría a los desarrolladores, usuarios y ejecutivos que la requieran. Es la persona o equipo de personas profesionales responsables del control y manejo del sistema de base de datos, generalmente tiene(n) experiencia en DBMS, diseño de bases de datos, Sistemas operativos, comunicación de datos, hardware y programación.

Un Administrador de Base de Datos de tiempo completo normalmente tiene aptitudes técnicas para el manejo del sistema en cuestión a demás, son cualidades deseables nociones de administración, manejo de personal e incluso un cierto grado de diplomacia. La característica más importante que debe poseer es un conocimiento profundo de las políticas y normas de la empresa, así como el criterio de la empresa para aplicarlas en un momento dado. La responsabilidad general del DBA es facilitar el desarrollo y el uso de la Base de Datos dentro de las guías de acción definidas por la administración de los datos.

El Administrador de Bases de Datos es responsable primordialmente de:

- Administrar la estructura de la Base de Datos.
- Administrar la actividad de los datos.
- Administrar el Sistema Manejador de Base de Datos.
- Establecer el Diccionario de Datos.
- Asegurar la confiabilidad de la Base de Datos.
- Confirmar la seguridad de la Base de Datos.

Administrar la estructura de la Base de Datos.

Esta responsabilidad incluye participar en el diseño inicial de la base de datos y su puesta en practica así como controlar, y administrar sus requerimientos, ayudando a evaluar alternativas, incluyendo los DBMS a utilizar y ayudando en el diseño general de la bases de datos. En los casos de grandes aplicaciones de tipo organizacional, el DBA es un gerente que supervisa el trabajo del personal de diseño de la BD.

Una vez diseñada las bases de datos, es puesta en práctica utilizando productos del DBMS, procediéndose entonces a la creación de los datos (captura inicial). El DBA participa en el desarrollo de procedimientos y controles para asegurar la calidad y la alta integridad de la BD.

Los requerimientos de los usuarios van modificándose, estos encuentran nuevas formas o métodos para lograr sus objetivos; la tecnología de la BD se va modificando y los fabricantes del DBMS actualizan sus productos. Todas las modificaciones en las estructuras o procedimientos de BD requieren de una cuidadosa administración.

Administración de la Actividad de Datos.

El DBA no es usuario del sistema, no administra valores de datos; sino la actividad de datos; protege los datos, no los procesa. Dado que la base de datos es un recurso compartido, el DBA debe proporcionar estándares, guías de acción, procedimientos de control y la documentación necesaria para garantizar que los usuarios trabajen en forma cooperativa y complementaria al procesar datos en la bases de datos.

Administrar el Sistema Manejador de Base de Datos.

Existe una gran actividad al interior de un DBMS. La concurrencia de múltiples usuarios requiere la estandarización de los procesos de operación; el DBA es responsable de éstas especificaciones y de asegurarse que estas lleguen a quienes concierne. Todo el ámbito de la base de datos se rige por estándares, desde la forma de como se captura la información (tipo de dato, longitud, formato), como es procesada y presentada. El nivel de estandarización alcanza hasta los aspectos más internos de la base de datos; como sé accesa a un archivo, como se determinan los índices primarios y auxiliares, registros, etc.

El DBA debe procurar siempre que los estándares que serán aplicados beneficien también a los usuarios, privilegiando siempre la optimización en la operación del DBMS y el apego de las políticas de la empresa. Entre las funciones del DBA se encuentra la de revisar los estándares periódicamente para determinar su operatividad, ajustarlos, ampliarlos o cancelarlos y hacer que éstos se cumplan.

Establecer el Diccionario de Datos.

Cuando se definen estándares sobre la estructura de la base de datos, se deben de registrarse en una sección del diccionario de datos a la que todos aquellos usuarios relacionados con ese tipo de proceso pueden acceder. Este metadato debe precisar información que nos indique con claridad el tipo de datos que serán utilizados, sus ámbitos de influencia y sus limitantes de seguridad.

Asegurar la Confiabilidad de la Base de Datos

Se trata de realizar un sistema de bases de datos lo suficientemente robusto para que sea capaz de recuperarse frente a errores o usos inadecuados. Se deben utilizar gestores con las herramientas necesarias para la reparación de los posibles errores que las bases de datos pueden sufrir, por ejemplo tras un corte inesperado de luz.

Confirmar la Seguridad de la Base de Datos.

Coordinar las nuevas propuestas para realizar ajustes en los derechos de acceso a datos compartidos y aplicaciones específicamente propuestas serían analizados en conjunto con los supervisores o directivos de las áreas involucradas para determinar si procede pudieran aparecer problemas cuando dos o más grupos de usuarios quedan autorizados para notificar los mismos datos. Uno de tales conflictos es el de la actualización perdida; este ocurre cuando el trabajo de un usuario queda sobrescrito sobre por el de un segundo usuario. El DBA queda responsabilizado para identificar la posible ocurrencia de dichos problemas así como de crear normas y procedimientos para su eliminación. Se obtendrán este tipo de garantías cuando el DBMS sea capaz de implementar las restricciones aplicables al acceso concurrente, y este sea utilizado adecuadamente por programadores y usuarios; para borrar lo anterior, se hace indispensable el apego a los estándares el seguimiento de instructivos y manuales y las reglas establecidas para los diversos procesamientos y procedimientos que se llevan acabo.

Entre las alternativas mas utilizadas por el DBA para tratar de resolver o minimizar este problema se encuentran las siguientes:

- Restringir el acceso a los procedimientos para ciertos usuarios.
- Restringir al acceso a los datos para ciertos usuarios procedimientos y/o datos.

- Evitar la coincidencia de horarios para usuarios que comparten.

Las técnicas de recuperación son otra función esencial del DBA al administrar la actividad de datos. A pesar de que el DBMS lleva a cabo una parte del proceso de recuperación, los usuarios determinan en forma critica la operatividad de esos sistemas de protección. El DBA debe anticipar fallas y definir procedimientos estándares de operación; los usuarios deben saber que hacer cuando el sistema este caído y que es lo primero que debe realizarse cuando el sistema este puesto en marcha nuevamente. El personal de operación deberá saber como iniciar el proceso de recuperación de la BD que copias de seguridad utilizar; como programar la reejecución del tiempo perdido y de las tareas pendientes; es importante también establecer un calendario para llevar a cabo estas actividades sin afectar a otros sistemas dentro de la organización que hagan uso de los mismos recursos de computo. Destacan por su importancia en el proceso de recuperación y a su vez en la atención que prestan a otros sectores de la organización. Los dispositivos de comunicación remota, los sistemas de interconexión y otros accesorios de uso compartido.

El DBA es el responsable de la publicación y mantenimiento de la documentación en relación con la actividad de los datos, incluyendo los estándares de la BD, los derechos de recuperación y de acceso a la BD, los estándares para la recuperación de caídas y el cumplimiento de las políticas establecidas. Los productos DBMS más populares que se encuentran en el mercado proporcionan servicios de utilerías para ayudar al DBA en la administración de los datos y su actividad. Algunos sistemas registran en forma automática los nombres de los usuarios y de las aplicaciones a las que tienen acceso así como a otros objetos de la BD. Incorpora también utilerías que permitan definir en el diccionario de datos las restricciones para que determinadas aplicaciones o módulos de ellas solo tengan acceso a segmentos específicos de la BD.

Objetivos del Administrador de la Base de Datos.

Mantener la Integridad de los Datos. Una base de datos debe protegerse de accidentes tales como los errores en la entrada de los datos o en la programación, del uso mal intencionado de la base de datos y de los fallos del hardware o del software que corrompen los datos. La protección contra accidentes, que ocasiona inexactitudes en los datos, es parte del objetivo de garantizar la integridad de los datos. Estos accidentes incluyen los fallos durante el procesamiento de las transacciones, los errores lógicos que infringen la suposición de que las transacciones preservan las restricciones de consistencia de la base de datos y las anomalías debido al acceso concurrente en la base de datos (acceso concurrente). La integridad, se encarga de asegurar que las operaciones ejecutadas por los usuarios sean correctas y mantengan la consistencia de la base de datos.

Mantener la Seguridad de los Datos. La protección de la base de datos de usos mal intencionados o no autorizados se denomina seguridad de los datos. La seguridad se encarga de limitar a los usuarios a ejecutar únicamente las operaciones permitidas.

Mantener la Disponibilidad de los Datos. La posibilidad de fallos de hardware o de software requiere procedimientos de recuperación de la base de datos. Tiene que proporcionar medios para el restablecimiento de las

bases de datos que se hayan corrompido por desperfectos del sistema, a un estado uniforme.

Funciones Básicas del Administrador de la Bases de Datos.

Creación de Bases de Datos y Tablas.

Creando Bases de Datos:

- Localización de las bases de datos.
- Tipo de base de datos (modo de direccionamiento).

Creando Tablas:

- Seleccionando tipos de datos.
- Tablas fragmentadas o no fragmentadas.
- Localización de la tabla.
- Determinación del espacio en disco.
- Modo de aseguramiento de candados.

Especificación de las Restricciones de Integridad de los Datos. Las

1.2 Funciones Específicas del DBMS

El sistema manejador de bases de datos es la porción más importante del software de un sistema de base de datos. Un DBMS es una colección de numerosas rutinas de software interrelacionadas, cada una de las cuales es responsable de alguna tarea específica. El DBMS es un conjunto de programas que coordina y controla la creación y los accesos a la base de datos. Se compone de un Lenguaje de Definición de Datos (DDL), que es la parte estática en donde se define la estructura de la base de datos; de un Lenguaje de Manipulación de Datos (DML) que es la parte dinámica y de un Lenguaje de Consulta (SQL).

A demás de administrar la actividad de datos y la estructura de la base de datos, el DBA debe administrar el DBMS mismo. Deberá compilar y analizar estadísticas relativas al rendimiento del sistema e identificar áreas potenciales del problema. Dado que la BD esta sirviendo a muchos grupos de usuarios, el DBA requiere investigar todas las quejas sobre el tiempo de respuesta del sistema, la precisión de los datos y la facilidad de uso. Si se requieren cambios el DBA deberá planearlos y ponerlos en práctica.

