

## Capítulo 6 Mecanismo de Copias de Seguridad como Estrategia de Recuperación

### Chapter 6 Backups as a Recovery Strategy

HERNÁNDEZ-CRUZ, Luz María†\*, CAB-CHAN, José Ramón, MEX-ALVAREZ, Diana Concepción, y VICENTE, Aaron Levit

*Universidad Autónoma de Campeche, Facultad de Ingeniería*

ID 1<sup>er</sup> Autor: *Luz María, Hernández-Cruz* / **ORC ID:** 0000-0002-0469-5298, **Researcher ID Thomson:** H-3153-2018, **Arxiv Author ID:** 2234586, **CVU CONACYT-ID:** 662220

ID 1<sup>er</sup> Coautor: *José Ramón, Cab-Chan* / **ORC ID:** 0000-0003-1043-629X, **Researcher ID Thomson:** I-5425-2018, **CVU CONACYT-ID:** 204250

ID 2<sup>do</sup> Coautor: *Diana Concepción, Mex-Alvarez* / **ORC ID:** 0000-0001-9419-7868, **Researcher ID Thomson:** I-4164-2018, **CVU CONACYT-ID:** 842039

ID 3<sup>er</sup> Coautor: *Aaron Levit, Vicente* / **ORC ID:** 0000-0001-6457-4415, **Researcher ID Thomson:** I-5568-2018, **arXiv Author ID:** 2244045, **CVU CONACYT-ID:** 904855

L. Hernández, J. Cab, D. Mex y A. Vicente

lmhernan@uacam.mx

A. Marroquín, H. Corres y L. Carpio. (Dir.) *Clima Organizacional Educativo, Laboral. Handbooks*-©ECORFAN-Mexico, Queretaro, 2018.

## Resumen

El presente artículo tiene como objetivo principal analizar la generación, administración y automatización de copias de seguridad como estrategia de recuperación, permitiendo como resultado exhibir una tecnología fácil, útil y automatizada para impedir la pérdida catastrófica de información. El estudio describe paso a paso el diseño de un plan estratégico para determinar cómo, cuándo y dónde se producen, almacenan y mantienen copias de seguridad como estrategia de recuperación. La investigación se realiza con una metodología descriptiva para el análisis de un caso de estudio. Concretando, principalmente, la información que se respalda, el tipo de copia de seguridad y su frecuencia. Así mismo, se destaca que la implementación de esta tecnología se emplea dentro del propio sistema gestor de base de datos (Microsoft SQL Server 2016), sin costo económico adicional y genera valor significativo que dicho proceso puede ser automatizado en su totalidad. En definitiva, una aportación valiosa para minimizar pérdidas de información, una tecnología que ha trascendido a través del tiempo por su flexibilidad.

## Medio de recuperación, Copias de seguridad, Microsoft SQL Server 2016

### Abstract

The principal objective of this article is to analyze the generation, administration and automation of backups as a recovery strategy, allowing the display of an easy, useful and automated technology to prevent the catastrophic loss of information. The study describes step by step the design of a strategic plan to determine how, when and where backups are produced, stored and maintained as a recovery strategy. The research is carried out with a descriptive methodology for the analysis of a case study. Specifying, the information that is backed up, the type of backup and its frequency. Likewise, it is highlighted that the implementation of this technology is used within the database management system itself (Microsoft SQL Server 2016), without additional economic cost and generates significant value that the process can be automated in its entirety. A valuable contribution to minimize information losses, a technology that has transcended through time due to its flexibility.

## Recovery, Backup, Microsoft SQL Server 2016

### 1. Introducción

La necesidad principal de esta investigación surge de poder garantizar que no exista pérdida significativa de información de una base de datos. Las empresas dependen totalmente de la información almacenada en las bases de datos. Es evidente que se requiere de una estrategia que brinde la posibilidad de recuperar o restaurar una base de datos dañada o corrupta. En el mundo real existe la inminente necesidad de implantar tecnologías que permitan la recuperación de datos al momento de una falla. Todas las empresas grandes, medianas o pequeñas se enfrentan a la decisión de elegir ¿qué tecnología emplear? ¿cuánto invertir? ¿quién la administrará? ¿qué porcentaje de recuperación de datos garantiza? En este sentido, se busca soluciones económicas, que garanticen la recuperación y, además, sean fáciles de administrar. Las copias de seguridad, mejor conocidas como backup, son una estrategia tecnológica que posibilita la recuperación parcial o total de datos minimizando el riesgo de una pérdida catastrófica de los mismos y que no requieren de capacitación significativa para su administración.

