

UNIDAD 7. GESTIÓN DE LA SEGURIDAD DE LOS DATOS

1.- SEGURIDAD EN LAS BASES DE DATOS.

Se entiende por seguridad de los datos al conjunto de medidas que se toman para evitar el acceso indebido y robos en estos para ser tratados de manera inadecuada.

Se puede decir que la seguridad de los datos tiene tres vertientes:

- **Confidencialidad:** Garantiza que la información no sea difundida sin consentimiento. La garantía de esta circunstancia se da con un conjunto de reglas que limitan el acceso a la información.
- **Integridad:** permite que solo puedan acceder a los datos personas autorizadas. A quienes accedan a los datos se les aplicarán protocolos de autenticación, políticas internas y sistemas de control de acceso.
- **Disponibilidad:** se refiere a que la información de la base de datos está dispuesta para ser usada. Debe garantizarse su funcionamiento y confiabilidad de esta.

Para cumplir estas condiciones, hay que intentar:

- Enmascarar los datos, es decir, permitir a los usuarios ver la información que necesitan.
- Limitarse a los servicios, aplicaciones y funcionalidades realmente necesarias, y así disminuir el riesgo de acceso a cualquier información.
- Mantener actualizadas las bases de datos.
- Utilizar herramientas que permitan analizar los datos.
- Hacer frecuentemente copias de seguridad.

2.- RECUPERACIÓN DE DATOS

Se entiende por fallo del sistema gestor de bases de datos aquellas caídas que se producen en el sistema debido al mal funcionamiento del hardware o del software que afectan a las transacciones o grupo de sentencias DML que se están produciendo.

Se dice que un SGBD es eficiente si siempre es capaz de levantarse o recuperarse automáticamente cuando se ha producido un fallo.

Siempre que existe una transacción el sistema gestor tiene que ser capaz de asegurar que dicha transacción se ha realizado de manera exitosa y por tanto que ha guardado los datos en la base de manera correcta.

Los fallos se pueden producir por:

- **Caída del sistema.** Durante la ejecución de la transacción se produce un fallo de software hardware o de red punto
- **Fallo de disco.** Algunos bloques del disco pueden perder los datos por mal funcionamiento de la lectura y escritura en el disco punto esto puede producirse cuando se lee o escribe una transacción.
- **Problemas físicos y catástrofes.** Se produce cuando falta suministro de energía incendio robo o sabotaje.
- **Ataques externos y virus.** Se produce si hay entrada de un virus que no permita que las transacciones se realicen correctamente. es conveniente que tenga un antivirus seguro y actualizado.

- **Producidos por errores de diseño de la base de datos.** Si la base de datos no tiene un buen diseño, es posible que las transacciones no se realicen de forma adecuada en la misma.
- **Un error de la transacción o del sistema.** En operaciones de la transacción puede hacer que esta falle, por ejemplo, si se produce un desbordamiento.
- **Condiciones de excepción de la transacción.** Durante la ejecución de transacciones puede presentarse condiciones que requiera la cancelación de esta punto
- **Concurrencia en la transacción.** Se entiende por concurrencia cuando dos usuarios acceden a la misma transacción al unísono. Cuando ocurre esto se producen bloqueos como forma de autoprotección del sistema gestor punto los bloqueos son mecanismos que previenen conflictos entre las transacciones, que acceden a los mismos recurso, bien sea un objeto de usuario o un objeto del sistema no visible por los usuarios.

3.- COPIAS DE SEGURIDAD

Se define copia de seguridad al proceso de consiste en duplicar la información de un soporte, con el fin de poder recuperarlos en caso de fallo del primer lugar donde está alojada la información. Las copias de seguridad en las empresas son importantísimas coma pues salvaguardan el negocio.

