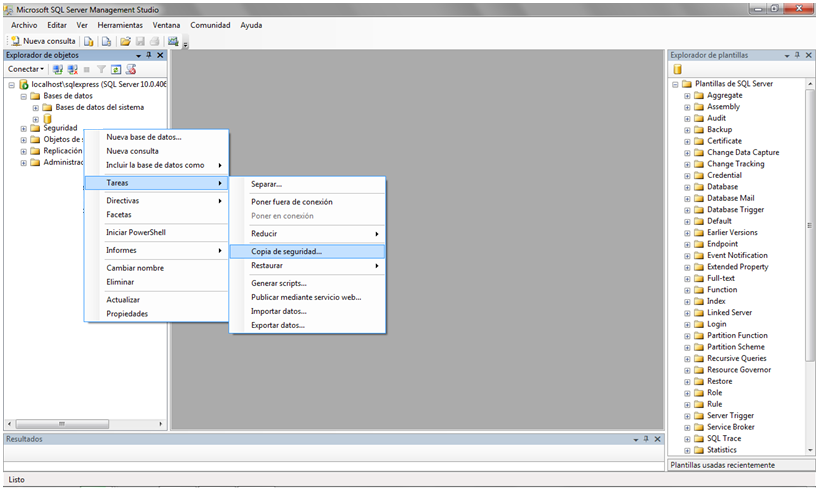
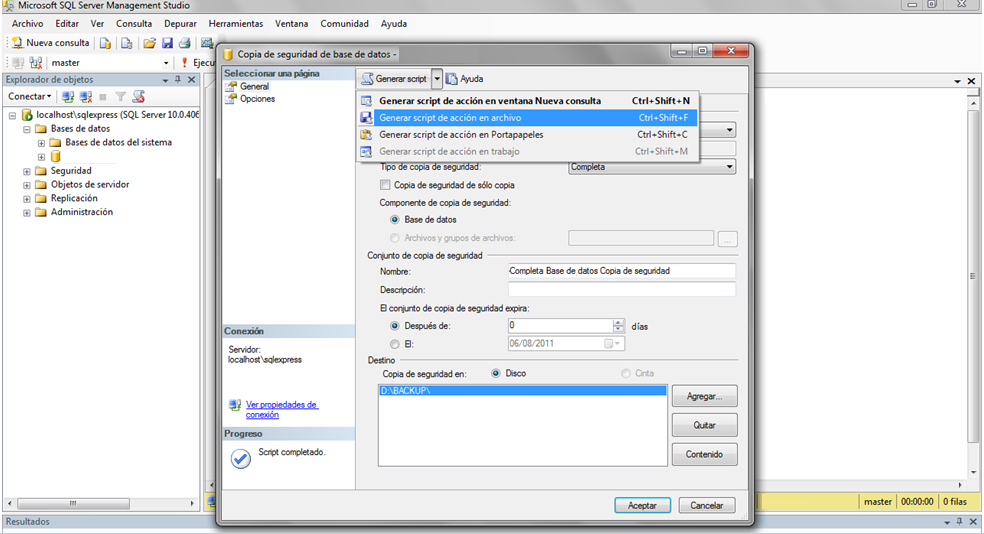
**POLÍTICA DE BACK UP**

La copia de seguridad de las bases de datos se realiza diariamente de manera automática. Para lograr esto, se siguió el siguiente procedimiento, que básicamente realiza el backup vía "script" a través de las tareas programadas de Windows:

1. Buscamos el ejecutable de "sqlcmd.exe". En nuestro caso, para SLQ Express 2008 se encuentra en: **"C:\Program Files\Microsoft SQL Server\100\Tools\Binn\sqlcmd.exe".**
2. Desde la interfaz gráfica del Management Studio, podemos seguir los pasos para realizar el backup: click derecho sobre la base de datos-> Tareas -> Copia de Seguridad.



Dentro del asistente seleccionamos la ruta donde deseamos guardar nuestro backup y las opciones que deseamos. Luego hacemos clic en el botón que nos permite generar el script, y seleccionamos la opción “Generar script de acción en ventana Nueva Consulta” y guardamos el archivo o bien seleccionamos "Generar script de acción en archivo".