El Administrador de Base de Datos (DBA) es el responsable de garantizar la integridad, disponibilidad y seguridad de la base de datos. Es por tal motivo, que requiere implementar una tecnología o herramienta para respaldar y recuperar una base de datos de forma fiable y en el mínimo de tiempo posible. Un uso fiable de manejo de copias de seguridad para la recuperación de información exige un plan estratégico para maximizar la disponibilidad de datos y minimizar la pérdida de estos, teniendo en cuenta las necesidades y características propias de la empresa.

La Hipótesis central de la presente investigación se enuncia como: “Una estrategia de copias de seguridad, podrá adoptar un enfoque de servicio y administrarse dentro del sistema gestor de base datos Microsoft SQL server 2016”.

Las copias de seguridad son una tecnología que ha trascendido a través del tiempo, el presente estudio propone un enfoque innovador que permita garantizar la calidad del proceso y la eficiencia del mismo.

Las secciones principales son:

- Marco Teórico. Contextualiza la importancia y fundamentos de las copias de seguridad.
- Metodología. Analiza y presenta la estrategia de copias de seguridad como un servicio proponiendo un procedimiento basado en el marco de buenas prácticas ITIL V3.0. Presenta de forma general, el caso de estudio, un sistema web para la administración de expedientes odontológicos "BITA". Se diseña e implementa un plan estratégico de copias de seguridad para el caso de estudio dentro del sistema gestor de base de datos Microsoft SQL server 2016 alineadas al procedimiento propuesto.

## 2. Marco Teórico

La recuperación después de una falla consiste en restaurar la base de datos a su estado correcto. Hay muchos tipos de fallas que llegan a afectar el procesamiento de una base de datos. Algunas fallas sólo afectan la memoria principal, mientras que otras involucran el almacenamiento en disco o los dispositivos de almacenamiento de respaldo. Entre las causas más comunes se encuentran las siguientes:

- Desastres físicos naturales, como incendios, inundaciones, terremotos o fallas de energía.
- Sabotaje, contaminación o destrucción intencional de los datos, hardware o software.
- Descuido, destrucción o contaminación no intencional de los datos o equipos por parte de los operadores o usuarios.
- Descomposturas de discos, como aterrizaje de cabezas, discos defectuosos o secciones ilegibles, que causan la pérdida de datos almacenados.
- Caídas del sistema debido a descomposturas del hardware, que ocasionan la pérdida de la memoria principal o cache.
- Errores del sistema de software, que originan la terminación anormal o un daño en el sistema de administración de la base de datos.
- Errores en el software de aplicaciones, como fallas de lógica en el programa que accede a la base de datos. (Ricardo, 2009).

Sin importar la causa de la falla, es necesario tomar medidas o estrategias que posibiliten la recuperación total o parcial de la información.

Cuando hablamos de implantar una tecnología o solución tecnológica, infaliblemente tenemos que considerar el proceso que se llevará a cabo para realizarlo de forma confiable y eficiente.

ITIL (IT Infrastructure Library, biblioteca de infraestructura de TI) es un Marco de referencia que describe un conjunto de mejores prácticas y recomendaciones para la administración de servicios de TI, con un enfoque de administración de procesos.

Según ITIL V3.0, Marco de buenas prácticas:

*“La copia de seguridad y restauración es esencialmente un componente del buen servicio de TI. Como tal, el diseño debe garantizar que haya una copia de seguridad sólida, las estrategias para cada servicio y la transición del servicio deben garantizar que estos sean debidamente probados.”*

*“Los datos de la organización deben estar protegidos y esto incluirá respaldo(copia) y almacenamiento de datos en ubicaciones remotas donde se puede proteger – y ser usados en caso de que necesite ser restaurado debido a pérdida, corrupción o implementación de TI en planes de continuidad del servicio.”*

Se debe acordar una estrategia general de respaldo, que abarque:

- La información que se va a respaldar, la frecuencia y los intervalos en los que se deben hacer las copias de seguridad.
- El tipo de copia de seguridad (completa, parcial, incremental) y los puntos de verificación que se utilizarán.
- Las ubicaciones que se usarán para el almacenamiento.
- Pruebas / comprobaciones a realizar, como lecturas de prueba y restauraciones de prueba.
- Objetivo del punto de recuperación. Esto describe el punto al cual los datos serán restaurados después de la recuperación.
- Objetivo de tiempo de recuperación. Esto describe el tiempo máximo permitido para recuperación después de una interrupción.
- Cómo verificar que las copias de seguridad funcionarán si es necesario restaurarlas. Los procedimientos de respaldo deben incluir un paso de verificación para garantizar que las copias de seguridad estén completas y que funcionarán si se necesita una restauración.
- Es necesario adquirir y gestionar los medios necesarios (discos, cintas, CD, etc.) que se utilizarán para copias de seguridad, para que no haya escasez de suministros.
- Cuando se utilizan dispositivos automatizados, la precarga de los medios necesarios debe ser por adelantado. Al cargar y borrar medios devueltos desde fuera del sitio almacenamiento es importante que haya un procedimiento para verificar que estos son los correctos. Esto evitará que se sobrescriba la copia de seguridad más reciente con fallas de datos, y luego no tener datos válidos para restaurar. Después de tener copias de seguridad exitosas tomadas, los medios deben ser eliminados para su almacenamiento.
- Las copias de seguridad deben ser generadas de forma automática.
- Si las copias de seguridad se automatizan o se realizan de forma remota, entonces la supervisión de eventos y capacidades deben ser consideradas para que cualquier falla pueda ser detectada de manera temprana y ser rectificadas antes de que causen problemas.
- En todos los casos, el personal de Operaciones de TI debe estar capacitado en respaldo (y restauración), los procedimientos deben estar bien documentados en las operaciones de TI de la organización (Manual de Procedimientos).

### 3. Metodología

La estrategia de copia de seguridad o backup, se ha usado y se siguen usando a través del tiempo, e incluso, a pesar de nuevas tecnologías que emergen como mecanismos de respaldo de información. En el presente documento analizaremos las copias de seguridad como un servicio, sentando las bases de un procedimiento propuesto partiendo del marco de referencia de buenas prácticas ITIL v3.0 y exhibiendo un nuevo punto de vista no explorado. Para el análisis del estudio se utiliza el proyecto BITA, cuyo contexto se describe brevemente a continuación.

La Facultad de Odontología de la Universidad Autónoma de Campeche es una dependencia de estudios de nivel superior que dispone de cinco clínicas dentro de su campus para realizar atención odontológica. La administración del proceso de atención a pacientes y el control de expedientes clínicos odontológicos se realiza mediante un sistema web denominado “BITA”, proveniente de la palabra bitácora. “BITA” es una aplicación web diseñada por estudiantes de Ingeniería en Sistemas Computacionales de la Facultad de Ingeniería desarrollada bajo un esquema de proyecto de investigación interno, lo que ha permitido enriquecer constantemente la aplicación y ser un instrumento para el estudio y aprendizaje de nuevas tecnologías.

Algunos datos relevantes que considerar son:

- Las actividades académicas y administrativas en la Facultad de Odontología son de 7:00am a 2:00pm y de 5:00pm a 8:00pm.
- El servicio de clínicas es de 9:00am a 2:00pm y de 5:00pm a 8:00pm.
- La información es crítica para el servicio, ya que, la aplicación almacena el expediente clínico odontológico digital de cada paciente.
- La autenticación se realiza con la cuenta de correo institucional.

- La información es de alto nivel crítico para el proceso de administración de prácticas en la atención a pacientes en las clínicas de la Facultad de Odontología.
- El soporte a la aplicación es responsabilidad de la Dirección General de Tecnologías de la Información (DGTI) de la Universidad Autónoma de Campeche (UAC). No se cuenta con recurso económico disponible propio para el soporte y mantenimiento de la aplicación web BITA.
- La Universidad Autónoma de Campeche cuenta con un convenio con la empresa Microsoft, haciendo de fácil acceso el licenciamiento del software con dicha empresa.

Es importante recalcar que el diseño del servicio debe facilitar la introducción del servicio en el ambiente soportado, asegurando su calidad y la satisfacción del cliente, manteniendo en todo momento un servicio rentable y que requiera mínima mejora a lo largo de su vida útil. A partir de esto, y considerando el contexto socioeconómico que envuelve la ciudad de Campeche, México donde se realiza el estudio, la estrategia de Copias de seguridad o Backup en definitiva se puede juzgar como un servicio significativo, aplicable y de fácil acceso para cualquier escuela, institución, empresa o negocio. El estudio se inicia con la aplicación de una encuesta (véase Anexo 1) realizada al personal administrativo, docente y alumnado de la Facultad de Odontología con base en la aplicación web BITA para la administración de expedientes odontológicos digitales con la finalidad de recoger información sustancial para el diseñar un procedimiento estándar como estrategia de servicio. La Tabla 6.1 muestra el resumen de los hallazgos obtenidos de las encuestas aplicadas.