Existen diferentes tipos de copias de seguridad coma pero los más usados son:

- **Completa.** Todos los datos se copian en sus diferentes archivos y carpetas coma es decir se hacen duplicados de todos los datos guardados. La restauración de una copia de seguridad completa es rápida. Sin embargo, cada ejecución es lenta y ocupa más espacio con respecto a las otras tipologías.
- **Incremental.** Se realiza una copia de seguridad completa, y las siguientes copias que se vayan haciendo incluirán únicamente los cambios desde la última copia de seguridad. El proceso de backup es mucho más rápido y requiere menos espacio que la copia completa.
- **Diferencial.** Se realiza una copia de seguridad de todos los cambios realizados desde la última copia de seguridad completa. Es mucho más rápida y requiere menos espacio de almacenamiento que una copia completa. Las restauraciones son más lentas que una copia de seguridad completa y más rápida que una incremental.
- **Espejo.** Guardan aquellos datos que se modifiquen en tiempo real. Es un reflejo fiel de la fuente que se está respaldando, lo que implica que un archivo eliminado en el origen, también se eliminará en la copia de seguridad. Debido a esto, este tipo de copia de seguridad debe usarse con precaución.

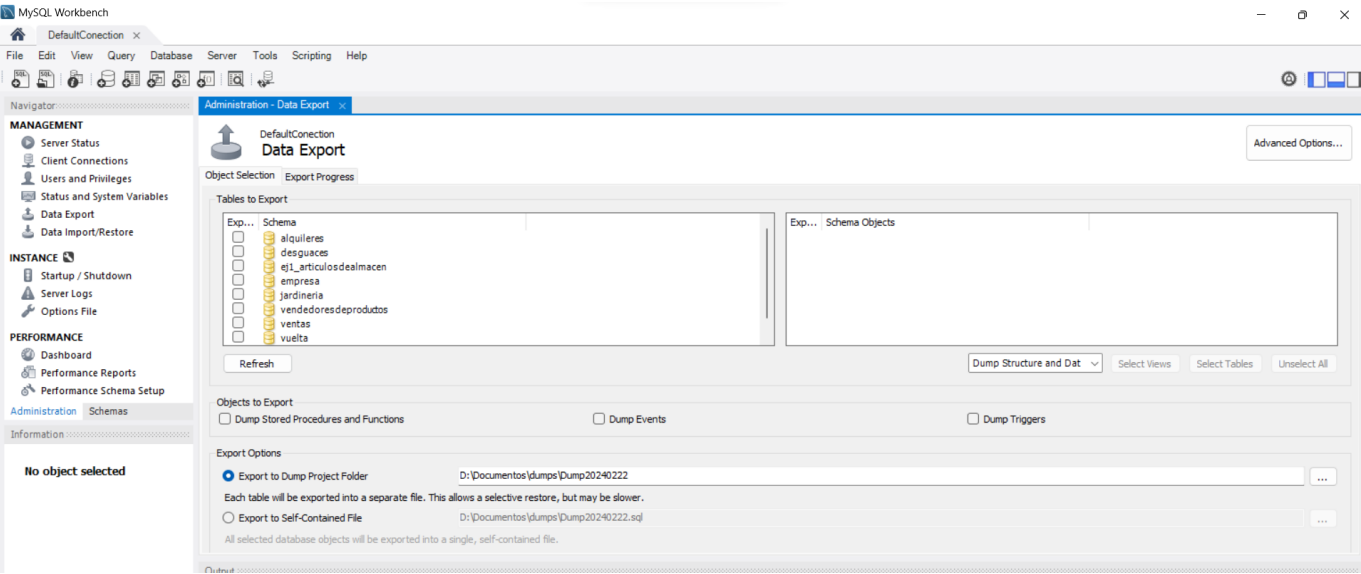
Otros autores también establecen la siguiente clasificación:

- **En frío,** esta copia de seguridad se hace parando la base de datos, evitando que los usuarios puedan conectarse cuando se esté haciendo la copia, lo que permite que se haga de manera estable.
- **En caliente,** no se detiene la base de datos, pudiendo acceder a ella a los usuarios mientras se realiza la copia de seguridad.

