



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

CATIC

Consejo Asesor en Tecnologías de
Información y Comunicación

DGTIC

Dirección General de Cómputo y de
Tecnologías de Información y Comunicación



Red Universitaria de Colaboración en
Ingeniería de Software y Bases de Datos

LINEAMIENTOS Y RECOMENDACIONES PARA LA ADMINISTRACIÓN DE BASES DE DATOS

MAYO DE 2017





LINEAMIENTOS DE ADMINISTRACIÓN DE BASES DE DATOS

Índice

LINEAMIENTOS DE ADMINISTRACIÓN DE BASES DE DATOS.....	3
I. Objetivo.....	3
II. Alcance.....	3
III. Lineamientos.....	4
A. Normativa general aplicable.....	4
B. Creación de bases de datos.....	4
C. Uso y operación de las bases de datos.....	5
D. Respaldos.....	7
E. Seguridad.....	7
F. Anexos.....	9
Solicitud de base de datos.....	9
Diccionario de Datos.....	11
Memoria de los Parámetros de configuración.....	12
G. Glosario.....	13
H. Créditos.....	17



LINEAMIENTOS DE ADMINISTRACIÓN DE BASES DE DATOS

Lineamientos y recomendaciones para la Administración de Bases de Datos

I. Objetivo

Las entidades académicas o dependencias universitarias de la UNAM tienen la necesidad de contar con diferentes bases de datos gestionadas con métodos profesionales, que les permitan brindar mejores servicios a partir de datos estructurados y consistentes, a fin de dar cumplimiento a las atribuciones y funciones que tienen encomendadas de manera alineada al Plan de Desarrollo Institucional vigente.

Estos lineamientos se presentan como guía de referencia en las tareas necesarias para la creación, uso, operación, aseguramiento, mantenimiento y administración de las bases de datos. Tienen como finalidad contribuir a que se consideren como prácticas probadas en las actividades referentes a la gestión del área.

El contenido del presente documento fue elaborado por especialistas pertenecientes a la Red de Ingeniería de Software y Base de Datos, la Dirección General de Cómputo y de Tecnologías de Información y Comunicación, así como estudiosos de otras áreas universitarias con la finalidad de dar respuesta a la solicitud del Consejo Asesor de Tecnologías de Información y Comunicación (CATIC) de la UNAM para promover la utilización de prácticas probadas, así como para homologar procedimientos en la materia al interior de la Universidad.

II. Alcance

Estos lineamientos son de uso general para todas las entidades académicas y dependencias universitarias que administran bases de datos de manera interna.

De manera complementaria, los mismos pueden ser de valor en caso de gestionar la realización y cumplimiento de estas actividades ante el escenario de un contrato con un tercero (proveedor de servicios).



LINEAMIENTOS DE ADMINISTRACIÓN DE BASES DE DATOS

III. Lineamientos

A. Normativa general aplicable

1. Toda base de datos que se genere con recursos o información de la Universidad, debe ser considerada propiedad de la UNAM, a menos que sea construida en colaboración con otras instituciones externas y que se tenga copropiedad, o que en los instrumentos legales de colaboración quede especificado lo contrario.
2. Cualquier base de datos que se cree y contenga datos personales debe observar los criterios que establece el Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, así como la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
3. Para cualquier persona u organización ajena a las entidades académicas o dependencias universitarias que tienen acceso a bases de datos de acuerdo con los permisos que hayan sido establecidos, está condicionado a:
 - a. Realizar una solicitud por escrito para su autorización por el titular de la entidad académica o dependencia administrativa de la UNAM. Únicamente se brindará el acceso, si ya se cuenta con evidencia positiva de la petición.
 - b. Que no sea información considerada reservada o confidencial.
 - c. Cuando exista una orden judicial o del Ministerio Público.
 - d. Al cumplimiento de lo establecido por el Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, la Ley General de Transparencia y Acceso a la Información Pública, así como la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
 - e. Que el tercero garantice la protección de la información indicando por escrito los métodos y recursos tecnológicos que utilizará.
4. Los datos personales contenidos en bases de datos sólo pueden ser requeridos por el titular de los mismos o salvo las excepciones contenidas en el Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, así como la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

B. Creación de bases de datos

1. Como parte del proceso de creación de la base de datos y sus objetos, se debe realizar un análisis del volumen y crecimiento de los datos, para realizar un dimensionamiento adecuado de la infraestructura, configuración y tamaño de la base de datos a crear. De la misma manera, es relevante conocer aspectos como el número de transacciones esperadas, niveles de