**Tabla 6.1** Resumen de Hallazgos

<b>Derivado de los resultados obtenidos en las encuestas, se puede evidenciar que:</b>
– La información sensible se encuentra 100% identificable.
– El total de los encuestados comprende el concepto de copias de seguridad.
– No existe un proceso interno establecido de respaldo de información o generación de copias de seguridad.
– No existe personal del área de sistemas computacionales en la escuela. El soporte es administrado por la Dirección General de Tecnologías de la Información. Se cuenta con un servidor interno propio para el manejo de la información sensible al proceso analizado.
– El tráfico de transacciones ocurre dentro de horarios de clase del alumnado.
– La información crítica dispuesta a perder es en período máximo de una semana.
– El análisis de la información se realiza por parcial y semestre durante el ciclo escolar activo.
– El fin de ciclo escolar es un punto crítico para el archivo de la información como histórica del ciclo escolar activo.
– No existe personal experto en el área de base de datos.

Fuente: Fuente Propia

Antes de aplicar el mecanismo de copias de seguridad en el caso de estudio, se define un procedimiento alineado a los fundamentos de servicios de ITIL v3.0 descritos en el Marco Teórico. La Tabla 6.2 muestra el Procedimiento propuesto para la implementación de Copias de Seguridad o Backups.

**Tabla 6.2** Procedimiento propuesto para la implementación de Copias de Seguridad alineado a ITIL v3.0

<b>Secuencia de actividades definidas para el Procedimiento de Implementación de una Estrategia de Copias de Seguridad o Backups</b>
1. Inicio
2. Identificar la base de datos o la información sensible.
3. Identificar y documentar la Infraestructura de TI que aloja la base de datos o la información sensible.
4. Analizar y documentar el rendimiento y cargas de datos por períodos cortos, medios y largos de tiempo.
5. Diseñar el plan estratégico de Copias de seguridad alineados a la información documentada previamente.
5.1. Definir software o herramienta para la realización de copia de seguridad.
5.2. Definir tipo de copia de seguridad a realizar.
5.3. Definir calendario de realización de la copia de seguridad.
5.4. Realizar copia de seguridad.
5.5. Validar y verificar el archivo de copia de seguridad generado.
5.6. Elegir el medio de respaldo y realizar la copia de seguridad.
5.7. Etiquetar el medio de respaldo de la copia de seguridad generada.
5.8. Documentar la copia de seguridad generada en la Bitácora de respaldo.
6. Fin

Fuente: Fuente Propia

### 3.1. Diseño del Plan Estratégico del caso de estudio

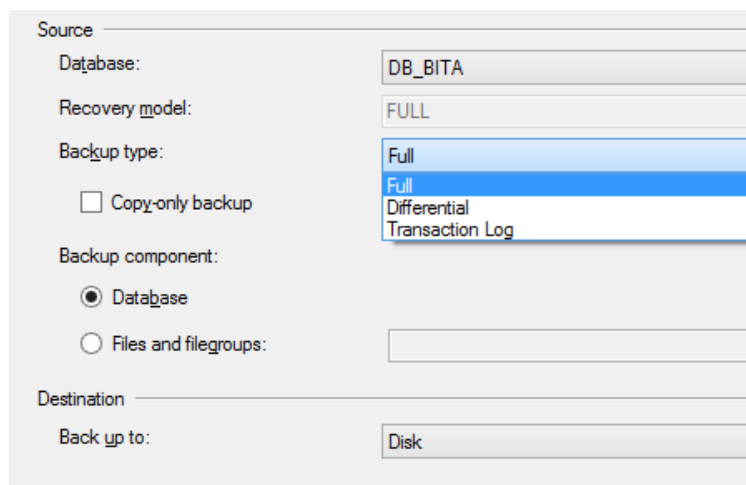
Enseguida, usando el procedimiento propuesto y considerando la información recolectada se analiza el caso de estudio BITA utilizando el sistema gestor de base de datos Microsoft SQL Server 2016. Según el sitio oficial de Microsoft diseñar una estrategia de copia de seguridad y restauración eficaz requiere mucho cuidado en el planeamiento, la implementación y las pruebas. Es forzoso realizar pruebas. No tendrá una estrategia de copia de seguridad hasta que haya restaurado correctamente las copias de seguridad en todas las combinaciones incluidas en su estrategia de restauración. Debe tener en cuenta varios factores. Entre ellas, destacan:

- Los objetivos de producción de la organización para las bases de datos, especialmente los requisitos de disponibilidad y protección de datos frente a pérdidas.
- La naturaleza de cada una de las bases de datos: el tamaño, los patrones de uso, la naturaleza del contenido, entre otros.
- Restricciones de los recursos, como hardware, personal, espacio para almacenar los medios de copia de seguridad y seguridad física de los medios almacenados.