Esto nos generará una salida de fichero "NombreScript.sql" del tipo:

BACKUP DATABASE **[NombreBaseDatos]** TO DISK = N'**E:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Backup\NombreBackup.bak**' WITH NOFORMAT, NOINIT, NAME = N'**NombreBaseDatos-Full Database Backup'**, SKIP, NOREWIND, NOUNLOAD, STATS = 10

GO

En nuestro caso:

**BACKUP DATABASE [SISTFLOTA] TO DISK = N'C:\Program Files\Microsoft SQL Server\MSSQL10.SQLEXPRESS\MSSQL\Backup\SISTFLOTA.bak' WITH NOFORMAT, NOINIT, NAME = N'SISTFLOTA-Completa Base de datos Copia de seguridad', SKIP, NOREWIND, NOUNLOAD, STATS = 10**

**GO**

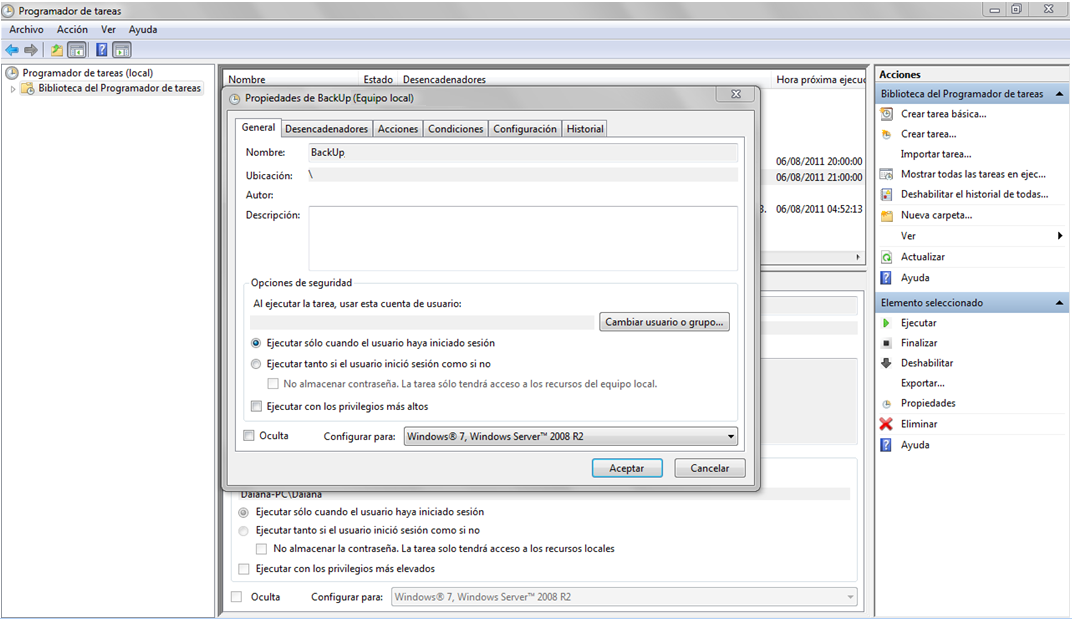
1. Creamos un archivo **.bat** que es el que vamos a programar a través de las tareas programadas de Windows. En nuestro caso, para SQL Server 2008, dentro del archivo bat colocamos el siguiente comando:

"C:\Program Files\Microsoft SQL Server\100\Tools\Binn\sqlcmd.exe" -S NOMBRESERVIDOR -i C:\Sistema\NombreScript.sql -o C:\Sistemas\Restore.log Importante mantener las comillas (") dentro de la parte inicial del comando ya que como la ruta contiene un espacio es necesario definirlo de esta manera. **NOMBRESERVIDOR** se debe reemplazar por el nombre correspondiente del servidor, **C:\Sistema\NombreScript.sql** debe ser la ruta donde se guardó el script que realiza el backup y **C:\Sistemas\Restore.log** debe ser la ruta donde se desea guardar el log de restauración.