LINEAMIENTOS DE ADMINISTRACIÓN DE BASES DE DATOS

- conurrencia, número de usuarios potenciales, entre otros puntos que puedan favorecer la realización de un dimensionamiento correcto e informado.
2. Al momento de generar una base de datos debe definirse un responsable técnico o administrador de bases de datos y un responsable o propietario de la información contenida.
 3. Utilizar una nomenclatura estándar para las bases de datos y sus objetos, para todos los proyectos y que sea constante durante todo su diseño.
 4. Se sugiere mantener nombres cortos y descriptivos, sin utilizar espacios en blanco o caracteres especiales.
 5. Se debe confirmar la longitud máxima permitida para los nombres por el Sistema Manejador de Bases de Datos Relacional (RDBMS por sus siglas en inglés) a emplear. Se recomienda un uso máximo de 30 caracteres para el nombre de tablas o campos.
 6. Como una práctica importante, se debe cumplir que las bases de datos sean documentadas de manera formal y completa por el responsable de diseñarlas cuando son desarrolladas en la UNAM. Ver sección de anexos.
 7. Cuando se trate de una adquisición o contrato con un tercero, solicitar que el proveedor proporcione la documentación del diccionario de datos, diagrama entidad-relación y parámetros de configuración como documentación mínima a entregar.
 8. Para bases de datos diseñadas o planeadas para compartir datos de objetos digitales como audio, texto, video e imágenes con otros sistemas y bases de datos, al momento de la definición de sus campos, es importante considerar estándares internacionales de catalogación que describan a través de metadatos, la información del contenido, propiedad intelectual, entre otros (como Dublin Core o Marc21).

C. Uso y operación de las bases de datos

1. Antes de implementar una base de datos en producción es importante realizar pruebas de estrés, para saber si la base de datos va a soportar el volumen de datos y peticiones que necesitará la aplicación y en su caso hacer los ajustes necesarios. Como ejemplo de lo anterior, se debe comprobar el tiempo de ejecución de las sentencias o consultas a las bases de datos para añadir índices, modificar parámetros de configuración o modificar el tipo de procedimiento de los datos.
2. Se recomienda llevar un formato de registro de cualquier información de uso y operación de las bases de datos a nivel entidad. Toda la documentación técnica y administrativa debe actualizarse antes de que transcurran tres días como parte de la responsabilidad de parte del personal técnico, así como por compromiso con quienes pudieran requerir consultar esta información de manera consistente y vigente. El responsable técnico o administrador de bases de datos debe mantener y actualizar la documentación formalmente ante cualquier creación o modificación de algún objeto dentro de la base de datos.



LINEAMIENTOS DE ADMINISTRACIÓN DE BASES DE DATOS

3. Deben definirse y documentarse bajo criterios específicos y claros, los niveles de autorización (control de acceso) a las bases de datos de las entidades académicas o dependencias administrativas de la UNAM. Se debe partir del principio de únicamente otorgar a los usuarios los permisos requeridos (justificados) para sus fines.
4. Se recomienda de manera importante, llevar un control de los nuevos permisos de acceso que se generen, así como de la modificación del nivel de permisos de un usuario en bitácoras. Se recomienda llevar un formato específico de control de registro para esta información a nivel entidad.
5. La entidad académica o dependencia universitaria debe generar un documento donde se indiquen los niveles de servicio que puede cumplir de acuerdo con los recursos e infraestructura disponibles por cada aplicación que establezca conexiones con las bases de datos. En caso de que se requiera un nivel de servicio mayor que la capacidad disponible, esta situación debe escalarse, para definir si se autorizan recursos distintos, se adquiere algún equipo o, por ejemplo, si se comparte o se traslada el alojamiento dentro de la UNAM o con un tercero (algún proveedor en un sitio alternativo).
6. Se sugiere utilizar procedimientos almacenados y vistas para la obtención de datos, ya que aportan seguridad, encapsulamiento, facilidad de mantenimiento y rapidez. Al usar este tipo de procedimientos, el motor de base de datos revisa la sintaxis una sola vez, y no cada vez que se ejecuta la sentencia, con ello se reduce el tiempo de ejecución.
7. El administrador debe realizar actividades de monitoreo y verificación del correcto funcionamiento de la base de datos y tareas de revisión de los archivos de bitácora (logs) para comprobar que no existan problemas por atender o riesgos potenciales que puedan afectar la operación.
8. Se sugiere mantener, de manera formal y suficiente, un registro completo de los incidentes relacionados con las bases de datos que incluya: la descripción del incidente, el impacto del mismo, la forma en que se resolvió y la fecha del suceso.
9. En caso de que una base de datos se considere crítica para las actividades sustantivas de la entidad o dependencia universitaria, la persona con el rol de administrador de bases de datos en conjunto con el responsable del servicio o sistema, deben definir un plan de continuidad para recuperar y restaurar la funcionalidad parcial o total de la misma ante algún incidente.
10. Cuando una base de datos vaya a ser dada de baja (retirada) con el sistema, el responsable deberá avisar al administrador de base de datos para establecer la fecha y la realización de un respaldo total.
11. Para el retiro y conservación de la información contenida en la base de datos deberá considerarse lo establecido en la normatividad aplicable.