Cuando se decide implantar un mecanismo de respaldo usando copias de seguridad es necesario diseñar un plan estratégico que sustente el proceso, conteniendo desde la generación de las copias de seguridad hasta la restauración en caso de ser necesario. Al hablar de un plan estratégico de copias de seguridad se incluye el tipo, la frecuencia y los medios de comunicación donde se van a crear y almacenar las copias de seguridad. También, se define el responsable de la restauración de la copia de seguridad y el procedimiento para la restauración de la base de datos usando los archivos de copia guardados. Una pregunta común es ¿Cómo empezar una estrategia de copia de seguridad? la estrategia de copia de seguridad debe cumplir el objetivo de punto de recuperación (RPO) y el objetivo de tiempo de recuperación (RTO). Es imprescindible contestar las preguntas ¿Cuándo generar copias de seguridad? ¿Qué tipo de copia de seguridad? y ¿Dónde y cómo almacenar las copias de seguridad?

Microsoft SQL Server 2016 permite manejar tres tipos de Copias de Seguridad: Full, Diferential y Transaccion Log. La Figura 6.1 muestra los tipos de Copias de Seguridad en Microsoft SQL Server 2016.

**Figura 6.1** Tipos de Copias de Seguridad en Microsoft SQL Server 2016



Fuente: Fuente Propia

Las copias de seguridad completa (Full) permiten crear una copia de toda la base de datos, incluyendo objetos, usuarios y configuraciones. A medida que la base de datos aumenta de tamaño, las copias de seguridad completas requieren una mayor cantidad de tiempo para generarse y mayor espacio de almacenamiento. Por ello, para una base de datos grande, es más conveniente usar una serie de copias de seguridad diferenciales.

Una copia de seguridad diferencial (Differential) sólo contiene los datos que se han cambiado o agregado desde la última copia de seguridad completa. De tal manera, las copias de seguridad diferenciales son acumulativas y sucesivas hasta que se vuelva a generar una copia de seguridad completa.

En Microsoft SQL Server en cada 4 GB de sección de cada archivo de datos existe una página de base de datos especial denominada *mapa de bits diferencial* que realiza el seguimiento de las partes (denominadas extensiones) en la cual se han cambiado datos desde la última copia de seguridad completa. Una copia de seguridad diferencial examina estos mapas de bits y realiza una sola copia de seguridad de los datos de las extensiones de archivo que están marcadas como modificados. Todo plan estratégico de copias de seguridad implica generar copias de seguridad completas y frecuentemente copias de seguridad diferenciales.

Rob y Coronel mencionan que un Sistema Manejador de Base de Datos (DBMS) utiliza un registro de transacciones para dar seguimiento a todas las transacciones que actualizan la base de datos. Mientras que el DBMS ejecuta transacciones que modifican la base de datos, también actualiza automáticamente el registro de transacciones. El registro de transacciones guarda:

- Un registro de inicio de la transacción.
- Por cada componente de transacción (sentencia de SQL) guarda:
  - El tipo de operación que se está realizando (actualización, eliminación, inserción).
  - Los nombres de los objetos afectados por la transacción (el nombre de la tabla).
  - Los valores “antes” y “después” de los campos que se están actualizando.
  - Señalizadores a los ingresos de registro de transacción previo y siguiente para la misma transacción.
- La finalización (COMMIT) de la transacción.

A pesar, que guardar el registro de transacciones en el DBMS aumenta el trabajo de procesamiento, la capacidad de restaurar una base de datos corrupta hasta el momento previo a la falla bien vale la pena. Una copia de seguridad del registro de transacciones contiene todos los registros de transacciones generados desde la última copia de seguridad del registro (o copia de seguridad completa que inicia una cadena de copia de seguridad del registro) y se utiliza para permitir que la base de datos pueda recuperarse en un punto específico en el tiempo (normalmente el tiempo en el cual se produce la falla). Las copias de seguridad de registro de transacciones son incrementales, es decir, si se desea restaurar la base de datos a un punto determinado en el tiempo, se necesitan todas las transacciones de entradas del registro para reproducir los cambios en la base de datos hasta dicho punto en el tiempo.

