Auditoría SQL Server

Fecha: 20/08/2022

F-SPN-031

Auditoría SQL Server

Índice de contenido

Auditoría SQL Server

Objetivo:

Conocer las ventajas de utilizar las auditorías de SQL Server y explicar el proceso para activarlas en el servidor de base de datos.

Auditoría SQL Server

1. **Ventajas:**

   Las auditorías de SQL Server le permiten a las empresas llevar un registro y seguimiento de los eventos que se producen sobre la estructura y sobre la data almacenada en las bases de datos.

   Es muy importante procurar monitorear permanentemente las bases de datos para poder saber, dada una eventualidad o no, quien tuvo acceso a los datos y el momento preciso del evento.

Auditoría SQL Server

2. Creación de auditorías en SQL Server:

Las auditorías de SQL Server se componen de dos elementos:

2.1.Objeto de Auditoría (SQL Server Audit).

2.2.Especificación de la auditoría.

Auditoría SQL Server

2.1.Objeto de Auditoría (SQL Server Audit).

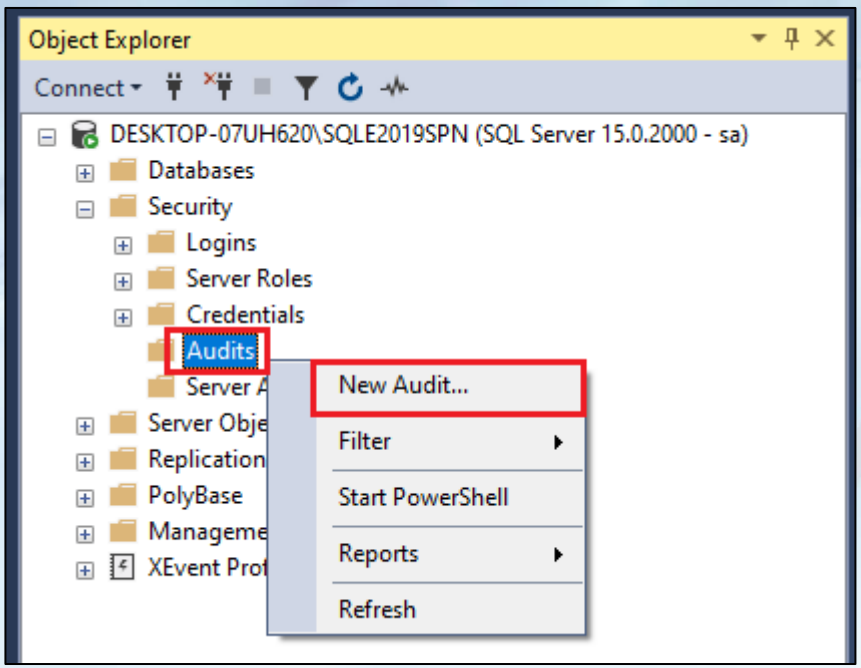
Es el elemento principal en las auditorías y es donde se especifica la configuración que va a tener el archivo físico donde se almacenan las auditorías.

Pasos para la creación de Auditoría (SQL Audit):

a) En el **Explorador de objetos de Microsoft SQL Management Studio**, expanda la carpeta **Seguridad**.
b) Haga clic con el botón derecho en la carpeta **Auditorías** y, después, seleccione **Nueva auditoría...**

Auditoría SQL Server

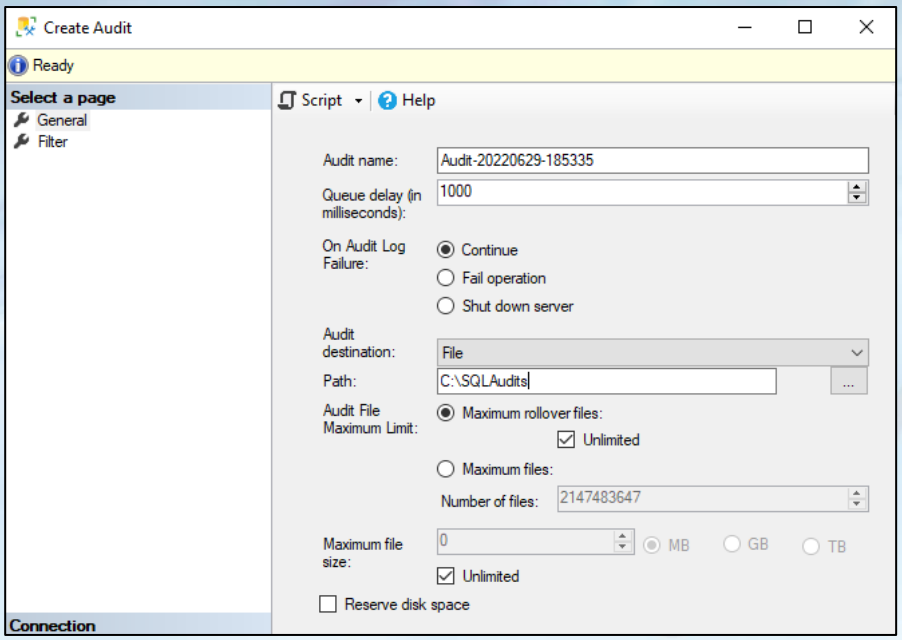
2.1.Objeto de Auditoría (SQL Server Audit).