LINEAMIENTOS DE ADMINISTRACIÓN DE BASES DE DATOS

D. Respaldos

1. Se recomienda que los propietarios de información determinen los requerimientos para resguardar los datos en función de su criticidad. Con base en ello, se define y documenta con el Administrador de la Base de Datos, un esquema de resguardo de la información adecuado.
2. Establecer los medios de almacenamiento, el proceso, el formato para guardar los respaldos de seguridad de las bases de datos, los tipos de respaldos a realizar, la periodicidad y el formato a usar de acuerdo con las características de la base de datos y al servicio solicitado por el responsable de la información.
3. Se resalta la responsabilidad de realizar respaldos periódicamente para protección de la información. La frecuencia de los respaldos se realiza de acuerdo con las necesidades de la entidad académica o dependencia universitaria. Por ejemplo, bases de datos que tienen un nivel elevado de transacciones y que contienen información importante, necesitan respaldos más frecuentes que aquéllas que tienen pocos cambios.
4. Se recomienda efectuar un registro que sirva de control de los respaldos realizados a las bases de datos que tenga como datos mínimos: el nombre de la base de datos, tipo de respaldo realizado, medio de almacenamiento y fecha.
5. La información confidencial que no sea necesaria conservar, se debe proteger y/o destruir de acuerdo con los mecanismos determinados por la normatividad vigente y por los criterios avalados por escrito de los responsables de los datos.
6. Para fines de contar con mecanismos de confiabilidad del proceso de respaldo, se sugiere probar los procesos de respaldo y recuperación periódicamente.
7. Definir el tiempo de almacenamiento de los respaldos y documentar la forma de destrucción de aquéllos que no son útiles.
8. Realizar respaldos de las bases de datos y depositar estos en un local externo a la dependencia administrativa o entidad académica. Tener un procedimiento que detalle de manera completa, la forma en que estos respaldos se recuperarán en caso de ser necesarios.

E. Seguridad

Mantener segura la información almacenada en las bases de datos de la Universidad, es una tarea indispensable para los administradores de bases de datos, debido al impacto y valor para la comunidad universitaria. Dicha seguridad también involucra a los propietarios o responsables de la información, a los usuarios de las bases de datos y a quienes las administran, así como los técnicos encargados.

Por lo anterior, se sugiere seguir las siguientes pautas como apoyo para la prevención de pérdida de datos, accesos no autorizados y fuga de información.