El DBA deberá vigilar periódica y continuamente las actividades de los usuarios en la base de datos. Los productos DBMS incluyen tecnologías que reúnen y publican estadísticas. Estos informes pudieran indicar cuales fueron los usuarios activos, que archivos y que elementos de datos han sido utilizados, e incluso el método de acceso que se ha aplicado. Pueden capturarse y reportarse las tasas de error y los tipos de errores. El DBA analizará estos datos para determinar si se necesita una modificación en el diseño de la BD para manejar su rendimiento o para facilitar las tareas de los usuarios; de ser así, el DBA la llevará a cabo.

El DBA deberá analizar las estadísticas de tiempo de ejecución sobre la actividad de la BD y su rendimiento. Cuando se identifique un problema de rendimiento, ya sea mediante una queja o un informe, el DBA deberá determinar si resulta apropiada una modificación a la estructura de la base de datos o al sistema. Casos como la adición de nuevas claves o su eliminación, nuevas relaciones entre los datos y otras situaciones típicas deberán ser analizadas para determinar el tipo de modificación procedente.

Cuando el fabricante del DBMS en uso anuncie una nueva versión del producto, debe realizarse un análisis de las características que esta incorpora

e insopesarlas contra las necesidades de la comunidad de usuarios. Si se decide la adquisición del producto, los usuarios deben ser notificados y capacitados en su uso. El DBA deberá administrar y controlar la migración tanto de las estructuras, como de los datos y las aplicaciones. El software de soporte y otras características de hardware pueden implicar también modificaciones de las que el DBA es responsable ocasionalmente, estas modificaciones traen como consecuencia cambios en la configuración o en algunos parámetros de operación del DBMS.

Las Funciones Principales de un DBMS son:

Manejo de un Diccionario de Datos. Definiciones y relaciones entre los datos.

Administración de los Datos Almacenados. Creación de estructuras complejas requeridas para el almacenamiento de los datos, descargando al usuario de definir y programar las características físicas de los datos.

Transformación y Presentación de los Datos. Transformación de los datos nuevos para que satisfaga la estructura ya definida.

Seguridad. Fortalece la seguridad y la privacidad.

Control de Concurrencia. Controla el acceso multiusuarios. Consiste en controlar la interacción entre los usuarios concurrentes para no afectar la inconsistencia de los datos.

Integridad de Datos. Minimiza la redundancia y maximiza la consistencia. Consiste en contar con mecanismos que permitan el control de la consistencia de los datos evitando que estos se vean perjudicados por cambios no autorizados o previstos.

Lenguaje de Acceso a la Base de Datos. (Interfaz para la programación de aplicaciones). Provee acceso a los datos vía lenguaje de consulta SQL y vía lenguaje procedural (pascal, c, etc.).

Interfaz de Comunicación de Datos. Permite el requerimiento de usuarios en ambiente de red. Crear y organizar la Base de datos. Establecer y mantener las trayectorias de acceso a la base de datos de tal forma que los datos puedan ser accesados rápidamente. Manejar los datos de acuerdo a las peticiones de los usuarios. Registrar el uso de las bases de datos.

Interacción con el manejador de archivos. Esto a través de las sentencias en DML al comando de el sistema de archivos. Así el Manejador de base de datos es el responsable del verdadero almacenamiento de los datos.

Respaldo y recuperación. Consiste en contar con mecanismos implantados que permitan la recuperación fácilmente de los datos en caso de ocurrir fallas en el sistema de base de datos.

Manejador de Bases de Datos.

Su propósito es definir una arquitectura que sirva como referencia. Esta también es llamada arquitectura referencial a tres niveles, consta de tres niveles:

Nivel Interno: Es el más cercano al almacenamiento físico; es decir, es el que se ocupa de la forma como se almacena físicamente los datos.

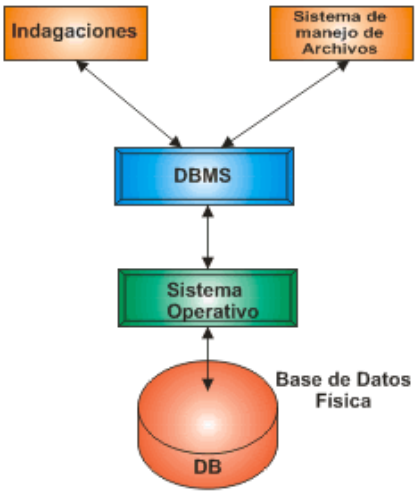
Nivel Externo: Es el más cercano a los usuarios; es decir, es el que se ocupa de la forma como los usuarios individuales perciben los datos.

Nivel Conceptual: Es el nivel de mediación entre los dos anteriores. En este se trabaja con información; esto es, con datos suficientes para provocar acciones. La vista conceptual es la representación de toda la información contenida en la base de datos, también una forma un tanto abstracta si se

compara con el almacenamiento físico de los datos. La información es una esencia nueva y no redundante por lo que su adquisición aumenta el conocimiento.

El Sistema Administrador de la Base de Datos.

Un sistema de base de datos, es la combinación de programas y archivos que se utilizan conjuntamente. Un conjunto integrado de programas para dar apoyo en una base de datos puede formar un sistema de manejo de bases de datos y sirve además para supervisar y mantener la vista lógica global de los datos. El DBMS es conocido también como Gestor de Base de datos.



Sistema Gestor de Base de Datos.

El DBMS sirve como interfase entre la base de datos física y las peticiones del usuario. El DBMS interpreta las peticiones de entrada/salida del usuario y las manda al sistema operativo para la transferencia de datos entre la unidad de memoria secundaria y la memoria principal. En sí, un sistema manejador de base de datos es el corazón de la base de datos ya que se encarga del control total de los posibles aspectos que la puedan afectar.

Actividad de Aprendizaje N° 03

Implementación del esquema conceptual (nivel lógico)

2. IMPLEMENTACIÓN DEL ESQUEMA CONCEPTUAL (NIVEL LÓGICO GLOBAL)

El nivel conceptual describe la estructura lógica global de la base de datos forma significativa el desempeño del sistema.

2.2 Esquema de Integridad.

Integridad: Consiste en conservar la seguridad en un sistema que se permite a múltiples usuarios el acceso al sistema y compartir la base de datos. Tiene como función proteger la base de datos contra operaciones que introduzcan inconsistencias en los datos. Se habla de integridad en el sentido de corrección, validez o precisión de los datos. Un control de integridad o restricciones es aquel que nos permite definir con precisión el rango de valores validos para un elemento y/o las operaciones que serán consideraciones validas en la relación de tale elementos.

El objetivo primordial de un control de integridad es la reducción de la inconsistencia en la BD.

Las restricciones de integridad normalmente se aplican en tres niveles:

- **Un Atributo Simple:** Se define un dominio del atributo que es totalmente independiente del resto del entorno de la Base de Datos. Es un atributo que tiene un solo componente, que no se puede dividir en partes mas pequeñas que tengan un significado propio(valor único). Se identifica por la letra inicial en mayúscula.
- **Un Atributo Dependiente de Otro:** Se definen subconjuntos de dominios posibles para un atributo X según el valor que previamente a sido asignado al atributo W. También es conocido como *atributos de grupo* y se representa por medio de corchetes.
- **Relaciones entre Tuplas de una o varias Tablas:** Se especifican valores posibles para registros completos según los valores acumulados registros previos o por valores existentes en registros de otras tablas. También es conocido como *objeto simétrico* y se representa con un rectángulo sombreado y todo con mayúscula.

Reglas de Integridad.

Integridad de referencial. Se aplica a las claves ajenas: si en una relación hay alguna clave ajena, sus valores deben coincidir con valores de la clave primaria a la que hace referencia, o bien, deben ser completamente nulo. Se enmarca en términos de estados de la base de datos indica lo que es un estado ilegal pero no dice como puede evitarse. Existen 2 opciones rechazar la operación o bien aceptar la operación y realizar operaciones adicionales compensatorias que conduzcan a un estado legal.

Por lo tanto, para cada clave ajena de la base de datos habrá que contestar a tres preguntas:

Reglas de los nulos: ¿tiene sentido que la clave ajena acepte nulos?

Regla de borrado: ¿Qué ocurre si se intenta borrar la tupla referenciada por la clave ajena?

- **Restringir*:*** no se permite borrar la tupla referenciada.
- **Propagar***:* se borra la tupla referenciada y se propaga el borrado a las tuplas la referencia mediante la clave ajena.
- **Anular:** se borra la tupla referenciada y las tuplas que la reverenciaba ponen a nulo la clave ajena (solo si acepta nulos).

Reglas de modificación: ¿Qué ocurre si se intenta modificar el valor de la clave primaria de la tupla referenciada por la clave ajena?

- **Restringir:** no se permite modificar el valor de la clave primaria de la tupla referenciada.
- **Propagar:** se modifica el valor de la clave primaria de la tupla referenciaba y se propaga la modificación a las tuplas que la referencia mediante clave ajena.
- **Anular:** se modifica la tupla referenciada y las tuplas que la referenciaban ponen a nulo la clave ajena (solo si acepta nulos).