Se abre la pantalla ***Crear auditoría*** con las siguientes opciones:

Auditoría SQL Server

2.1.Objeto de Auditoría (SQL Server Audit).



c) Nombre de auditoría.

d) Retardo de cola (en milisegundos):

Indica la cantidad de tiempo, en milisegundos, que puede transcurrir antes de exigir que se procesen las acciones de auditoría.

Auditoría SQL Server

2.1. Objeto de Auditoría (SQL Server Audit).

e) **Si hay un error de registro de auditoría:**
Continuar, Apagar el servidor o Error en la operación.

f) **Destino de auditoría:**
Especifica el destino de los datos de la auditoría.

g. **Ruta de acceso del archivo.**

h. **Límite máximo del archivo de auditoría.**

i. **Ilimitado:**
Permite un número ilimitado de archivos de auditoría.

j. **Número de archivos.**

k. **Tamaño máximo del archivo.**

l. **Reservar espacio en disco.**

Auditoría SQL Server

2.2.Especificación de la auditoría.

Permite recopilar las acciones que se desean auditar. Este objeto recoge los eventos ocurridos en la base de datos y los envía al **SQL Server Audit** que tenga asociado (*ver el punto 2.1*).

Estas especificaciones se pueden configurar tanto a nivel de instancia o servidor (permite auditar varias bases) o a nivel de base de datos (cuando solo se quiere auditar una sola base de datos).

Las especificaciones de auditoría se componen por los grupos de acciones o las acciones que ocurren en la base de datos y que se quieren auditar.

Auditoría SQL Server

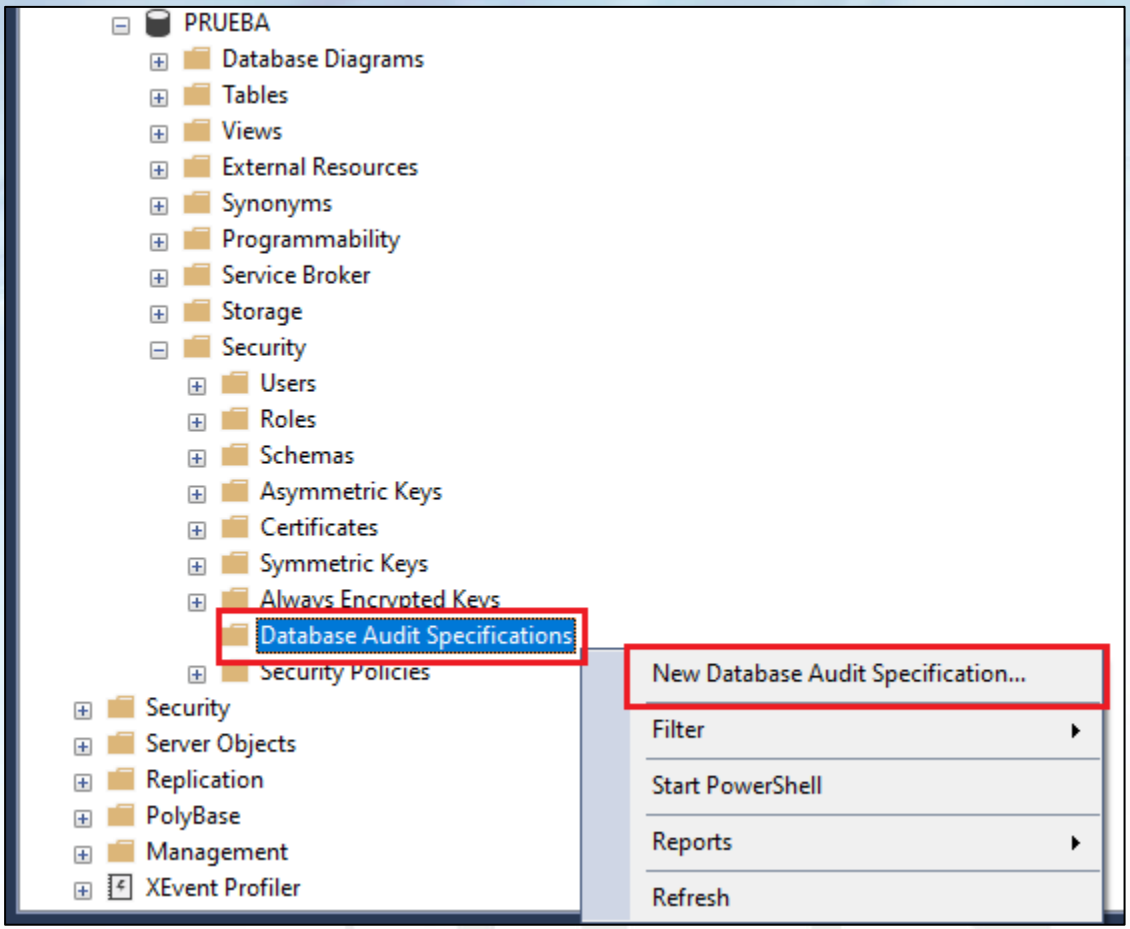
2.2.Especificación de la auditoría.