Estos se incluyen en la cadena de copia de seguridad del registro. Una cadena de copia de seguridad del registro es una serie continua de copias de seguridad del registro que contienen todos los registros de transacción necesarios para recuperar una base de datos a un punto en el tiempo. Una cadena comienza con una copia de seguridad completa de la base de datos y continúa hasta que algo interrumpe la cadena, evitando más registro de copias hasta que se toma otra copia de seguridad completa (o diferencial).

Después de analizar toda la información recopilada del caso de estudio y de la tecnología dentro del sistema gestor de base de datos Microsoft SQL Server 2016 se diseña un plan específico para el caso de estudio presentado. La Tabla 6.3 muestra el Plan Estratégico de Copias de Seguridad para el caso de estudio DB\_BITA.

**Tabla 6.3** Plan Estratégico de Copias de Seguridad para el caso de estudio App BITA

Tipo de Copia de Seguridad	Lunes	Viernes	Sábado	Domingo
Completa				Cada fin de ciclo escolar 23:59hrs Cada fin de año 23:59hrs
Diferencial	Cada primer lunes de mes 6:00hrs		Cada inicio y fin de parcial 6:00hrs	
Transacción		Semanal 23:59hrs		

Fuente: Fuente Propia

Usando el asistente para la creación de copias de seguridad de Microsoft SQL Server, se implementa el plan estratégico diseñado previamente (véase Anexos). Una vez obtenidos los archivos correspondientes, se verifica su consistencia con la sentencia VERIFYONLY.

**Figura 6.2** Sentencias para Verificar la Integridad de los archivos de Copias de Seguridad generados

```
RESTORE VERIFYONLY
FROM DISK = 'C:\Program Files\Microsoft SQL
Server\MSSQL13.SERVIDOR\MSSQL\Backup\DB_BITA
.bak'
```

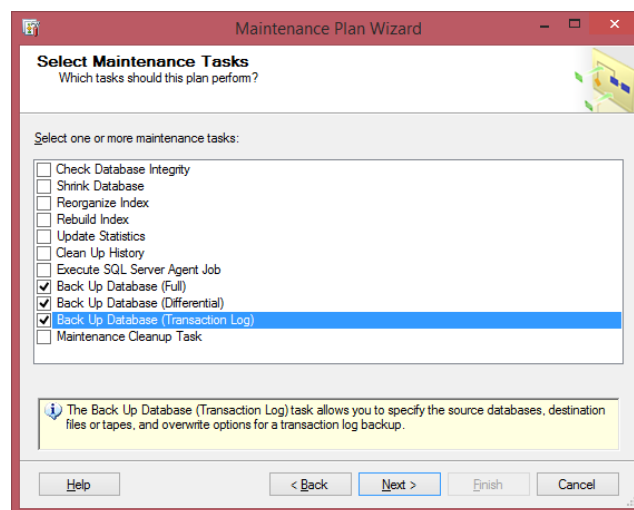
Fuente: Fuente Propia

En esta prueba, todos los archivos generados tuvieron a bien un resultado válido de análisis. Sin embargo, por no ser suficiente para asegurar la consistencia de los datos y la recuperación de la base de datos, se realiza otro escenario de prueba usando CHECKSUM, este comando se asegurará que SQL Server puede leer los contenidos de la copia de seguridad realizando una suma de comprobación cuando lee una página de datos, cuyos cálculos se almacenan en el archivo de copia. La Figura 2 muestra las instrucciones en lenguaje SQL-Transact que permiten asegurar la consistencia del archivo de copia de seguridad generado usando el comando CHECKSUM. Como resultado se obtiene que el conjunto de copia de seguridad de cada archivo de copia de seguridad es válido.

Hasta este punto, se ha podido generar y verificar correctamente los archivos de copias de seguridad generados como parte del plan estratégico de copias de seguridad diseñado como mecanismo de recuperación dentro del sistema gestor Microsoft SQL Server 2016.

Por otro lado, es de suma importancia, poder *automatizar* el proceso, esto para facilitar la administración de la base de datos y evitar pérdida de tiempo en la supervisión y mantenimiento del proceso. Microsoft SQL Server 2016 en sus versiones Enterprise y Estándar contienen la herramienta Planes de mantenimiento (Maintenance Plans) para la automatización de procesos. Mediante el manejo del Asistente para crear planes de mantenimiento (Maintenance Plans Wizard) se puede determinar qué tareas se realizarán de forma automática (véase Figura 6.3).