Reglas de Integridad de Dominio. Un dominio de valores posibles puede estar asociado con cada atributo. Los límites de dominio son la forma mas elemental de restricciones de integridad. Son fáciles de probar por el sistema siempre que se introduce un nuevo dato en la base de datos.
Tipos de dominios: Es posible que varios atributos tengan el mismo dominio. Podemos ver que una definición adecuada de restricciones de dominio no solo nos permite probar consultas para asegurar que la comparación que se hace tiene sentido. El principio que hay detrás de los dominios de atributo es similar al que hay detrás de la asignación de tipos a variables en los lenguajes de programación. Los lenguajes de programación fuertemente tipiados permiten que el compilador el programa con mayor detalle.
Integridad de relaciones. Esta regla se aplica a las claves primarias de las relaciones base: *ningún atributo que forme parte de una llave primaria puede aceptar valores nulos.* Por definición, una clave primaria es irreducible que se utiliza para identificar de modo único las tuplas. Irreducible significa que ningún subconjunto de la clave primaria sirve para identificar las tuplas de modo único. Si se permite que parte de la clave primaria sea nula, se está diciendo que no todos sus atributos son necesarios para distinguir las tuplas, con lo que se contradice la irreducibilidad. Esta regla solo se aplica a las relaciones base y a las claves primarias, no a las claves alternativas.
Nulos: Ningún atributo que forme parte de una llave primaria puede aceptar valores nulos. Un valor *nulo* es un valor que esta fuera de la definición de cualquier dominio el cual permite dejar el valor del atributo "latente"; en otras palabras, un valor nulo no representa el valor cero, ni una cadena vacía, éstos son valores que tienen significado; implica ausencia de información por que se desconoce el valor del atributo o simplemente no tiene sentido.
Reglas de negocio: Los usuarios o los administradores de la base de datos pueden imponer ciertas restricciones específicas sobre los datos, a esto se le conoce como *reglas de negocio*.

2.3 Esquema de Seguridad y Autorización.

Seguridad: El objetivo es proteger la Base de Datos contra accesos no autorizados. Se le conoce también como privacidad.
Incluye aspectos de:

- Aspectos legales, sociales y éticos.
- Políticas de la empresa, niveles de información pública y privada.
- Controles de tipo físico, acceso a las instalaciones.
- Identificación de usuarios: voz, retina del ojo, etc.
- Controles de sistema operativo.

En relación al SGBD, debe mantener información de los usuarios, su tipo y los accesos y operaciones permitidas a éstos.

El problema de la seguridad consiste en lograr que los recursos de un sistema sean, bajo toda circunstancia, utilizados para los fines previstos. Para eso se utilizan mecanismos de protección. Un aspecto importante de la seguridad es el de impedir la pérdida de información, la cual puede producirse por diversas causas: fenómenos naturales, guerras, errores de hardware o de software, o errores humanos. La solución es una sola: mantener la información respaldada, de preferencia en un lugar lejano

Otro aspecto importante de la seguridad, es el que tiene que ver con el uso no autorizado de los recursos:

- Lectura de datos.
- Modificación de datos.
- Destrucción de datos.
- Uso de recursos: ciclos de CPU, impresora, almacenamiento.

Otras amenazas y ataques posibles:

Virus. Un virus es parecido a un gusano, en cuanto se reproduce, pero la diferencia es que no es un programa por sí sólo, si no que es un trozo de código que se adosa a un programa legítimo, contaminándolo. Cuando un programa contaminado se ejecuta, ejecutará también el código del virus, lo que permitirá nuevas reproducciones, además de alguna acción (desde un simple mensaje inocuo hasta la destrucción de todos los archivos).

Caballo de troya. Un caballo de troya es un programa aparentemente útil que contiene un trozo de código que hace algo no deseado.

Puerta trasera. Una puerta trasera es un punto de entrada secreto, dejado por los implementadores del sistema para saltarse los procedimientos normales de seguridad. La puerta trasera puede haberse dejado con fines maliciosos o como parte del diseño; en cualquier caso, son un riesgo.

Caza claves. Dejar corriendo en un terminal un programa que pida "login:" y luego "password:", para engañar a los usuarios de modo que estos revelen su clave.

Solicitar recursos como páginas de memoria o bloques de disco, y ver qué información contienen; muchos sistemas no los borran cuando se liberan, de modo que se puede encontrar información "interesante". Sobornar o torturar al administrador para que suelte la clave.

Principios básicos para la seguridad:

- Suponer que el diseño del sistema es público.
- El defecto debe ser: sin acceso.
- Chequear permanentemente.
- Los mecanismos de protección deben ser simples, uniformes y construidos en las capas más básicas del sistema.
- Los mecanismos deben ser aceptados sicológicamente por los usuarios.

Tipos de usuarios:

Podemos definir a los usuarios como toda persona que tenga todo tipo de contacto con el sistema de base de datos desde que este se diseña, elabora, termina y se usa.

- DBA, están permitidas todas las operaciones, conceder privilegios y establecer usuarios. Usuario con derecho a crear, borrar y modificar objetos y que además puede conceder privilegios a otros usuarios sobre los objetos que ha creado. Privilegios sobre los objetos, añadir nuevos campos, indexar, alterar la estructura de los objetos, etc.

- Programadores de aplicaciones. Los profesionales en computación que interactúan con el sistema por medio de llamadas en DML (Lenguaje de Manipulación de Datos), las cuales están incorporadas en un programa escrito en un lenguaje de programación (Por ejemplo, Cobol, PL/I, Pascal, C, etc.).
- Usuarios sofisticados. Los usuarios sofisticados interactúan con el sistema sin escribir programas. En cambio escriben sus preguntas en un lenguaje de consultas de base de datos.
- Usuarios especializados. Algunos usuarios sofisticados escriben aplicaciones de base de datos especializadas que no encajan en el marco tradicional de procesamiento de datos.
- Usuarios ingenuos. Los usuarios no sofisticados interactúan con el sistema invocando a uno de los programas de aplicación permanentes que se han escrito anteriormente en el sistema de base de datos, podemos mencionar al usuario ingenuo como el usuario final que utiliza el sistema de base de datos sin saber nada del diseño interno del mismo por ejemplo: un cajero.

Los SGBD tienen opciones que permiten manejar la seguridad, tal como GRANT, REVOKE, etc. También tienen un archivo de auditoria en donde se registran las operaciones que realizan los usuarios.

Medidas de Seguridad

Físicas: Controlar el acceso al equipo. Tarjetas de acceso, etc.
Personal: Acceso sólo del personal autorizado. Evitar sobornos, etc.
SO: Seguridad a nivel de SO.
SGBD: Uso herramientas de seguridad que proporcione el SGBD. Perfiles de usuario, vistas, restricciones de uso de vistas, etc.

Un SMBD cuenta con un subsistema de seguridad y autorización que se encarga de garantizar la seguridad de porciones de la BD contra el acceso no autorizado:

- Identificar y autorizar a los usuarios: uso de códigos de acceso y palabras claves, exámenes, impresiones digitales, reconocimiento de voz, barrido de la retina, etc.
- Autorización: usar derechos de acceso dados por el terminal, por la operación que puede realizar o por la hora del día.
- Uso de técnicas de cifrado: para proteger datos en Base de Datos distribuidas o con acceso por red o internet.
- Diferentes tipos de cuentas: en especial del ABD con permisos para: creación de cuentas, concesión y revocación de privilegios y asignación de los niveles de seguridad.
- Manejo de la tabla de usuarios con código y contraseña, control de las operaciones efectuadas en cada sesión de trabajo por cada usuario y anotadas en la bitácora, lo cual facilita la auditoria de la Base de Datos.

Identificación y Autentificación.

En un SGBD existen diversos elementos que ayudan a controlar el acceso a los datos. En primer lugar el sistema debe identificar y autentificar a los usuarios utilizando alguno de las siguientes formas:

- Código y contraseña.
- Identificación por hardware.
- Características bioantropométricas.
- Conocimiento, aptitudes y hábitos del usuario.

- Información predefinida (Aficiones, cultura, etc.)

Además, el administrador deberá especificar los privilegios que un usuario tiene sobre los objetos:

- Usar una B.D.
- Consultar ciertos datos.
- Actualizar datos.
- Crear o actualizar objetos.
- Ejecutar procedimientos almacenados.
- Referenciar objetos.
- Indexar objetos.
- Crear identificadores.

Mecanismos de Autentificación.

La autentificación, que consiste en identificar a los usuarios que entran al sistema, se puede basar en posesión (llave o tarjeta), conocimiento (clave) o en un atributo del usuario (huella digital).

Claves: El mecanismo de autentificación más ampliamente usado se basa en el uso de claves o passwords; es fácil de entender y fácil de implementar. Sin embargo, una proporción demasiado grande de las claves escogidas por los usuarios son fáciles de adivinar, pues la idea es que sean también fáciles de recordar. La clave también se puede descubrir mirando (o filmando) cuando el usuario la digita, o si el usuario hace login remoto, interviniendo la red y observando todos los paquetes que pasan por ella. Por último, además de que las claves se pueden descubrir, éstas también se pueden "compartir", violando las reglas de seguridad. En definitiva, el sistema no tiene ninguna garantía de que quien hizo login es realmente el usuario que se supone que es.

Identificación física: Un enfoque diferente es usar un elemento físico difícil de copiar, típicamente una tarjeta con una banda magnética. Para mayor seguridad este enfoque se suele combinar con una clave (como es el caso de los cajeros automáticos). Otra posibilidad es medir características físicas particulares del sujeto: huella digital, patrón de vasos sanguíneos de la retina, longitud de los dedos. Incluso la firma sirve.

Algunas medidas básicas:

- Demorar la respuesta ante claves erróneas; aumentar la demora cada vez. Alertar si hay demasiados intentos.
- Registrar todas las entradas. Cada vez que un usuario entra, chequear cuándo y desde dónde entró la vez anterior.
- Hacer chequeos periódicos de claves fáciles de adivinar, procesos que llevan demasiado tiempo corriendo, permisos erróneos, actividades extrañas (por ejemplo cuando usuario está de vacaciones).

Matriz de Autorización.

Autorizaciones. Para facilitar la administración los SGBD suele incorporar el concepto de perfil, rol o grupo de usuarios que agrupa a una serie de privilegios por lo que el usuario que se asigna a un grupo hereda todos los privilegios del grupo. El mecanismo de control de acceso se encarga de denegar o conceder el acceso a los usuarios. En un SGBD puede existir diferentes tipos de autorización:

Una primera distinción puede hacerse entre:

Autorización explicita. Normalmente usada en los sistemas tradicionales. Consiste en almacenar que sujetos pueden accesar a ciertos objetos con

determinados privilegios para lo que suele utilizarse una matriz de control de accesos.