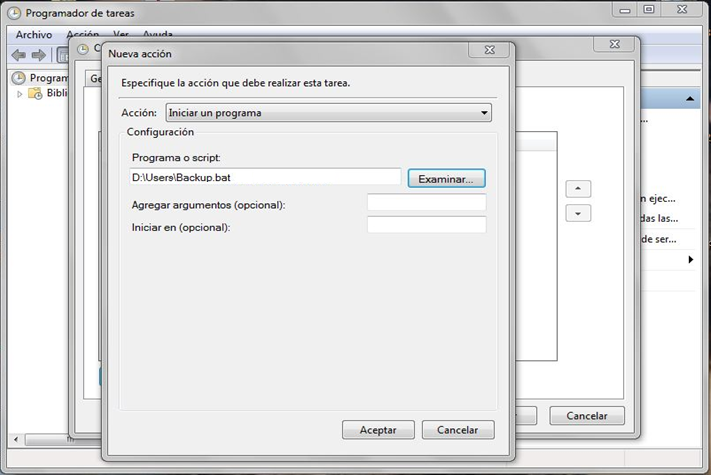
En nuestro caso, el script para la base de datos del Sistema de Flotas sería:

**"C:\Program Files\Microsoft SQL Server\100\Tools\Binn\sqlcmd.exe" -S localhost\sqlexpress -i D:\Users\guillermo.cejas\Desktop\ScriptBackUp.sql -o C:\SistFlota\Restore.log**

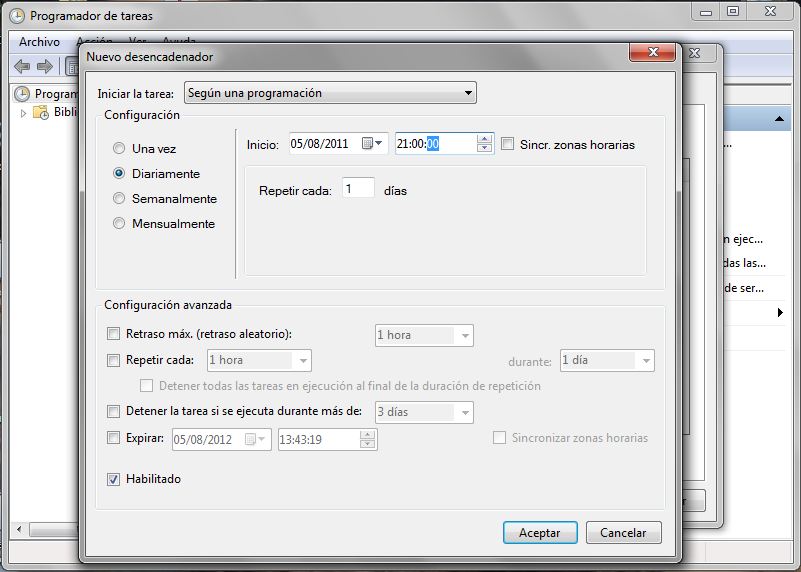
1. Por último desde el Programador de Tareas de Windows se crea una nueva tarea:



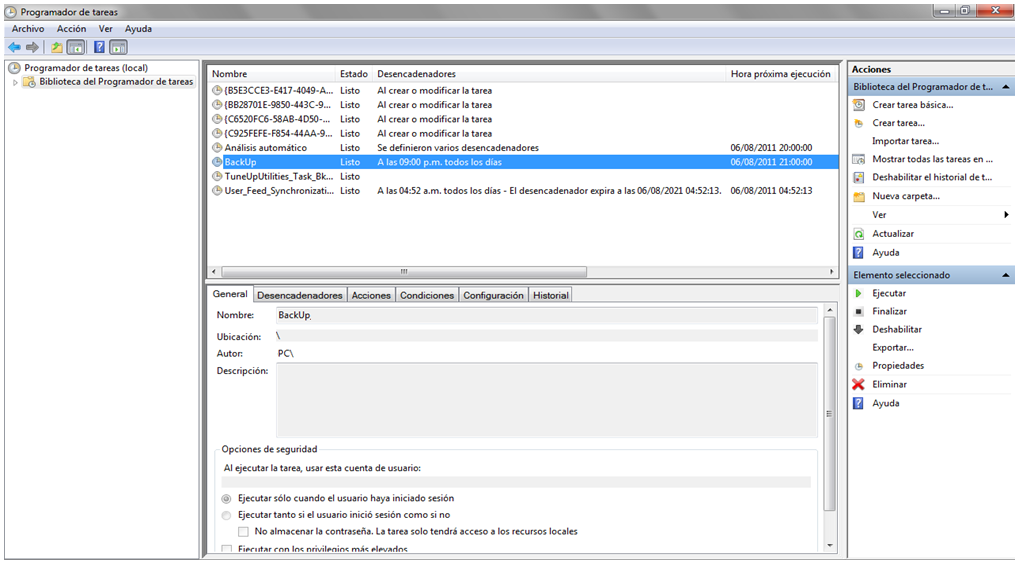
Dentro de la pestaña **“Acciones”** seleccionamos la opción **“Iniciar un programa”** y seleccionamos la ruta del .bat que creamos:



Dentro de la pestaña **“Desencadenadores”** definimos la periodicidad de la ejecución:



Finalmente podemos observar la tarea que hemos creado en la **“Lista del programador de tareas”**:



El mismo procedimiento se realizó además para la base de datos de auditoría y seguridad.

El plan de BACKUP definido realiza una copia entera de cada una. Está programado para ejecutarse diariamente a las 21:00:00 hs. Los archivos de copia de seguridad se almacenan en un disco distinto al del sistema operativo.

Adicionalmente a las copias de seguridad diarias, se realizan copias semanales: todos los viernes se copia el backup más actual en un pen drive y se almacena bajo llave.

**Procedimiento para guardar el backup en un pen drive:**

**1)** Conectar el pen drive en algún conector USB del equipo.

**2)** Abrir a la ubicación: C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Backup.

**3)** Seleccionar los archivos a copiar (archivos .bak)

**4)** Abrir la ubicación del pen drive y copiar allí los archivos seleccionados.

**5)** Realizar “Extracción segura del dispositivo” (pen drive) para evitar daños en el medio de almacenamiento.

**6)** Quitar el pen drive del conector USB.

**Backup del código fuente**

El código fuente va a estar alojado en un file hosting pago, el mismo posee transferencia encriptada de datos (SFTP o Secure File Transfer Protocol) para evitar la captura de información en la transferencia.

Además se guarda el código en un pen drive propio y almacenado físicamente bajo llave.

El pen drive estará protegido con encriptación usando **BitLocker** (sistema incluido en Windows 7 y [Windows Server 2008](http://es.wikipedia.org/wiki/Windows_Server_2008_R2) que permite cifrar las unidades extraíbles, lo cual nos garantizará la confidencialidad de los datos almacenados).

El Cifrado de unidad **BitLocker** es una característica de seguridad integral del sistema operativo Windows 7 que ayuda a proteger los datos almacenados en unidades de datos fijas y extraíbles y en la unidad del sistema operativo. BitLocker protege de "ataques sin conexión", que son aquéllos que se realizan deshabilitando o evitando el sistema operativo instalado, o bien, quitando físicamente el disco duro para atacar los datos por separado. En el caso de las unidades de datos fijas y extraíbles, BitLocker ayuda a garantizar que los usuarios pueden leer y escribir datos en la unidad solo cuando cuentan con la contraseña correspondiente, con credenciales de tarjeta inteligente o cuando usan la unidad de datos en un equipo protegido con BitLocker que tenga las claves adecuadas. Si en su organización hay equipos que ejecuten versiones anteriores de Windows, se puede usar el Lector de BitLocker To Go™ para permitir a esos equipos leer las unidades extraíbles protegidas con BitLocker.

La protección de BitLocker en unidades del sistema operativo admite la autenticación de dos factores mediante el uso del Módulo de plataforma segura (TPM) junto con un número de identificación personal (PIN) o clave de inicio, así como la autenticación de un solo factor mediante el almacenamiento de una clave en una unidad flash USB o mediante el uso solo del TPM. El uso de BitLocker con un TPM proporciona una mayor protección a los datos y ayuda a garantizar la integridad del componente de arranque inicial. Esta opción requiere que el equipo disponga de un microchip de TPM y una BIOS compatibles. Un TPM compatible se define como la versión 1.2 del TPM. Una BIOS compatible debe admitir el TPM y la raíz estática de Trust Measurement, tal y como define Trusted Computing Group.

El TPM interactúa con la protección de la unidad del sistema operativo de BitLocker para ayudar a proporcionar protección al inicio del sistema. El usuario no puede apreciar esto y el inicio de sesión de usuario no cambia. Sin embargo, si la información de inicio varía, BitLocker pasará al modo de recuperación y se necesitará una contraseña o clave de recuperación para volver a tener acceso a los datos.