**Figura 6.3** Plan de Mantenimiento en Microsoft SQL Server 2016



Fuente: Fuente Propia

En este caso de estudio, la generación de copias de seguridad y la comprobación de los archivos generados. Se crea un plan de mantenimiento que permita automatizar el plan estratégico de copias de seguridad diseñado para el caso de estudio. Otro plan de mantenimiento permite comprobar la integridad de la base de datos del caso de estudio BITA de forma automática.



#### 4. Resultados

En definitiva, la estrategia de Copias de Seguridad son un Servicio, éste provee al usuario la capacidad de respaldar información y tenerla disponible para la recuperación de la misma ante una pérdida. El Marco de buenas prácticas ITIL en su última versión, en definitiva, son una excelente oportunidad para administrar esta estrategia, brindándole un valor agregado a su utilización.

Por otro lado, también podemos enlistar las siguientes fortalezas del sistema gestor de bases de datos Microsoft SQL Server 2016:

- Cuenta con un Asistente gráfico que guía al usuario en la creación de los archivos de respaldo y para la restauración de la información.
- Es de fácil manejo, no es necesario ser un especialista.
- Las herramientas de copias de seguridad y restauración están disponibles en todas las versiones del sistema gestor, incluyendo las gratuitas.
- Permite la utilización de Planes de Mantenimiento para la automatización de la generación de copias de seguridad.
- Posibilita la verificación de integridad de los archivos de copia de seguridad generados.
- Permite elegir el lugar de almacenamiento de los archivos de copias de seguridad.

Por último, la Tabla 6.4 presenta una lista de cotejo comparando las actividades del procedimiento propuesto que se fueron realizadas en el caso de estudio BITA.

**Tabla 6.4** Lista de Cotejo de Análisis de Resultados

<b>Actividades definidas para el Procedimiento de Implementación de una Estrategia de Copias de Seguridad o Backups según ITIL v3.0</b>		<b>Cumple</b>
1.	Identificar la base de datos o la información sensible.	1. Sí
2.	Identificar y documentar la Infraestructura de TI que aloja la base de datos o la información sensible.	2. No
3.	Analizar y documentar el rendimiento y cargas de datos por períodos cortos, medios y largos de tiempo.	3. No
4.	Diseñar el plan estratégico de Copias de seguridad alineados a la información documentada previamente.	4. Sí
5.	Definir software o herramienta para la realización de copia de seguridad.	5. Sí
6.	Definir tipo de copia de seguridad a realizar.	6. Sí
7.	Definir calendario de realización de la copia de seguridad.	7. Sí
8.	Realizar copia de seguridad.	8. Sí
9.	Validar y verificar el archivo de copia de seguridad generado.	9. Sí
10.	Elegir medio de respaldo y realizar la copia de seguridad.	10. Sí
11.	Etiquetar el medio de respaldo de la copia de seguridad generada.	11. No
12.	Documentar la copia de seguridad generada en la Bitácora de respaldo.	12. No

Fuente: Fuente Propia

Sin lugar a duda, se tiene como resultado que el procedimiento propuesto es aplicable para implantar estrategias de Copias de Seguridad como un servicio alineados al Marco de buenas prácticas ITIL v3.0. Después de evidenciar el mecanismo de copias de seguridad como una estrategia de recuperación es oportuno resaltar que su implementación no está limitada al uso del sistema gestor de base de datos Microsoft SQL Server, mismo que solo se utiliza en este documento como una herramienta de software disponible y viable para el caso de estudio. Sin embargo, cualquier sistema de gestión de bases de datos proporciona una forma eficiente de realizar copias de respaldo de la información y suministra herramientas para la verificación y automatización de estas.

Las herramientas tecnológicas disponibles que permiten llevar a cabo las actividades propuestas en la Tabla 6.2. Procedimiento de Implementación de una Estrategia de Copias de Seguridad quedarán a criterio y evaluación del administrador de la base de datos dependiendo del contexto de que se trate. En este ámbito, una oportunidad de estudios futuros puede ser, precisamente, la comparación del manejo de diferentes herramientas tecnológicas en el procedimiento aquí propuesto.