Autorización implícita. Consiste en que una autorización definida sobre un objeto puede deducirse a partir de otras (por ejemplo si se puede acceder a una clase en un SGBD se puede también acceder a todas las instancias de esa clase).

Los usuarios pueden tener varios tipos de autorización para diferentes partes de la base de datos. Entre ellas están las siguientes:

- **La autorización de lectura** permite la lectura de los datos, pero no su modificación
- **La autorización de inserción** permite la inserción de datos nuevos, pero no la modificación de los existentes.
- **La autorización de actualización** permite la modificación de los datos, pero no su borrado.
- **La autorización de borrado** permite el borrado de los datos.

Los usuarios pueden recibir todos los tipos de autorización o ninguno de ellos, o una combinación determinada de los mismos. Además de estas formas de autorización para el acceso a los datos los usuarios pueden recibir autorización para modificar el esquema de la base de datos:

- **La autorización de índices** permite la creación y borrado de índices.
- **La autorización de recursos** permite la creación de las relaciones nuevas.
- **La autorización de alteración** permite el añadido o el borrado de atributos de las relaciones.
- **La autorización de eliminación** permite el borrado de relaciones.

Las autorizaciones de eliminación y de borrado se diferencian en que la autorización de borrado solo permite el borrado de tuplas. Si un usuario borra todas las tuplas de una relación, la relación sigue existiendo, vacía. Si se elimina una relación, deja de existir. La capacidad de crear nuevas relaciones queda regulada mediante la autorización de recursos. El usuario con la autorización de recursos que crea una relación nueva recibe automáticamente todos los privilegios sobre el sistema.

La autorización de índices puede parecer innecesaria, dado que la creación o borrado de un índice no afecta a los datos de las relaciones. Más bien, los índices son una estructura para las mejoras de rendimiento. Sin embargo, los índices también ocupan espacio y se exige que las modificaciones de las bases de datos actualicen los índices , los que llevaran a cabo actualizaciones estarían tentados de borrar los índices , los que llevan a cabo actualizaciones estarían tentados de borrar los índices, mientras que los que formulara consultas estarían tentados de crear numeroso índices.

La forma superior de autoridad es la concebida al administrador de la base de datos. El administrador de la base de datos puede autorizar usuarios nuevos, reestructurar la base de datos, etc. Esta forma de autorización es análoga a la proporcionada al súper usuario u operador del sistema operativo.

Riesgos para la Seguridad de la Información.

Riesgos en la Implantación. Cuando se esta instalando o actualizando un sistema, los principales factores de riesgo son aquellos relacionados con el ajuste de formatos, dominios y otros parámetros que pueden verse afectados por la conversión del sistema; ya sea manual-automatizado o automatizado-automatizado. Cuando el sistema que se implanta ha de recibir nueva

información, es importante el establecimiento de códigos que permitan validar la captura para minimizar los riesgos de información no confiable.

Riesgos en la Operación. Mientras el sistema se encuentra en uso, se dice que las operaciones se realizan en línea; es decir, la información se afecta por medio de los procedimientos definidos en el sistema. La protección más común para reducir estos riesgos consiste en el establecimientos de claves de operación (password) tanto para accesar a la aplicación como a las diversas operaciones que esta desempeña.

Las claves pueden asignarse:

- Genérico
- Por niveles de seguridad
- Por tipos de acceso a los datos.

Criterios para la selección de las claves de acceso:

- No información que pueda asociarse al usuario.
- Fácil de recordar, difícil de adivinar.
- Debe utilizar un parámetro variable o algoritmo

Algunos sistemas que manejan claves fijas pueden incluir controles sobre el usuario que lo obliguen a modificar su clave de acceso con cierta regularidad. Es importante que el código que mantiene la tabla de claves de usuarios en el sistema se encuentre codificada o encriptada.

Riesgos en Tiempos Muertos. Cuando el sistema no se encuentra en operación la información esta expuesta a ser alterada fuera de línea; es decir, sin utilizar los programas de aplicación diseñados para este fin. Algunas de las técnicas más utilizadas para evitar y en algunos casos solo para ejecutar modificaciones fuera de línea son:

- *Encriptamiento*.- Consiste en convertir la información de la BD a un formato que resulte ilegible sino se dispone del algoritmo de conversión.
- *Aplicación de Totales de Control.*- Consiste en generar registros ficticios que son agregados a la BD y que permitirán detectar la inserción, eliminación o modificación de datos en la gran mayoría de los casos. Los registros ficticios son creados con información que se obtiene de acumulados o valores estadísticos de los registros reales.
- *Dígitos de Control*.- son caracteres que se anexan a las claves o a los datos que serán manejados con el objeto de autentificar su validez. Su aplicación se extiende a procesos en línea y protección fuera de línea.

Consideraciones en Ambiente Multiusuario.

Precauciones adicionales a las anteriores, deben ser tomadas en cuenta para elevar el nivel de seguridad en redes de usuarios. Las más comunes son:

- Validar no contraseñas repetidas.
- Eliminar claves de acceso de usuarios deshabilitados.
- Establecer políticas y sanciones por desatender estaciones desconectadas (con acceso).
- Restringir procesos de alto riesgo a terminales con mayor nivel de seguridad y/o vigilancia.
- Establecer controles dial-up/call-back para el acceso validado a las terminales; es decir, implementar sistemas electrónicos de autenticación de terminal.
- Establecer políticas para denegar el acceso después de una cantidad determinada de intentos fallidos de un tiempo transcurrido.

Controles Genéricos de Acceso.

Debe considerarse la posibilidad de controles alternos cuando el sistema maneja información o recursos altamente privilegiados para la organización. Las formas más comunes para autentificar la identidad del usuario son:

- Algo que el usuario conoce.- Password, contraseña, algoritmos de acceso.
- Algo que el usuario tiene.- Tarjetas de acceso, bandas magnéticas etc.
- Identificación de aspectos físicos del usuario.- Huellas digitales, examen de la retina, voz etc.

2.4 Herramientas.

El esquema conceptual se construye utilizando la información que se encuentra en la especificación de los requisitos de usuario. El diseño conceptual es completamente independiente de los aspectos de implementación, como pueden ser el SGBD que se va a usar, los programas de aplicación, los lenguajes de programación, el hardware disponible o cualquier otra consideración física. Durante todo el proceso de desarrollo del esquema conceptual éste se prueba y se valida con los requisitos de los usuarios. El esquema conceptual es una fuente de información para el diseño lógico de la base de datos.

Actividad de Aprendizaje N° 04

Implementación del esquema interno (Nivel físico)

3. IMPLEMENTACIÓN DEL ESQUEMA INTERNO (NIVEL FÍSICO).

Es el nivel más bajo de abstracción, describe que datos son almacenados realmente en la base de datos y las relaciones que existen entre los mismos, describe la base de datos completa en términos de su estructura de diseño. El diseño físico es el proceso de producir la descripción de la implementación de la base de datos en memoria secundaria: estructuras de almacenamiento y métodos de acceso que garanticen un acceso eficiente a los datos. Entre el diseño físico y el diseño lógico hay una realimentación, ya que alguna de las decisiones que se tomen durante el diseño físico para mejorar las prestaciones, pueden afectar a la estructura del esquema lógico.

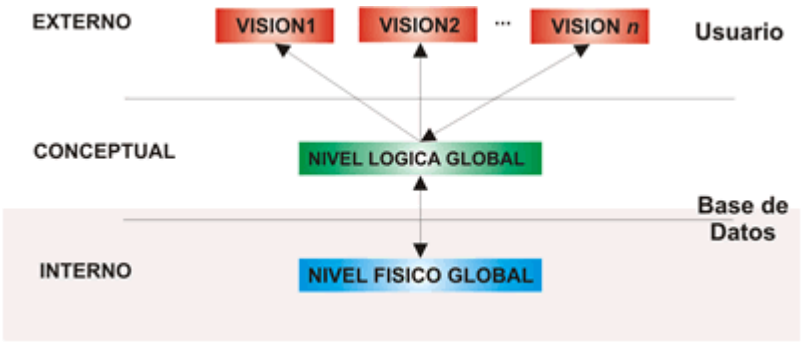


Diagrama del Esquema Físico.

El propósito del diseño físico es describir cómo se va a implementar físicamente el esquema lógico obtenido en la fase anterior. Concretamente en el modelo relacional, consiste en:

- Obtener un conjunto de relaciones (tablas) y las restricciones que se deben cumplir sobre ellas.
- Determinar las estructuras de almacenamiento y los métodos de acceso que se van a utilizar para conseguir unas prestaciones óptimas.
- Diseñar el modelo de seguridad del sistema.

En el nivel físico se debe especificar:

- Estrategias de Almacenamiento:- Asignación de espacio de almacenamiento para el conjunto de datos.
- Estrategias de Emplazamiento de los Datos:- Para optimizar los recursos a la hora de exportar la base de datos (tiempo de respuesta, disco, memoria, etc.).
- Caminos de Acceso:- Se incluye la especificación de claves como la de índices y punteros. El administrador debe especificar dispositivos de memoria, tamaño de página, número de páginas asignadas a cada área de almacenamiento, tamaño de buffer, correspondencia entre esquemas y organizaciones físicas, agrupamiento, índices, y dependiendo del SGDB podrá también definir punteros entre registros.

Ventajas:

- Aplicaciones Independientes del Nivel Interno:- Un cambio en la estrategia en los accesos a datos, no cambia el esquema conceptual.
- Transportabilidad para cambiar el SGDB a otro Entorno:- Basta rescribir la correspondencia interna/física.

- Aplicaciones Independientes del Nivel Conceptual:- Se puede modificar sin que afecte a las aplicaciones. Esto garantiza la confidencialidad de los datos.