Pasos para la creación de la especificación de auditoría de nivel de base de datos:

a) En el **Explorador de objetos** de **Microsoft SQL Management Studio**, expanda la base de datos donde quiera crear la especificación de auditoría.
b) Expanda la carpeta **Seguridad**.
c) Haga clic con el botón derecho en la carpeta **Especificaciones de auditoría de base de datos** y seleccione **Nueva especificación de auditoría de base de datos...**

Auditoría SQL Server

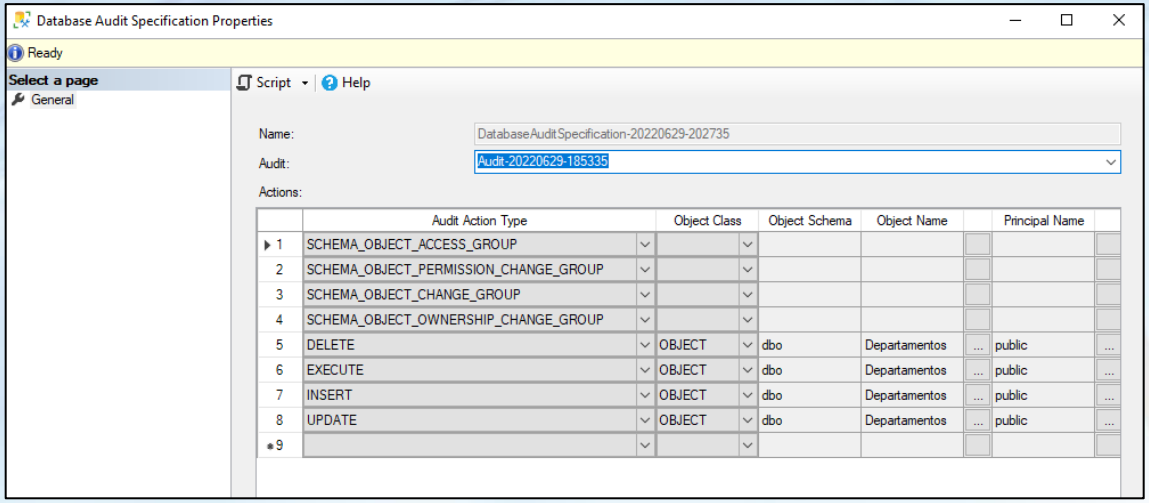
2.2.Especificación de la auditoría.



Auditoría SQL Server

2.2.Especificación de la auditoría.

Se abre la pantalla ***Crear especificación de auditoría de base de datos*** con las siguientes opciones:



d) Nombre de la especificación.

e) Auditoría:

Aquí seleccionamos el nombre de la Auditoría SQL (*objeto SQL Audit*) creada anteriormente.

Auditoría SQL Server

2.2. Especificación de la auditoría.

f) Tipo de acción de auditoría:

Especifica los *grupos de acciones de auditoría* y las *acciones de auditoría* en el nivel de base de datos que se desea capturar.

Para obtener la lista de grupos de acciones de auditoría y de acciones de auditoría de nivel de base de datos, favor consultar:

Grupos de acciones y acciones de SQL Server Audit

NOTA**: Para auditar las operaciones **CREATE**, **ALTER** o **DROP** en el esquema, se debe seleccionar el tipo de acción: ***SCHEMA_OBJECT_CHANGE_GROUP.