Procedimiento de **BitLocker**:

1. Haga clic en **Inicio**, en **Panel de control**, en **Sistema y seguridad** y, a continuación, en **Cifrado de unidad BitLocker**.
2. Haga clic en **Activar BitLocker** para la unidad de datos fija o extraíble que desea cifrar.
3. Digitar la clave de recuperación (EJ: SistemaFlota2012\*). Cuando finalizo el proceso de guardar la clave de recuperación, haga clic en **Siguiente**.
4. El Asistente para la instalación de BitLocker le pregunta si está listo para cifrar la unidad. Haga clic en **Iniciar cifrado**.
5. Aparece la barra de estado **Cifrando**.
6. Al completar este procedimiento, habrá cifrado una unidad de datos fija o extraíble, asociado un protector de clave con un método de desbloqueo para la unidad y creado una clave de recuperación que es única para esta unidad.

Tanto el pen drive donde se almacena el backup de base de datos y el de código fuente deberán estar claramente identificados, con etiquetas que indiquen como mínimo:

a) Equipo al que pertenecen

b) Fecha y hora de ejecución

c) Frecuencia: anual, mensual, semanal, diario

d) número de secuencia o lote

e) Tipo de backup

f) Nombre del sistema o aplicativo

Todos los procedimientos de respaldo deberán generar un log en el equipo que permita la revisión del resultado de la ejecución. Los mismos se almacenarán en **“C:\SistFlota”**

Se efectuarán pruebas de recuperación de las copias de resguardo al menos una vez cada 30 días. Estas pruebas servirán para constatar que se puedan obtener correctamente los datos grabados tanto en el disco como en el pen drive al momento de ser necesarios, de forma de garantizar su propósito.

# Restauración de los archivos de Backup:

La recuperación de sistemas resulta necesaria posterior a la interrupción del Servicio. En tales circunstancias se exige una acción rápida para recuperar el estado operativo anterior a la ocurrencia del siniestro.

El responsable de realizar la restauración es el administrador del sistema, y el proceso de restauración consiste en:

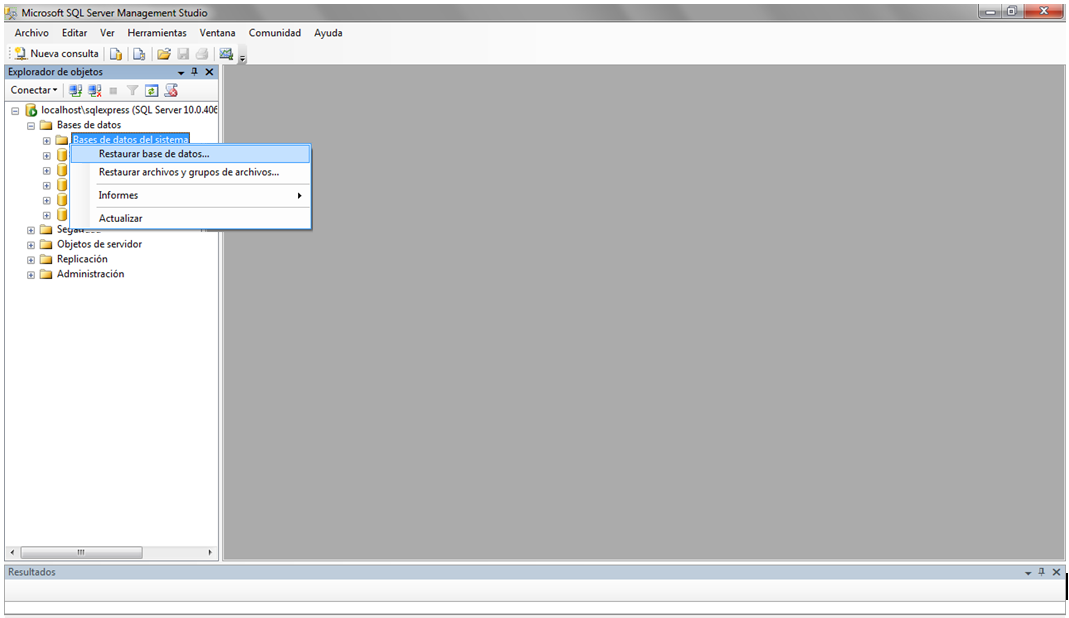
- Determinar cuál/es base/s de datos fueran afectadas

- Seleccionar el backup mas reciente.