3.1 Estructura de Datos.

Un sistema de base de datos se encuentra dividido en módulos cada uno de los cuales controla una parte de la responsabilidad total de sistema. En la mayoría de los casos, el sistema operativo proporciona únicamente los servicios más básicos y el sistema de la base de datos debe partir de esa base y controlar además el manejo correcto de los datos. Así el diseño de un sistema de base de datos debe incluir la interfaz entre el sistema de base de datos y el sistema operativo.

Los componentes funcionales de un sistema de base de datos, son:

Gestor de Archivos. Gestiona la asignación de espacio en la memoria del disco y de las estructuras de datos usadas para representar información.

Manejador de Base de Datos. Sirve de interfaz entre los datos y los programas de aplicación.

Procesador de Consultas. Traduce las proposiciones en lenguajes de consulta a instrucciones de bajo nivel. Además convierte la solicitud del usuario en una forma más eficiente.

Compilador de DDL. Convierte las proposiciones DDL en un conjunto de tablas que contienen metadatos, estas se almacenan en el diccionario de datos.

Archivo de Datos. En él se encuentran almacenados físicamente los datos de una organización.

Diccionario de Datos. Contiene la información referente a la estructura de la base de datos. Información que nos indique con claridad el tipo de datos que serán utilizados, sus ámbitos de influencia y sus limitantes de integridad.

Índices. Permiten un rápido acceso a registros que contienen valores específicos. Son estructuras, se definen para un atributo o conjunto de atributos asociados, que nos permiten simular una secuencia lógica para las entidades. La principal cualidad de un índice reside en la capacidad para acelerar el acceso a un dato específico.

Datos Estadísticos. Almacenan información estadística sobre los datos en la base de datos. El procesador de consultas usa esta información para seleccionar las formas eficientes para ejecutar una consulta.

Diseño Físico de una Base de Datos.

El diseño físico es el proceso de escoger las estructuras de almacenamiento en disco y métodos de acceso a los datos más adecuada para lograr un buen rendimiento de la base de datos. En el momento del diseño físico es importante conocer la carga de trabajo (combinación de consultas y actualizaciones) que la base de datos debe soportar y los requerimientos del usuario. Es importante también que el diseñador conozca las técnicas de procesamiento de consultas e indexación soportadas por el SGBD.

La clave de un buen diseño físico es una correcta descripción de la carga de trabajo: lista de consultas y actualizaciones, indicando sus frecuencias de operación y el resultado esperado. Para cada consulta es necesario indicar las relaciones a las que se accede, los atributos de salida y los que intervienen en filtros y condiciones. Igualmente para las actualizaciones deben

conocerse los atributos sobre los que se expresan condiciones y el tipo de actualización y la relación y atributos actualizados.
Durante el diseño físico es necesario realizar importantes decisiones:

- Que índices crear. Las consultas y actualizaciones pueden beneficiarse de la presencia de índices. Sin embargo las actualizaciones requieren de un tiempo adicional para mantener los índices sobre atributos modificados.

Aspectos para realizar cambios en el esquema conceptual:
Esquemas normalizados alternativos. En general existen diferentes alternativas para descomponer esquemas en una forma normal.
Desnormalización. Podemos reconsiderar las descomposiciones realizadas durante la normalización para la mejora de consultas aplicadas sobre atributos de varias relaciones.
Particionamiento vertical. En ocasiones puede resultar de interés dividir una relación en más relaciones para la mejora de consultas que afectan sólo a ciertos atributos.
Vistas. Añadir vistas para ocultar a los usuarios los cambios en el esquema conceptual.

3.2 Métodos de Acceso.

Organización de Ficheros.

La organización de ficheros es la forma de situar los registros cuando se almacenan en disco. La eficiencia en las operaciones de manipulación de registros depende de una correcta organización de ficheros.
Los gestores soportan diferentes técnicas de organización de ficheros y es una tarea importante del administrador de la base de datos elegir la opción en función del patrón de uso. Existen tres organizaciones básicas de archivos:

a) **Ficheros Heap.** Sus registros están colocados en forma aleatoria, este tipo de organización resulta adecuada cuando la forma de acceso más frecuente es la recuperación de todos los registro.
b) **Ficheros Ordenados.** Sus registros están ordenados según los valores de una secuencia de campos (denominada clave de búsqueda). Éste tipo resulta adecuado cuando los registros se recuperan en un cierto orden o cuando se recupera sobre un cierto rango de registro.
c) **Ficheros Hash.** El hashing consiste en convertir el valor de un campo (o conjunto de campos) en una posición dentro del archivo aplicándole una función denominada función de randomización o hash.

3.3 Herramientas.

Herramientas CASE.

Una de las herramientas para llevar a cabo el resto de tareas del modo más eficiente y efectivo posible en la primera etapa del ciclo de vida de las aplicaciones de bases de datos, es hacer uso de la herramienta CASE (Computer-Aided Software Engineering).
La tecnología CASE supone la automatización del desarrollo del software, contribuyendo a mejorar la calidad y la productividad en el desarrollo de sistemas de información.

Una herramienta CASE suele incluir:

- Un diccionario de datos para almacenar información sobre los datos de la aplicación de la base de datos.
- Herramienta de diseño para dar apoyo al análisis de datos.
- Herramientas que permitan desarrollar el modelo de datos corporativo, así como los esquemas conceptual y lógico.
- Herramientas para desarrollar los prototipos de las aplicaciones.

El uso de las herramientas CASE puede mejorar la productividad en el desarrollo de una aplicación de base de datos. Y por productividad se entiende tanto la eficiencia en el desarrollo, como la efectividad del sistema desarrollado. La eficiencia se refiere al coste, tanto en tiempo como en dinero, de desarrollar la aplicación. La efectividad se refiere al grado en que el sistema satisface las necesidades de los usuarios. Para tener una buena productividad, subir el nivel de efectividad puede ser más importante que aumentar la eficiencia.

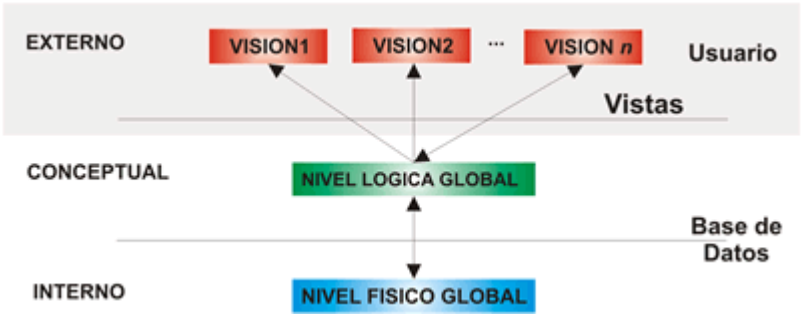
Actividad de Aprendizaje N° 05

Implementación del esquema Externo (Vistas)

4. IMPLEMENTACIONES DE LOS ESQUEMAS EXTERNOS (VISTAS)

4.1 Estructura de Datos.

Es el nivel más alto de abstracción, es lo que el usuario final puede visualizar del sistema terminado, describe sólo una parte de la base de datos al usuario acreditado para verla. El sistema puede proporcionar muchas visiones para la misma base de datos.



Esquema del nivel de Vistas.

Las **Vistas**:- Son una especie de tablas virtuales; es decir no existen físicamente sino que forman mediante la selección y/o filtrado de los componentes de otras tablas, una vista puede ser definida en base a una lista previa. Esto significa que pueden crearse dependencia entre las vistas. Cuando una vista es definida en base a otra, se dice que es dependiente de esta por lo tanto, se suprimirá automáticamente la vista dependiente si se suprime la vista original. La eliminación de una tabla provoca también la eliminación automática de todas las vistas que se hayan definido haciendo referencia a ella.

Las vistas son una forma lógica de ver los datos físicos ubicados en tablas. Cuando creamos una vista, seleccionamos un formato que incluye datos que pueden ser tomados de una o más tablas. La vista queda almacenada en forma permanente, si bien los datos grabados permanecen inalterados en las tablas correspondientes. Una vista sólo es una ventana a los datos almacenados.

Una vista es el resultado dinámico de una o varias operaciones relacionales realizadas sobre las relaciones base. Una vista es una relación virtual que se produce cuando un usuario la consulta. Al usuario le parece que la vista es una relación que existe y la puede manipular como si se tratara de una relación base, pero la vista no está almacenada físicamente. El contenido de una vista está definido como una consulta sobre una o varias relaciones base. Cualquier operación que se realice sobre la vista se traduce automáticamente a operaciones sobre las relaciones de las que se deriva. Las vistas son *dinámicas* porque los cambios que se realizan sobre las tablas base que afectan a una vista se reflejan inmediatamente sobre ella. Cuando un usuario realiza un cambio sobre la vista (no todo tipo de cambios están permitidos), este cambio se realiza sobre las relaciones de las que se deriva.

El nivel más alto de abstracción describe sólo parte de la base de datos completa. A pesar del uso de estructuras más sencillas en el nivel conceptual, permanece algo de complejidad debido al gran tamaño de

la base de datos. Muchos usuarios del sistema de bases de datos no se interesarán por toda la información. En cambio, dichos usuarios sólo necesitan una parte de la base de datos. Para simplificar su interacción con el sistema, se define el nivel de abstracción de visión. El sistema puede proporcionar muchas visiones de la misma base de datos.

La fase concluyente en el diseño de aplicaciones es la generación de las interfaces que la aplicación proporcionara para establecer comunicación con el usuario. Tradicionalmente estas interfaces han sido escritas y/o capturadas, de tal forma que el usuario revisa información desplegada en pantalla o impresa en papel y responde introducción de datos por el teclado y/o con el auxilio del ratón.

Objetivos y Ventajas de las Vistas.

El objetivo primordial de la utilización de esquemas externos es facilitar al usuario la percepción que este tiene de la base de datos así como el trabajo que van a desarrollar sobre ésta.