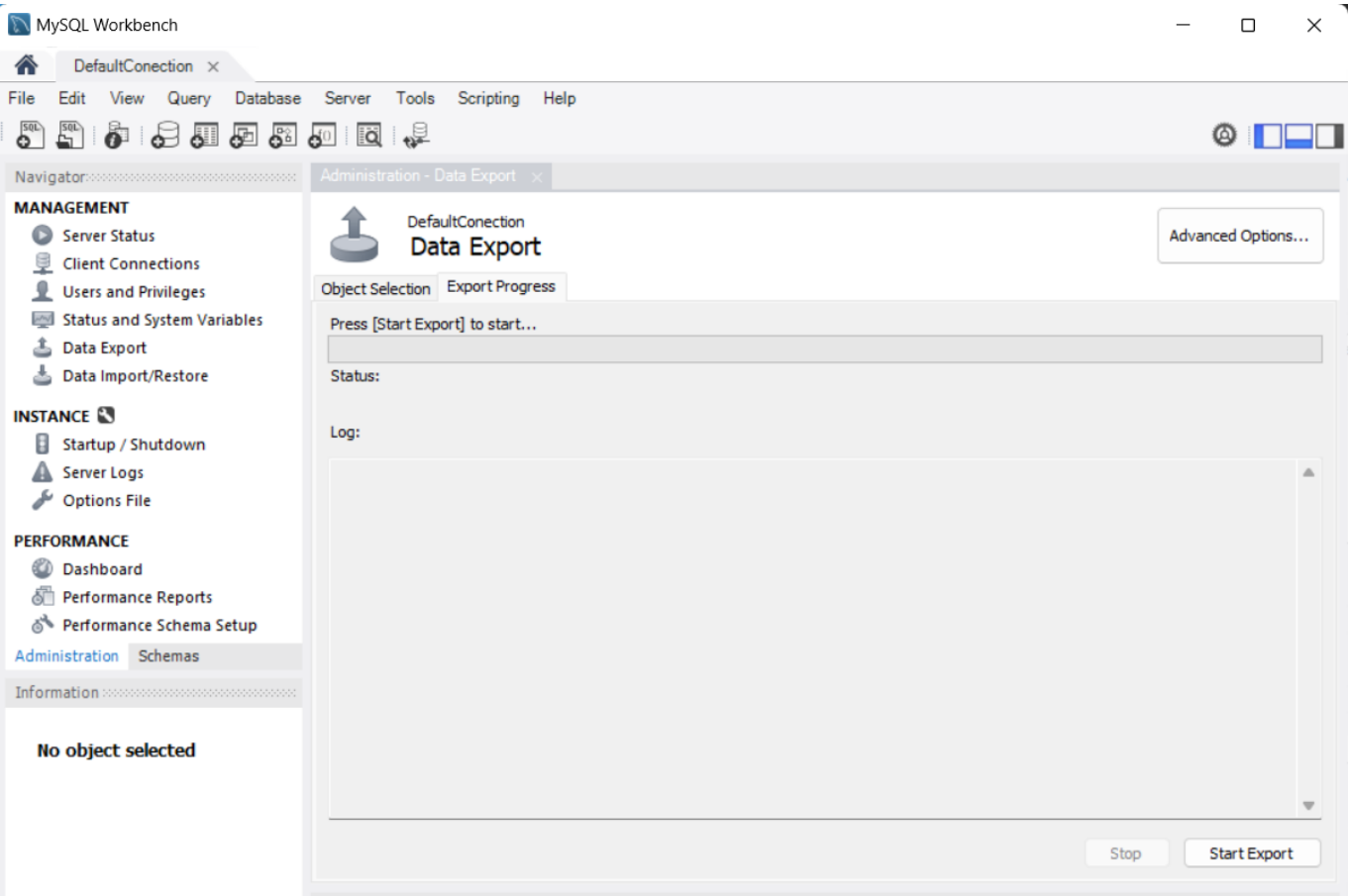
Las copias de seguridad deben de realizarse de forma periódica, pudiéndose hacer de forma diaria si es completa o una copia semanal completa y una diferencial o incremental diaria.

4.- COPIA DE SEGURIDAD EN MYSQLWORKBENCH

Para realizar una copia de seguridad en MySQL Workbench, tenemos la opción de realizarlo exportando una o varias bases de datos.



En esta pantalla se pueden elegir de que bases de datos se quiere hacer copia de seguridad, si solo se quiere guardar la estructura o los datos también, si se quiere guardar en una carpeta o en un fichero autocontenido. Una vez elegidas todas las opciones, además de la ubicación y el nombre, se pasa a la segunda pestaña para llevar a cabo la operación.



El proceso de recuperación se realiza a la inversa, con la opción de importar las bases de datos.