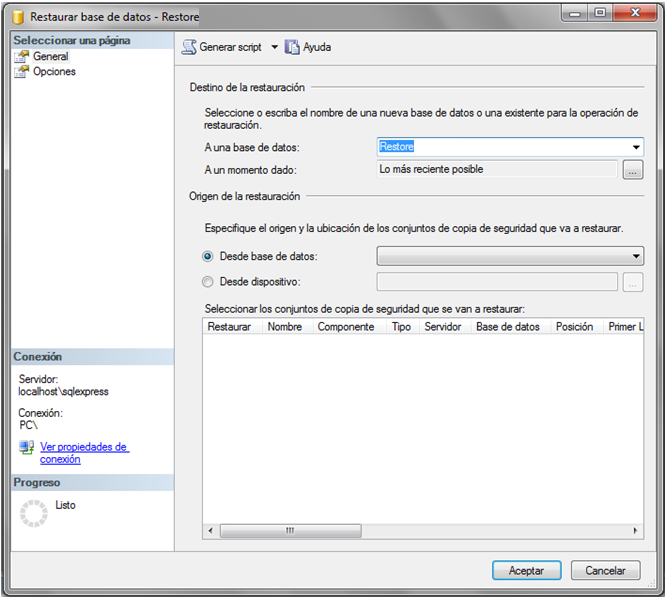
- Restaurar la/s base/s de datos.

### Restaurar una base de datos a partir de una copia de seguridad.

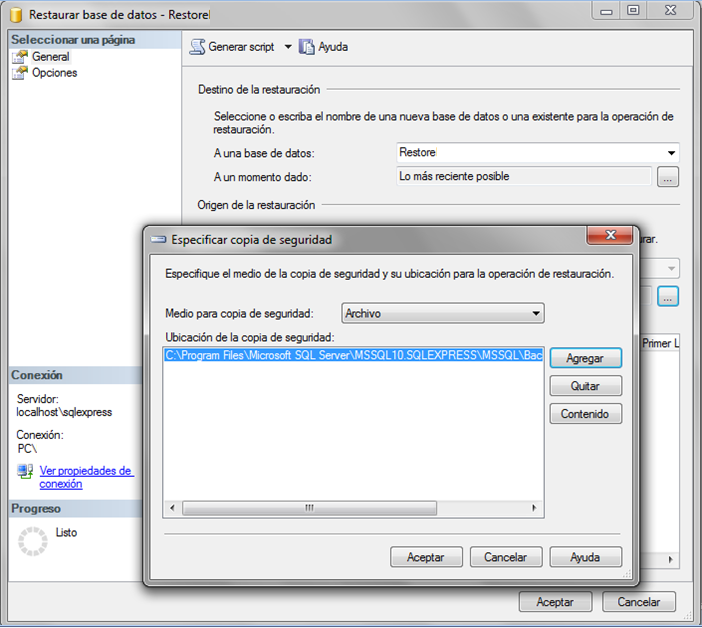
1. En el Explorador de objetos, pulsa con el botón secundario sobre la carpeta Bases de datos y del menú desplegable, selecciona “Restaurar base de datos”:



Si se va a restaurar como una nueva base de datos, se deberá escribir el nombre correspondiente en la caja de texto “**A una base de datos”**, en nuestro caso por ejemplo, la base de datos que voy a restaurar se llama **Restore**:



Antes de poder hacer la restauración de la base de datos, debemos informar dónde está guardada la copia de seguridad. Para ello marcamos la opción **Desde dispositivo** y pulsamos el botón para seleccionar el fichero de copia de seguridad de la base y luego en el botón **Agregar** para que nos muestre el cuadro de diálogo para seleccionar la copia de seguridad:



Pulsamos Aceptar y marcamos la opción “Restaurar” del cuadro de diálogo “Restaurar base de datos – Restore”.

Finalmente pulsa en el botón Aceptar y se realizará la restauración de la base de datos.