Las principales ventajas que se obtienen al utilizar vistas son:

- Perspectivas Directas.- Proporcionarse diversos modelos de información basados en los mismos datos, enfocándolos hacia distintos usuarios con necesidades específicas. El mostrar la información desde distintos ángulos nos ayuda a crear ambientes de trabajo y operación acordes a los objetivos de la empresa. Debe evaluarse el perfil y requerimientos de información de los usuarios destino de la vista.
- Transparencias en las Modificaciones.- El usuario final no se vera afectado por el diseño o alteraciones que se realicen en el esquema conceptual de la base de datos. Si el sistema requiere una modificación en su funcionamiento interno, podrán afectarse diversas estructuras que proveen el desempeño de este; se pretende que los usuarios finales no adviertan tales alteraciones.
- Seguridad.- Las vistas proporcionan de manera natural un medio para ocultar y proteger datos, dado que solo se presenta al usuario una selección de lo atributos existentes.

4.2 Control de Acceso.

Una vista es una forma de proporcionar al usuario un modelo personalizado de la base de datos. Aunque es imposible impedir que un usuario tenga acceso directo a una relación, puede permitírsele acceso a parte de esa relación por medio de una vista. En una vista pueden implementarse controles que restrinjan los valores de entrada ó salida al dominio válido de los atributos, mejorando así el nivel de integridad de la BD. De igual manera, el nivel de seguridad se incrementa al incluir en la vista sólo los elementos que sean considerados al alcance del usuario.

Actualmente los Sistemas Administradores de Bases de Datos (DBMS) soportan generalmente uno o ambos enfoques con respecto a la seguridad de los datos. Estos enfoques son conocidos como Control Discrecional y Control Obligatorio.

- **Control Discrecional**, un usuario específico tendrá generalmente diferentes derechos de acceso (conocidos como privilegios) sobre diferentes objetos; además, existen muy pocas limitaciones sobre que usuarios pueden tener que derechos sobre que objetos.

- **Control Obligatorio**, cada objeto de datos está etiquetado con un nivel de clasificación determinado y a cada usuario se le da un nivel de acreditación.

Las vistas utilizadas como mecanismo de seguridad, restringen el acceso de un usuario a determinadas columnas de la tabla. Si la columna excluida es la clave de la fila, también se está impidiendo que el usuario pueda relacionar dos tablas. La vista deberá ser propiedad del mismo usuario que posea objetos subyacentes.

Las vistas son útiles por varias razones:

- Proporcionan un poderoso mecanismo de seguridad, ocultando partes de la base de datos a ciertos usuarios. El usuario no sabrá que existen aquellos atributos que se han omitido al definir una vista.
- Permiten que los usuarios accedan a los datos en el formato que ellos desean o necesitan, de modo que los mismos datos pueden ser vistos con formatos distintos por distintos usuarios.
- Se puede simplificar operaciones sobre las relaciones base que son complejas. Por ejemplo, se puede definir una vista como la concatenación de dos relaciones. El usuario puede hacer restricciones y proyecc iones sobre la vista, que el SGBD traducirá en las operaciones equivalentes sobre la concatenación.

4.3 Herramientas.

La tecnología nos permite ahora establecer una comunicación más eficiente por medios auditivos, táctiles y hasta de realidad virtual. Dentro de las aplicaciones que procesan información podemos encontrar diversas alternativas mediante las que el usuario indica al sistema las acciones a realizar:

- Menús de opciones
- Secuencia preestablecida (con opción a interrumpirla)
- Comunicación con la interfase directa de comando.

Elementos Relevantes de una Vista.

Además de la información particular que la vista presenta o requiere, debe contener información referente a:

Tiempo. Deben especificarse los periodos en los que debe considerarse esta información como vigente posibles fechas de caducidad o actualización así como fechas en que se genera la información presentada.

Origen. Debe contener información precisa de las fuentes utilizadas para generar la información; de los responsables directos o indirectos de esta generación y de los medios utilizados para ello.

Destino. Se describe a los departamentos y/o personas para quienes la información es útil o valida; de igual forma, deben especificarse destinatarios indirectos o afectados por la información presentada en la vista.

Especificaciones Particulares. En casos especiales, pueden incluirse valores o datos que permitan la toma de decisiones o la aplicación de un criterio sobre la información contenida en la vista. Estos datos adicionales pueden ser utilizados para completar procesos, cálculos o delimitar áreas de acción.

Actividad de Aprendizaje N° 06

Diccionario de Datos

5. DICCIONARIO DE DATOS.

5.1 Definición.

El primer paso en el diseño de una base de datos es recolectar información acerca de la empresa, que es, acerca de su uso, relaciones y significado de datos. Como el diseño de procesos es progresivo, es necesario depositar información acerca de la opinión lógica, interna y externa del modelo en la localización central. Una herramienta que facilita el control y manejo de la información acerca de datos en el diseño, implementación, operación y expansión de fases de una base de datos es llamado **diccionario de datos.**

El diccionario de datos es un lugar dónde se deposita información acerca de datos como origen, descripción, relaciones y otros datos, es decir el diccionario de datos es una base de datos misma, la cual deposita datos acerca de los datos, el diccionario de datos es una guía y contiene "mapas guías" para la base de datos en vez de "nuevos datos", es decir es un lugar en dónde se almacena o se mantiene un conjunto de estados (controles), información relacionada con los diferentes tipos de registros (tablas) privilegios de los usuarios y estadísticas (cuantos registros tiene cada tabla, índices, etc.)

Los diccionarios de datos de los Sistemas de Base de datos (DBMS) no son iguales, aunque mantienen los mismos lineamientos o las mismas características.

En otras palabras, es un catálogo, un depósito, de los elementos en un sistema. Contiene las características lógicas de los sitios donde se almacenan los datos del sistema, incluyendo nombre, descripción, alias, contenido y organización. Identifica los procesos donde se emplean los datos y los sitios donde se necesita el acceso inmediato a la información, se desarrolla 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.

En un diccionario de datos se encuentra la lista de todos los elementos que forman parte del flujo de datos en todo el sistema. Los elementos más importantes son flujos de datos, almacenes de datos y procesos. El diccionario guarda los detalles y descripciones de todos estos elementos.

Si los analistas desean conocer cuántos caracteres abarca un determinado dato o qué otros nombres recibe en distintas partes del sistema, o dónde se utiliza, encontrarán las respuestas en un diccionario de datos desarrollado en forma apropiada.

5.2 Explotación.

Razones para la utilización de los diccionarios de datos:

1. Para manejar los detalles en sistemas muy grandes, ya que tienen enormes cantidades de datos, aun en los sistemas más chicos hay gran cantidad de datos. Los sistemas al sufrir cambios continuos, es muy difícil manejar todos los detalles. Por eso se registra la información, ya sea sobre hoja de papel o usando procesadores de texto. Los analistas mas organizados usan el diccionario de datos

automatizados diseñados específicamente para el análisis y diseño de software.

2. Para asignarle un solo significado a cada uno de los elementos y actividades del sistema. Los diccionarios de datos proporcionan asistencia para asegurar significados comunes para los elementos y actividades del sistema y registrando detalles adicionales relacionados con el flujo de datos en el sistema, de tal manera que todo pueda localizarse con rapidez.
3. Para documentar las características del sistema, incluyendo partes o componentes así como los aspectos que los distinguen. También es necesario saber bajo que circunstancias se lleva a cabo cada proceso y con que frecuencia ocurren. Produciendo una comprensión mas completa. Una vez que las características están articuladas y registradas, todos los participantes en el proyecto tendrán una fuente común de información con respecto al sistema.
4. Para facilitar el análisis de los detalles con la finalidad de evaluar las características y determinar donde efectuar cambios en el sistema. Determina si son necesarias nuevas características o si están en orden los cambios de cualquier tipo. Se abordan las características:
   - **Naturaleza de las transacciones:** las actividades de la empresa que se llevan a cabo mientras se emplea el sistema.
   - **Preguntas:** solicitudes para la recuperación o procesamiento de información para generar una respuesta específica.
   - **Archivos y bases de datos:** detalles de las transacciones y registros maestros que son de interés para la organización.
   - **Capacidad del sistema:** Habilidad del sistema para aceptar, procesar y almacenar transacciones y datos.
5. Localizar errores y omisiones en el sistema, detectan dificultades, y las presentan en un informe. Aun en los manuales, se revelan errores.

Contenido de un Registro de un Diccionario de Datos.

El diccionario tiene dos tipos de descripciones para el flujo de datos del sistema, son los elementos datos y estructura de datos.

Elementos Datos: Son los bloques básicos para todos los demás datos del sistema, por si mismos no le dan un significado suficiente al usuario. Se agrupan para formar una estructura de datos.

- Descripción: Cada entrada en el diccionario consiste de un conjunto de detalles que describen los datos utilizados o producidos por el sistema.

Cada uno esta identificado con:

- Un nombre: para distinguir un dato de otro.
- Descripción: indica lo que representa en el sistema.
- Alias: porque un dato puede recibir varios nombres, dependiendo de quien uso este dato.
- Longitud: porque es de importancia de saber la cantidad de espacio necesario para cada dato.
- Valores de los datos: porque en algunos procesos solo son permitidos valores muy específicos para los datos. Si los valores de los datos están restringidos a un intervalo especifico, esto debe estar en la entrada del diccionario.

Estructura de Datos: Es un grupo de datos que están relacionados con otros y que en conjunto describen un componente del sistema.

- Descripción: Se construyen sobre cuatro relaciones de componentes. Se pueden utilizar las siguientes combinaciones ya sea individualmente o en conjunción con alguna otra.
- Relación secuencial: Define los componentes que siempre se incluyen en una estructura de datos.
- Relación de selección: (uno u otro), define las alternativas para datos o estructuras de datos incluidos en una estructura de datos.
- Relación de iteración: (repetitiva), define la repetición de un componente.
- Relación opcional: los datos pueden o no estar incluidos, o sea, una o ninguna iteración.
- Notación: Los analistas usan símbolos especiales con la finalidad de no usar demasiada cantidad de texto para la descripción de las relaciones entre datos y mostrar con claridad las relaciones estructurales. En algunos casos se emplean términos diferentes para describir la misma entidad (alias) estos se representan con un signo igual (=) que vincula los datos.