LINEAMIENTOS DE ADMINISTRACIÓN DE BASES DE DATOS

1. Se sugiere que la información sea clasificada en función de su valor, requisitos legales, confidencialidad, sensibilidad y criticidad para la organización. Esta clasificación está a cargo del responsable de la información, quien debe indicar la necesidad, prioridades y grado de protección de que requiere la organización.
2. Los mecanismos de seguridad aplicables serán definidos por el responsable o propietario de la información contenida junto con el responsable técnico o administrador de bases de datos, cumpliendo con lo establecido en la normatividad universitaria y prácticas probadas de seguridad.
3. Se recomienda observar las siguientes medidas de seguridad:
 - a. Mantener actualizado un inventario de los activos de la base de datos para identificar riesgos críticos para establecer salvaguardas y responsables de su ejecución.
 - b. Quitar o inhabilitar todos los servicios que no sean necesarios.
 - c. Eliminar las cuentas que no sean necesarias.
 - d. Utilizar contraseñas seguras para las cuentas y otorgarles el mínimo de privilegios.
 - e. Aplicar regularmente las actualizaciones del software del Sistema Manejador de Bases de Datos probadas previamente.
 - f. Utilizar puertos diferentes a los que se plantean por defecto por el Sistema Manejador de Bases de Datos.
4. Se recomienda que el equipo físico que contenga una base de datos se encuentre en un lugar seguro, con cerradura y, de ser posible, en ambiente monitoreado, para prevenir el acceso no autorizado, pérdida de datos o robo. Este espacio debe mantener una temperatura adecuada para los servidores.
5. Se recomienda que siempre que sea factible, los servidores Web se almacenen en equipos distintos a los de las bases de datos.
6. Preferentemente se recomienda no iniciar sesión en los servidores con la cuenta de administración de la base de datos, sino hacerlo con cuentas individuales y después ingresar a la cuenta por medio del sistema operativo respectivo.
7. Cuando el Sistema Manejador de Bases de Datos lo permita, bloquear los usuarios de administración por defecto y cambiarlos por otros usuarios creados para fines administrativos.
8. Las cuentas de tareas administrativas deben ser cuentas individuales, es decir, que no sean compartidas por un grupo de personas.
9. Se recomienda establecer auditorías sobre datos críticos, siempre que las características del RDBMS lo permitan. Una auditoría es el proceso que permite revisar, medir y dar seguimiento del uso de la base de datos.
10. Revisar las listas de verificación de la seguridad de la base de datos y recomendaciones emitidas por el proveedor y aplicarlas.



LINEAMIENTOS DE ADMINISTRACIÓN DE BASES DE DATOS

11. Usar estas pautas para complementar las políticas de seguridad de la dependencia y/o el análisis específico que algún experto haya realizado de las necesidades de seguridad establecidas para la base de datos de acuerdo con sus características.
12. El puerto de acceso a la base de datos deberá estar restringido por firewalls o sistemas de prevención de intrusiones (IPS), permitiendo sólo el acceso a aquellos equipos que así lo requieran.

F. Anexos

Solicitud de base de datos.

El objetivo principal de elaborar solicitudes de creación de bases de datos es mantener un control y seguimiento de las mismas. Es útil para los Administradores de Bases de Datos, porque les permite identificar fácilmente las peticiones recibidas y características solicitadas, así como facilitar su mantenimiento.

Se recomienda que la solicitud incluya los datos de:

- **Sistema Manejador de Base de Datos (RDBMS) y versión.** Nombre del Sistema Manejador de Bases de Datos solicitado y la versión requerida, por ejemplo: MySQL 5.7, PostgreSQL 10, Oracle 12c, SQL Server 2016, SAP SYBASE ASE 16, entre otros.
- **Nombre de la base de datos sugerido.** Nombre que se solicita que tenga la base de datos y que se puede asignar si está disponible.
- **Valores solicitados de los parámetros de configuración diferentes a la instalación por defecto.** Nombre de los parámetros de configuración de la base de datos y el valor que se solicita que se asigne, la siguiente tabla muestra un ejemplo de una solicitud de parámetros de procesos y sesiones superiores a los valores por defecto de Oracle 11g:

Parámetro	Valor
SESSIONS	400
PROCESSES	500

- **Conjunto de caracteres e idioma solicitado:** Nombre del conjunto de caracteres (carácter set) e idioma solicitado. Por ejemplo: UTF8 Spanish Mexico.
- **Nombre(s) sugerido(s) de la(s) cuenta(s) de usuario de la base de datos:** Nombre de las cuentas de usuario de bases de datos solicitadas, se pueden asignar siempre y cuando estén disponibles y cumplan con las restricciones de nombrado de objetos de la base de datos, las cuales pueden variar de un manejador de bases de datos a otro, por ejemplo: que los nombres de usuario no sean palabras reservadas, que no inicien con caracteres numéricos, por mencionar algunos ejemplos.
- **Perfil y/o permisos que va a tener la cuenta solicitada:** Perfil que se requiere para el usuario de la base de datos, por ejemplo:



LINEAMIENTOS DE ADMINISTRACIÓN DE BASES DE DATOS

Rol: Public

Con permisos para crear índices y vistas

- **Nombre del host o direcciones IP de los equipos que van a tener acceso a la base de datos:** Listado de direcciones IP desde las cuales se puede acceder a la base de datos directamente. Incluye la dirección IP de los servidores de aplicaciones o equipos de cómputo con herramientas que usaran la información de la base de datos, se recomienda que esta lista contenga sólo las direcciones IP de los equipos que es indispensable que se conecten a la base de datos. Los equipos de usuarios que van a consultar la base de datos a través de una aplicación Web, no deben ser incluidos en esta lista, sólo la dirección IP del servidor de aplicaciones.
- **Fecha de inicio:** Fecha a partir de la cual se estima que se va a empezar a utilizar la base de datos.
- **Fecha de término:** Fecha a partir de la cual la base de datos ya no será utilizada (en caso de conocerse). Esta deberá respaldarse y eliminarse del servidor.
- **Tipo de respaldo y periodicidad solicitada:** Indicar el tipo de respaldo a realizar. Los tipos de respaldo, las herramientas para generarlo y el formato varían dependiendo del RDBMS utilizado. El ejemplo siguiente se puede aplicar para una base de datos de Oracle:

Realizar respaldo incremental diario y completo 1 vez por semana con RMAN.
Realizar respaldo en frío 1 vez al mes.

- **Datos del solicitante:** Nombre completo del solicitante, teléfono, correo electrónico, área universitaria y función. Con la finalidad de mantener los datos de contacto actualizados, para aclarar dudas o dar avisos importantes tales como: baja programada del servicio por mantenimiento, entre otros.



LINEAMIENTOS DE ADMINISTRACIÓN DE BASES DE DATOS

Diccionario de Datos.

El diccionario de datos es un documento importante para poder dar mantenimiento a la base de datos y las aplicaciones que hacen uso de la información almacenada en la misma. Debido a que describe de forma ordenada los datos almacenados en ella. A continuación se propone un formato con los datos básicos que se debe llenar por cada tabla.

Nombre de la tabla	
Descripción	

- **Nombre de la tabla:** Nombre de la tabla.
- **Descripción:** Descripción de los datos que almacenará la tabla, por ejemplo: La tabla almacenará los datos personales de los alumnos.

Nombre del campo	Tipo de Dato	Restricción de nulidad (Sí/No)	PK (Sí/No)	FK (Sí/No)	Descripción

- **Nombre del campo:** Contiene el nombre del campo o atributo en la base de datos.
- **Tipo de Dato:** Es la clasificación del tipo de dato del campo y su longitud, por ejemplo: varchar(20), integer, char(5).
- **Restricción de nulidad (Not Null Constraint):** Indicar por medio de los valores Sí o No, si el atributo es obligatorio o puede almacenar valores nulos.
- **Llave primaria (PK):** Indicar si el campo forma parte de la llave primaria o primary key.
- **Llave secundaria (FK):** Indicar si el campo forma parte de la llave foránea o foreign key.
- **Descripción:** Explicación breve de los datos que va a contener el campo y los valores por defecto (en caso de que se haya especificado alguno), por ejemplo: *Almacena el nombre del alumno.*

Los datos propuestos para el diccionario de datos no son restrictivos, pueden aumentarse de acuerdo con las necesidades de cada proyecto para que se tenga toda la información que se requiera para facilitar el trabajo de los desarrolladores, analistas, probadores, administradores de la base de datos y otros involucrados.

Además de los datos básicos mencionados anteriormente, si es posible la documentación se puede completar con los datos siguientes:



LINEAMIENTOS DE ADMINISTRACIÓN DE BASES DE DATOS

Ejemplos del dato: Esto se refiere a la indicación de cuáles son los valores que se pueden almacenar en el campo, para hacerlo más entendible, es decir, si se trata de un atributo que va a almacenar el estado civil de una persona, un ejemplo sería: “soltero”.

Nombres de los índices a los que pertenece el campo: Nombre del índice o índices que se hayan creado en la tabla y de los cuales forma parte el campo, por ejemplo: IDX_NOMBRE. Se sugiere se especifique el tipo de índice requerido.

Otro tipo de constraints o restricciones: Indicar si el atributo tiene algún otro tipo de limitante además del constraint de Not Null, por ejemplo: de tipo **CHECK** que se utiliza para controlar los valores que se pueden almacenar en el campo, por ejemplo: para un atributo que contendrá el género de una persona, los posibles valores se pueden restringir por: “M” o “F” solamente.

También se pueden agregar otro tipo de restricciones como el constraint de tipo **UNIQUE**, para que el valor almacenado en el campo sea único.