## 5. Anexos

### Anexo 1 Encuesta



1. ¿Identifica la información crítica manejada por la escuela?
2. ¿Qué periodo máximo de tiempo considera crítico que afecte la pérdida de información a) diario b) semanal c) mensual d) semestral?
3. Marque los periodos críticos de información relevante
  - a) inicio de ciclo escolar
  - b) primer parcial
  - c) segundo parcial
  - d) exámenes finales
  - e) exámenes extraordinarios
  - f) fin de ciclo escolar
4. ¿La escuela tiene un área de Cómputo responsable de la información crítica?
5. ¿Conoce el concepto de Backup o Copias de seguridad?
6. ¿Según su experiencia, las copias de seguridad son una estrategia eficiente para el respaldo de información?
7. ¿Considera que la recuperación del uso de los sistemas informáticos es crítica en la escuela?
8. ¿Si existe una falla en los sistemas informáticos, son restablecidos en un periodo máximo de 24hrs?
9. ¿Se utiliza la estrategia de copias de seguridad o respaldo para asegurar la recuperación de la información ante una falla?
10. ¿Existe o conoce de la existencia de un procedimiento institucional o documental establecido para realizar copias de seguridad o respaldo de información en la escuela?
11. ¿El proceso de copias de seguridad o respaldo se realiza obedeciendo a un cronograma o plan estratégico establecido?
12. ¿La escuela tiene personal con alguna certificación, especialidad, maestría y/o doctorado en el área de base de datos?

Datos relevantes que desee comentar: \_\_\_\_\_

Fuente: Fuente Propia

## 6. Agradecimiento

Un agradecimiento al apoyo otorgado por la Universidad Autónoma de Campeche, al director de la Facultad de Odontología, M. en C. Juan Ricardo Oliva Luna y al director de la Facultad de Ingeniería, M.C.C. Guadalupe Manuel Estrada Segovia. Asi mismo, se reconocer la dedicación y participación a los alumnos que formaron parte del equipo de trabajo para la implementación de la aplicación web BITA.

## 7. Conclusiones

En el presente artículo se ha expuesto un mecanismo de respaldo considerando la importancia de la información. Las diversas situaciones que ponen en riesgo la consistencia y disponibilidad de los datos es justificación suficiente para considerar herramientas o mecanismos para prevenir pérdidas ante cualquier falla o daño en una base de datos. Mendiante el empleo de un caso de estudio se ilustra cómo implementar un plan estratégico de copias de seguridad. Particularmente, se detallan y resaltan las diferentes alternativas que se pueden utilizar en las copias de seguridad como estrategia de recuperación. No cabe duda, el futuro próximo los sistemas gestores de bases de datos, Microsoft SQL Server inclusive, proporcionarán diversas estrategias de respaldo y recuperación. Por tanto, es importante analizar y elegir los mecanismos y herramientas que se adapten a las necesidades propias de cada empresa. Existe un amplio campo de investigación en el área de respaldo y recuperación, no sólo con diferentes tecnologías, sino también con diferentes sistemas gestores de bases de datos usando de información no incluidos en el alcance del presente.

## 8. Referencias

Catherine M. Ricardo. (2004). conceptos del base de datos. En Base de Datos (666). Mc Graw Hill.

Dusan Petrovic. (2008). A BEGINNERS GUIDE. Germany: Mc Graw Hill.

Carlos Coronel, Steven Morris, Peter Rob. (2011). Base de Datos. CENGAGE LEARNING.

Microsoft. (2012). Backup and restore of SQL Server Database. Microsoft.

VÍCTOR JOSÉ VERGEL RODRÍGUEZ. (2008). Administración de base de datos con SQL Server. Europa: Excelente Innova

MARIA PEREZ MARQUEZ. (2016). Motor de base de datos y Administracion. Madrid España: Libros RC

STACIA VARGA, DENNY CHERRY, JOSEPH D'ANTONI. (2016). Introducing Microsoft SQL Server 2016. Redmond, Washington: Microsoft Press A division of Microsoft Corporation.

JOSEPH D'ANTONI. (2016). Introducing Microsoft SQL Server 2016. Redmond, Washington: Microsoft Press A division of Microsoft Corporation

ANDY OPPEL, ROBERT SHELDON. (2006). Fundamentos de SQL Server. Mc Graw Hill.  
Ross Mistry, Stacia Misner. (2012). introduccion a SQL Server 2012. Waypoint Press.

LARSON, B. Microsoft SQL Server 2016 reporting services (5th ed., p. 15). Mexico: Mc Graw Hill Education.