Diccionario de Datos y las Interfases.

El diccionario de datos puede componerse básicamente de dos interfases así:

- La interfase con la gente involucrada, por ejemplo, el administrador de la base de datos, programador de sistemas, programador de aplicaciones, manejadores, y finalmente usuarios y observadores.
- La interfase con el software por ejemplo, sistema de manejo de bases de datos, librerías, sistemas operativos y generador de reportes.

El diccionario de datos puede ser usado como una herramienta efectiva para la función de administrador de base de datos en el diseño, implementación y fase de operaciones en la base de datos. Es responsabilidad del DBMS proteger el diccionario de datos por refuerzos estándar, seguridad y obligaciones privadas. Un diccionario de datos es el lugar ideal para encontrar respuestas a las preguntas como " **dónde se usa** ", " **quién usa** ", " **cuando se usa"**.

Estas interfases muestran que existen dos tipos de usos del diccionario de datos, un tipo de uso es por la gente que tiene funciones como administrador de base de datos, programador de sistemas, analista de sistemas, programador de aplicaciones, usuarios. Y el otro tipo de uso es por el software en áreas semejantes como manejadores de base de datos, sistemas, librerías, sistemas operativos y generador de reportes.

Estos dos tipos de interfase enlazan al manejador y control del medio de la base de datos como un resultado de la eficiente comunicación entre las partes involucradas.

Diccionario de Datos Ideal: Sus requerimientos y su Organización.

La siguiente es una lista de requerimientos convenientes de un diccionario de base de datos para describir los datos, no quiere decir que cualquier paquete de diccionario de datos particular abarca ahora todos estos requerimientos.

Modelo Conceptual.- la información acerca de los datos necesaria en el proceso de diseño del modelo conceptual incluye entidades, campos o

atributos y las relaciones entre campos, atributos, también incluye información acerca de cuales departamentos y usuarios están usando o intentan usar que atributos y con que frecuencia estos datos son usados, conjuntamente con las descripciones textuales y con significados y propósitos. Las entidades y relaciones deberían tener títulos apropiados, versiones, estados, los membership (campo de una entidad el cual va ha servir de referencia).

Modelo Lógico.- la información siguiente acerca del modelo lógico de la base de datos debería ser almacenada en el diccionario de datos: el campo de agrupación con su llave (estos grupos pueden ser los subgrupos de los grupos especificados en el modelo conceptual), el fundamento del modelo de datos, la relaciones de los grupos basados en el modelo de datos, el modelo externo soportado por el modelo lógico, las transacciones lógicas, los programas y los módulos, la referencia cruzada de la información entre las transacciones, también deberían ser almacenados. Otra información necesaria es el lenguaje de programación y el tipo de programa (bath o en línea) para los programas y transacciones.

Modelo Interno.- la información física acerca de los atributos como por ejemplo: longitud (caracteres), modo (cadena de caracteres, decimales, datos de simple precisión, empaquetados), justificación (derecha izquierda), formas de presentación, reglas de edición (constantes, rango de valores), derivación algorítmica, secuencia o posición secuencial que un atributo particular ocupa en una ocurrencia, seguridad (códigos de seguridad para leer, actualizar), medio de almacenamiento (tarjetas, discos, cintas, video), el control de acceso a la información debería ser almacenado en el diccionario de datos.

Un diccionario de datos ideal debería se una parte integral de todo el medio ambiente de la base de datos y el administrador de la base de datos es el responsable de la entrada al diccionario de datos, señalando que un diccionario de datos tiene que ser salvado en copias de respaldo para evitar efectos desastrosos debido a un mal funcionamiento del sistema o cualquier destrucción no intencional de la versión producida del diccionario de datos, la función del administrador de base de datos lleva la gran responsabilidad de proteger la parte vital del medio de la base de datos "el diccionario de datos".

Sistemas Ideales del Diccionario de Datos.

1. El diccionario de datos debe soportar los modelos conceptual, lógico, interno y externo.
2. El diccionario de datos debe ser integrado con el manejador del sistema de base de datos.
3. El diccionario de datos debe soportar varias versiones de documentación (historial)
4. El diccionario de datos debe apoyar la transferencia eficiente de información al manejador del sistema de base de datos. Idealmente la conexión entre los modelos interno y externo debe ser realizada en tiempo de ejecución.
5. Un diccionario de datos debería comenzar con la reorganización de versiones de producción de la base de datos como un resultado de los cambios para la descripción de la base de datos. Similarmente, cualquier cambio a la descripción de programas debe ser reflejado

automáticamente en la librería de descripción de programas con la ayuda del diccionario de datos.

6. El diccionario de datos para ser eficiente deberá ser almacenado en un medio de almacenamiento con acceso directo para la fácil recuperación de información.

Herramientas del Sistema)

6. HERRAMIENTAS DEL SISTEMA.

6.1 Afinación, Medición del Desempeño, Reorganización Física y Lógica.

Afinación.

La **afinación** se refiere a ajustes y cambios en la organización del almacén de datos después de que el sistema ha entrado en servicio y se han aclarado suficientemente las pautas de uso. Este proceso de ajuste de la base de datos se llama afinación (Tunning).

El uso de la base de datos evoluciona continuamente, a medida que más personas se van familiarizando con ella y se van creando más programas de aplicación. Los ajustes en la organización del almacén para el óptimo desempeño se convierten en un proceso continuo.

El responsable de realizar la afinación de la base de datos es el administrador de o su grupo, y es importante que este tenga libertad para introducir los cambios que sean necesarios, sin hacer estragos en los programas de aplicación.

Requisitos para una correcta afinación:

- **Independencia física de los datos.** Es la capacidad de modificar el esquema interno sin alterar el esquema conceptual, ni los programas de aplicación.
- **Medios:** Para supervisar automáticamente el uso de la base de datos con el fin de que puedan hacerse los ajustes necesarios.

Los manejadores actuales de bases de datos ya incorporan medios para la afinación automática.

Medición del Desempeño.

Es responsabilidad del DBA organizar el sistema de modo que se obtenga el desempeño que sea "mejor para la empresa", y realizar los ajustes apropiados cuando cambien los requerimientos. Es necesario reorganizar la base de datos (descargarla y volverla a cargar) en forma periódica con el fin de garantizar que los niveles de desempeño sigan siendo aceptables.

Los datos obtenidos del desempeño se comparan con aquellos datos esperados. esta razón proporciona los factores de multiprogramación, Mn, para cada uno de los procesos básicos h que son parte de los cálculos de la base de datos. En la práctica estos factores pueden variar de 1 a 0.1.

$$M_h = \frac{desempeño\ medido\ de\ h}{desempeño\ calculado\ de\ h}$$

Tales pruebas no requieren la existencia de la base de datos completa y puede ser que ni siquiera exista el estudio piloto, que consiste en la ejecución de una secuencia adecuada de operaciones aleatorias o secuenciales de lectura o escritura, junto con una cantidad equivalente del uso del cpu. Es posible escribir y ejecutar un programa que imite la operación propuesta, en el sistema real que se va a utilizar, con el costo del esfuerzo de unos cuantos días.

Reorganización Física y Lógica.

La reorganización consiste en leer el archivo en forma en que se utilizaría al realizar el procesamiento serial y escribir los registros nuevos y viejos en el archivo nuevo, dejando fuera todos los registros marcados como

eliminados lógicamente; y se crearán nuevos índices con base a los nuevos valores.

La frecuencia de reorganización depende de la actividad de inserción dentro del archivo; y se debe de realizar antes de que el archivo esté realmente lleno para evitar problemas en tiempos de mucha actividad. Las reorganizaciones físicas son necesarias para mejorar el rendimiento, añadir una nueva estructura de acceso, agilizar las operaciones de obtención y actualización, disminuir los tiempos de respuesta, minimizar el espacio de almacenamiento y optimizar el consumo de recursos. Las reorganizaciones lógicas pueden modificar el esquema conceptual, pero no alterar el esquema externo ni los programas de aplicación; puede ser un orden de visualización en las vistas.

6.2 Auditoria.

Para asegurar la calidad de la información contenida en el sistema, es necesario tener un experto que esté involucrado en el ajuste o hacer uso de un sistema que examine la información para asegurar su confiabilidad.

Existen dos tipos de auditores:

- **Internos.** Trabajan para la misma organización, dueña del sistema.
- **Externos.** Contratados del exterior de la organización que auditan el sistema para asegurar la legalidad de los estados financieros.

6.3 Respaldo y Recuperación.

El DBA debe definir y poner en práctica un plan de recuperación adecuado que incluya una descarga o vaciado periódico de la base de datos en un medio de almacenamiento de respaldo y procedimientos para volver a cargar la base de datos a partir del vaciado más reciente. El respaldo y recuperación consiste en contar con un mecanismo que permiten la fácil recuperación de los datos en caso de ocurrir fallos en el sistema de la base de datos.

El objetivo del concepto de recuperación es el de proteger la base de datos contra fallas lógicas y físicas que destruyan los datos en todo o en parte independientemente de la naturaleza de las fallas estas pueden afectar los aspectos de almacenamiento de la base de datos como son:

- Fallas que provocan la pérdida de la memoria volátil.
- Fallas que provocan la pérdida del contenido de la memoria secundaria.

En un sistema de base de datos, recuperación significa, restaurar la base de datos a un estado que se sabe que es correcto, después de una falla que provoca que se considere que el estado actual es incorrecto. Podemos tener la seguridad de que la base de datos es recuperable, si aseguramos que cualquier parte de la información que contiene, puede ser reconstruida, a partir de otra información que se encuentra almacenada redundantemente en algún lugar del sistema.