Observaciones o notas adicionales. Se puede registrar información importante para las tareas de uso, mantenimiento o desarrollo de la base de datos, por ejemplo: que se deban ingresar registros considerando una secuencia, si existe algún trigger (disparador en cumplimiento de un evento específico) que afecte los datos almacenados, si existe alguna política de respaldo y borrado de los datos almacenados en la tabla, entre otros.

Triggers y funciones. Se recomienda mantenerlos documentados, en aspectos tales como su objetivo, descripción breve de los mismos, entre otros.

Memoria de los Parámetros de configuración.

Para poder realizar el mantenimiento de bases de datos de producción, migrar a un nuevo servidor o solucionar problemas de producción, es recomendable identificar los valores de los parámetros de configuración de la base de datos que se han modificado. Es recomendable conservar un listado con el nombre del parámetro y el valor asignado, en caso de que el cambio requiera de una autorización, se puede agregar la fecha de aprobación del cambio y nombre de la persona que autoriza.

Parámetro de la base de datos	Valor anterior	Nuevo valor	Fecha de cambio

Parámetro de la base de datos: Nombre del parámetro de la base de datos.



LINEAMIENTOS DE ADMINISTRACIÓN DE BASES DE DATOS

Valor: Valor asignado al parámetro.

G. Glosario

Administrador de bases de datos. El Administrador de bases de datos (DBA) es el profesional de tecnologías de la información y la comunicación, responsable de los aspectos técnicos, tecnológicos, científicos, inteligencia de negocios y legales de bases de datos.

Base de datos. Una base o banco de datos es un conjunto de datos que pertenecen al mismo contexto almacenados sistemáticamente para su posterior uso. O bien definirla como: una colección integrada y generalizada de datos, estructurada atendiendo a las relaciones naturales de modo que suministre todos los caminos de acceso necesarios a cada unidad de datos con objeto de poder atender todas las necesidades de los diferentes usuarios.

Backup. Una copia de seguridad, copia de respaldo en Tecnologías de la Información es una copia de los datos originales que se realiza con el fin de disponer de un medio de recuperarlos en caso de su pérdida. Las copias de seguridad son útiles ante distintos eventos y usos: recuperar los sistemas informáticos y los datos de una catástrofe informática, natural o ataque; restaurar una pequeña cantidad de archivos que pueden haberse eliminado accidentalmente, corrompido, infectado por un virus informático u otras causas; guardar información histórica de forma más económica que los discos duros y además permitiendo el traslado a ubicaciones distintas de la de los datos originales.

Constraint. Los constraints o restricciones son reglas establecidas en las columnas de datos de las tablas. Son usadas para limitar los datos que se pueden almacenar en una tabla, lo que asegura exactitud y confiabilidad de los datos almacenados.

Constraint de tipo Not Null. Es una restricción que se utiliza para asegurar que un campo no pueda tener valores nulos.

Constraint de tipo Check. Asegura que los datos en una columna satisfagan ciertas condiciones especificadas en la regla de verificación de la restricción.

Dirección IP. Una dirección IP es una etiqueta numérica que identifica, de manera lógica y jerárquica, a un interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del Modelo OSI.

Firewall. Es el mecanismo encargado de proteger una red, permitiendo únicamente el tráfico autorizado de acuerdo con las políticas de seguridad establecidas.



LINEAMIENTOS DE ADMINISTRACIÓN DE BASES DE DATOS

Foreign Key. Véase llave foránea.

Índice. Son objetos de las bases de datos usados para aumentar la velocidad de acceso a los datos.

Integridad. El término **integridad** de datos se refiere a la corrección y exactitud de los datos en una base de datos.

IPS. Sistema de prevención de intrusiones, se refiere a dispositivos que ejerce el control de acceso a una red a partir de la identificación y bloqueo de patrones específicos de ataque en su tránsito por la red.

Llave foránea. En el contexto de bases de datos relacionales, una clave foránea o clave ajena (o Foreign Key FK) es una limitación referencial entre dos tablas. La clave foránea identifica una columna o grupo de columnas en una tabla (tabla hija o referendo) que se refiere a una columna o grupo de columnas en otra tabla (tabla maestra o referenciada). Las columnas en la tabla referendo deben ser la clave primaria u otra clave candidata en la tabla referenciada.