Pasos para recuperar la información:

- **Detección del error.-** El proceso de recuperación se inicia al detectar la existencia de un error. Es posible distinguir una variedad de puntos de entrada en le proceso de recuperación. Se considerarán fallas de sistemas detectadas por falta de acción del sistema o por verificaciones irrecuperables de redundancia y salida incorrecta observada por un usuario.
- **Determinación de la fuente del error.-** para decidir cual es la mejor acción correctora es necesario determinar la extensión del daño. Desde luego este esfuerzo es muy relacionado con la determinación del tiempo

y la causa del error. Después de una caída o cuando el procesamiento sea interrumpido debido a una señal de error, es necesario determinar tantos aquellas áreas del archivo de datos que sean sospechosas como cuál fue la transacción que no se concluyo.

- **Ubicación de errores secundarios.-** cuando se ha detectado un error que provocó una modificación inadecuada a un archivo un rastreo a través de las listas de actividad encontrara aquellas transacciones que emplearon el bloque correcto. Entonces es posible volver a introducir automáticamente el bloque correcto de las transacciones afectadas y producir resultados correctos. Si se actualizaron bloques mediante transacciones que leyeron bloques incorrectos antes de existir es necesario restaurar a un más el archivo.
- **Aplicación de correcciones.** Si la extensión del daño es limitada, puede utilizarse un proceso de volver a enrollar. Las porciones dañadas del archivo se restauran aplicando primero aquellas imágenes anteriores a los bloques en error reemplazando después de las transacciones incompletas. La salida proveniente de estas transacciones se suprime de ser posible, para evitar duplicar resultados que previamente se hayan enviado a los usuarios.

6.4 Migración de Datos.

Es conveniente mudar un conjunto de datos dentro del almacén de datos a posiciones accesibles de acuerdo con su actividad. En algunos sistemas se hace automáticamente, en otros, los hacen los programadores del sistema o el DBA.

El DBA se encarga de supervisar y mantener la vista lógica global de los datos. Es deseable almacenar los datos de uso frecuente de manera que resulte fácil y rápido de acceder a ellas.

Otra forma de migrar datos es cuando se migra de una versión anterior del SGBD a otra versión más actualizada (se trabaja con la versión 8i de Oracle y se desea actualizar esta versión a la 9i, por lo que se tiene que respaldar la información y migrarlo a la versión 9i de Oracle) o cuando se cambia de un manejador a otro (supongamos que actualmente se trabaja con S QL Server y se desea migrar a otro manejador como Oracle, entonces, se tiene que migrar la tablas de la base de datos de SQL a tablas de Oracle).

I Implicación de las Bases de Datos Distribuidas

7.1. Implicaciones de Bases de datos Distribuidas.

La evolución de los sistemas de información y el crecimiento no planeado de la capacidad de procesamiento del sistema en cada nodo

7.2 Seguridad y Control de Concurrencia.

La protección de los datos deberá llevarse a cabo contra fallos físicos, fallos lógicos y fallos humanos (intencionados o no). Estos fallos alteran indebidamente los datos, los corrompen con lo que la base de datos ya no puede servir a los fines para los que fue creada.

El SGBD facilita normalmente mecanismos para prevenir los fallos (subsistema de control), para detectarlos una vez que se han producido (subsistema de detección) y para corregirlos después de haber sido detectados (subsistema de recuperación).

Aspectos fundamentales de la seguridad:

- **Confidencialidad.** No desvelar datos a usuarios no autorizados. Comprende también la privacidad (protección de datos personales).
- **Accesibilidad.** La información debe estar disponible.
- **Integridad.** Permite asegurar que los datos no han sido falseados.

La seguridad en las bases de datos abarca varios temas:

- Cuestiones éticas y legales relativas al derecho a tener acceso a cierta información.
- Cuestiones de política en el nivel gubernamental, institucional o corporativo relacionadas con la información que no debe estar disponible para el público.
- Cuestiones relacionadas con el sistema.
- Necesidad en algunas organizaciones de identificar múltiples niveles de seguridad y de clasificar los datos y los usuarios según estos niveles.

El SGBD debe proveer técnicas que permitan a ciertos usuarios tener acceso a porciones selectas de una base de datos sin tener acceso al resto. Por lo regular un SGBD cuenta con un subsistema de seguridad de autorización de la base de datos que se encarga de garantizar la seguridad de porciones de la base de datos contra el acceso no autorizado.

Existen dos tipos de mecanismos de seguridad:

- Discrecionales, se usan para otorgar privilegios a los usuarios.
- Obligatorios, sirven para imponer seguridad de múltiples niveles clasificando los datos y los usuarios en varias clases de seguridad e implementando después la política de seguridad apropiada de la organización.

Otro problema de seguridad es el acceso a una base de datos estadística, la cual sirve para proporcionar información estadística a partir de diversos criterios. Los usuarios de bases de datos estadísticas están autorizados para usarlas para obtener información estadística sobre una población pero no para tener acceso a información confidencial detallada sobre individuos específicos. La seguridad en bases de datos estadísticas debe cuidar que la información sobre

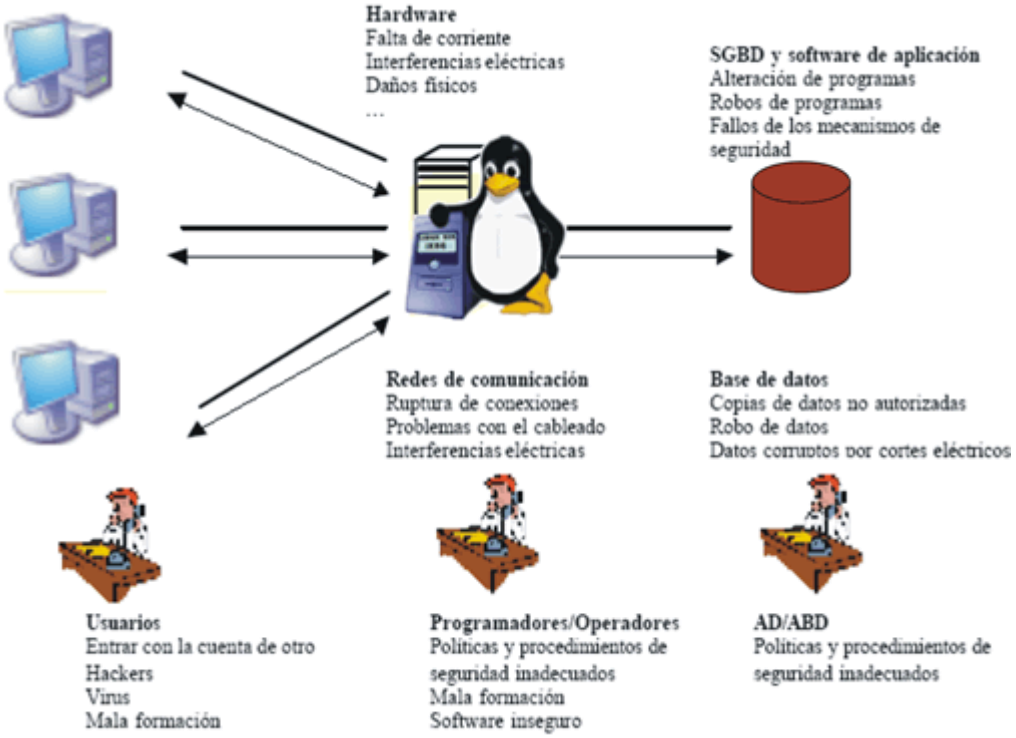
individuos no sea accesible. En ocasiones es posible deducir ciertos hechos relativos a los individuos a partir de consultas, esto tampoco debe permitirse.

Otra técnica de seguridad es el cifrado de datos que sirve para proteger datos confidenciales que se transmiten por satélite o algún tipo de red de comunicaciones. Asimismo el cifrado puede proveer protección adicional a secciones confidenciales de una base de datos. Los datos se codifican mediante algún algoritmo de codificación. Un usuario no autorizado tendrá problemas para descifrar los datos codificados, pero un usuario autorizado contará con algoritmos para descifrarlos.

Entre las obligaciones del DBA está otorgar privilegios a los usuarios y clasificar los usuarios y los datos de acuerdo con la política de la organización. Las órdenes privilegiadas del DBA incluyen los siguientes tipos de acciones:

1. Creación de cuentas
2. Concesión de privilegios.
3. Revocación de privilegios.
4. Asignación de niveles de seguridad.

La acción 1 de la lista sirve para controlar el acceso al SGBD en general, la 2 y la 3 para controlar las autorizaciones discrecionales y la 4 controla la autorización obligatoria.



Amenazas a la seguridad.

Un sistema de manejo de bases de datos confiable es aquel que puede continuar procesando las solicitudes de usuario aún cuando el sistema sobre el que opera no es confiable. En otras palabras, aun cuando los componentes de un sistema distribuido fallen, un DDMBS confiable debe seguir ejecutando las solicitudes de usuario sin violar la consistencia de la base de datos. El control de concurrencia trata con

los problemas de aislamiento y consistencia del procesamiento de transacciones.

El control de concurrencia distribuido de una DDBMS asegura que la consistencia de la base de datos se mantiene en un ambiente distribuido multiusuario. Si las transacciones son internamente consistentes, la manera más simple de lograr este objetivo es ejecutar cada transacción sola, una después de otra. Sin embargo, esto puede afectar grandemente el desempeño de un DDBMS dado que el nivel de concurrencia se reduce al mínimo. El nivel de concurrencia, el número de transacciones activas, es probablemente el parámetro más importante en sistemas distribuidos. Por lo tanto, los mecanismos de control de concurrencia buscan encontrar un balance entre el mantenimiento de la consistencia de la base de datos y el mantenimiento de un alto nivel de concurrencia.

Si no se hace un adecuado control de concurrencia, se pueden presentar dos anomalías. En primer lugar, se pueden perder actualizaciones provocando que los efectos de algunas transacciones no se reflejen en la base de datos. En segundo término, pueden presentarse recuperaciones de información inconsistentes.