Llave primaria. En el diseño de bases de datos relacionales, se llama clave primaria a un campo o a una combinación de campos que identifica de forma única a cada fila de una tabla. Una clave primaria comprende de esta manera una columna o conjunto de columnas. No puede haber dos filas en una tabla que tengan la misma clave primaria.

Modelo OSI. El modelo de interconexión de sistemas abiertos (ISO/IEC 7498-1), también llamado OSI (en inglés, Open System Interconnection) es el modelo de red descriptivo, que fue creado por la Organización Internacional para la Estandarización (ISO) en el año 1984. Es un marco de referencia para la definición de arquitecturas en la interconexión de los sistemas de comunicaciones.

Nulo. En informática es el término usado para referirse a la ausencia de valor.

Niveles de servicio. Resultados medidos y reportados frente a uno o más Objetivos de Nivel de Servicio. El término Nivel de Servicio es a veces empleado para referirse a un Objetivo de Nivel de Servicio.

Puerto. Un puerto de red es una interfaz para comunicarse con un programa a través de una red. En el modelo OSI quien se preocupa de la administración de los puertos y los establece en el encabezado de los segmentos es la capa de transporte o capa 4, administrando así el envío y re-ensamblaje de cada segmento enviado a la red haciendo uso del puerto especificado. Un puerto suele estar numerado para de esta forma poder identificar la aplicación que lo usa. La implementación del protocolo en el destino utilizará ese número



LINEAMIENTOS DE ADMINISTRACIÓN DE BASES DE DATOS

para decidir a qué programa entregará los datos recibidos. Esta asignación de puertos permite a una máquina establecer simultáneamente diversas conexiones con máquinas distintas, ya que todos los paquetes que se reciben tienen la misma dirección, pero van dirigidos a puertos diferentes.

Primary Key. Véase llave primaria.

RDBMS. Véase Relational Database Management System.

Relational Database Management System. Un sistema manejador de bases de datos relacionales RDBMS por sus siglas en inglés, es un sistema de administración de bases de datos (DBMS) que está basado en el modelo relacional presentado por E.F. Codd del Laboratorio de Investigación de San José de IBM.

Respaldo de la base de datos. Véase Backup.

Salvaguarda. Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. (Nota: Control es también utilizado como sinónimo de salvaguarda o contramedida.

Secuencia. Una secuencia (sequence) se emplea para generar valores enteros secuenciales únicos y asignárselos a campos numéricos; se utilizan generalmente para las claves primarias de las tablas garantizando que sus valores no se repitan.

Servidor de aplicaciones. Un servidor de aplicaciones es un software que proporciona aplicaciones a los equipos o dispositivos cliente, por lo general a través de Internet y utilizando el protocolo HTTP.

Sistema Manejador de Bases de Datos. El sistema de gestión de la base de datos (SGBD) es una aplicación que permite a los usuarios definir, crear y mantener la base de datos, y proporciona acceso controlado a la misma.

El SGBD es la aplicación que interacciona con los usuarios de los programas de aplicación y la base de datos.

Trigger. Un trigger (o disparador) en una Base de datos, es un procedimiento que se ejecuta cuando se cumple una condición establecida al realizar una operación. Dependiendo de la base de datos, los triggers pueden ser de inserción (INSERT), actualización (UPDATE) o borrado (DELETE).



LINEAMIENTOS DE ADMINISTRACIÓN DE BASES DE DATOS

Algunas bases de datos pueden ejecutar triggers al crear, borrar o editar usuarios, tablas, bases de datos u otros objetos.



LINEAMIENTOS DE ADMINISTRACIÓN DE BASES DE DATOS

H. Créditos

Elaboración

Dirección General de Cómputo y de Tecnologías de Información y Comunicación

Hugo Alonso Reyes Herrera (Coordinación), Alberto González Guízar, Susana Laura Corona Correa, José Luis Chávez Sánchez.

Revisión

Red Universitaria de Ingeniería de Software y Bases de Datos

Beatriz Peralta Cortés (Instituto de Investigaciones sobre la Universidad y la Educación), Carlos Cruz Santos (Dirección General de Administración Escolar), Dante Ortiz Ancona (Dirección General de Bibliotecas), José Antonio Salazar Carmona (Instituto de Investigaciones Bibliográficas), Ana Yuri Ramírez Molina (Instituto de Investigaciones Bibliográficas).

Validación

Consejo Asesor en Tecnologías de Información y Comunicación