Auditoría SQL Server

2.2. Especificación de la auditoría.

g) Nombre de objeto:

Nombre del objeto que se va a auditar. Esta opción solo está disponible para las acciones de auditoría. No se aplica a los grupos de auditoría.

h) Nombre de la entidad:

La cuenta por la que se va filtrar la auditoría para el objeto que se va a auditar.

i) Clic en **Aceptar** para guardar los cambios**.**

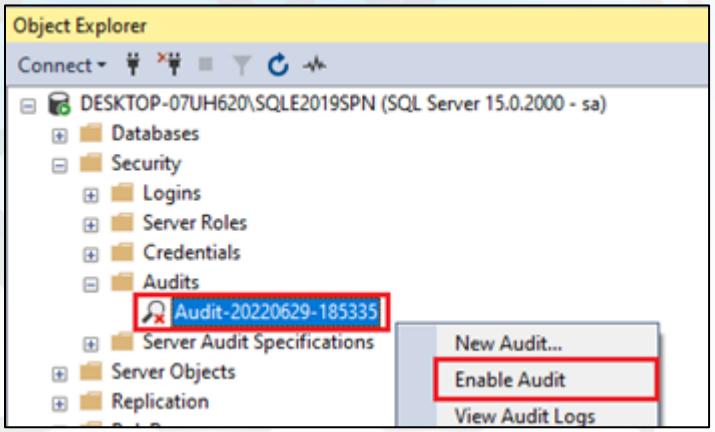
Auditoría SQL Server

3. Activación de auditoría y de la especificación de auditoría de base de datos:

Luego de configuradas las auditorías, se deben habilitar:

3.1. Habilitar las Auditorías.

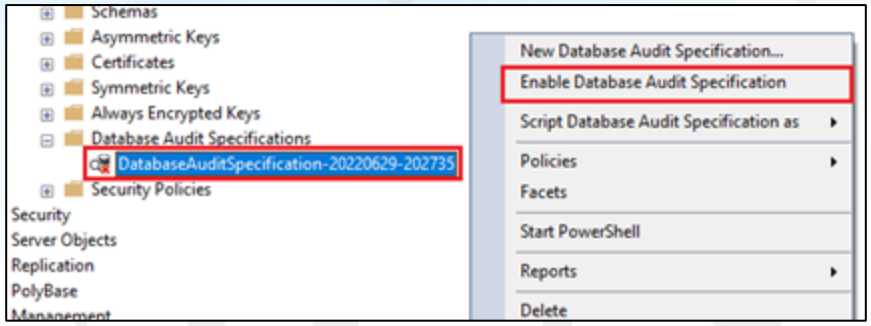
- En el **Explorador de objetos** de **Microsoft SQL Management Studio**, expanda la carpeta **Seguridad**.
- Luego expanda la carpeta **Auditorías**, haga clic con el botón derecho en la auditoría que desea activar y seleccione **Activar Auditoría.**



Auditoría SQL Server

3.2.Habilitar la especificación de auditoría de base de datos.

- En el **Explorador de objetos** de **Microsoft SQL Management Studio**, expanda la base de datos donde se encuentra la especificación de auditoría que desea activar.
- Expanda la carpeta **Seguridad**.
- Luego expanda la carpeta **Especificaciones de auditoría de base de datos**, haga clic con el botón derecho en la especificación de auditoría que desea activar y seleccione **Activar especificación de auditoría de base de datos.**

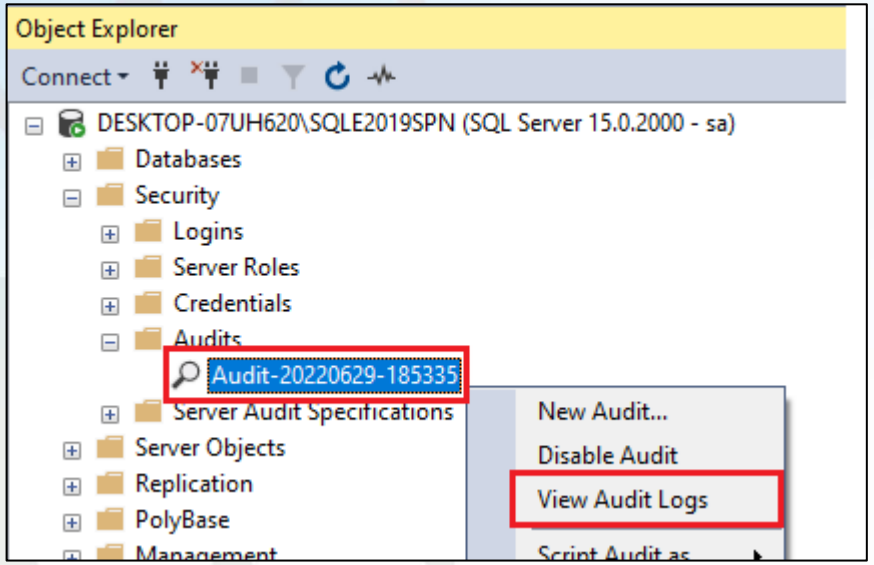


Auditoría SQL Server

4. Consultar la auditoría en SQL Server:

Para consultar los registros de auditoría en la base de datos:

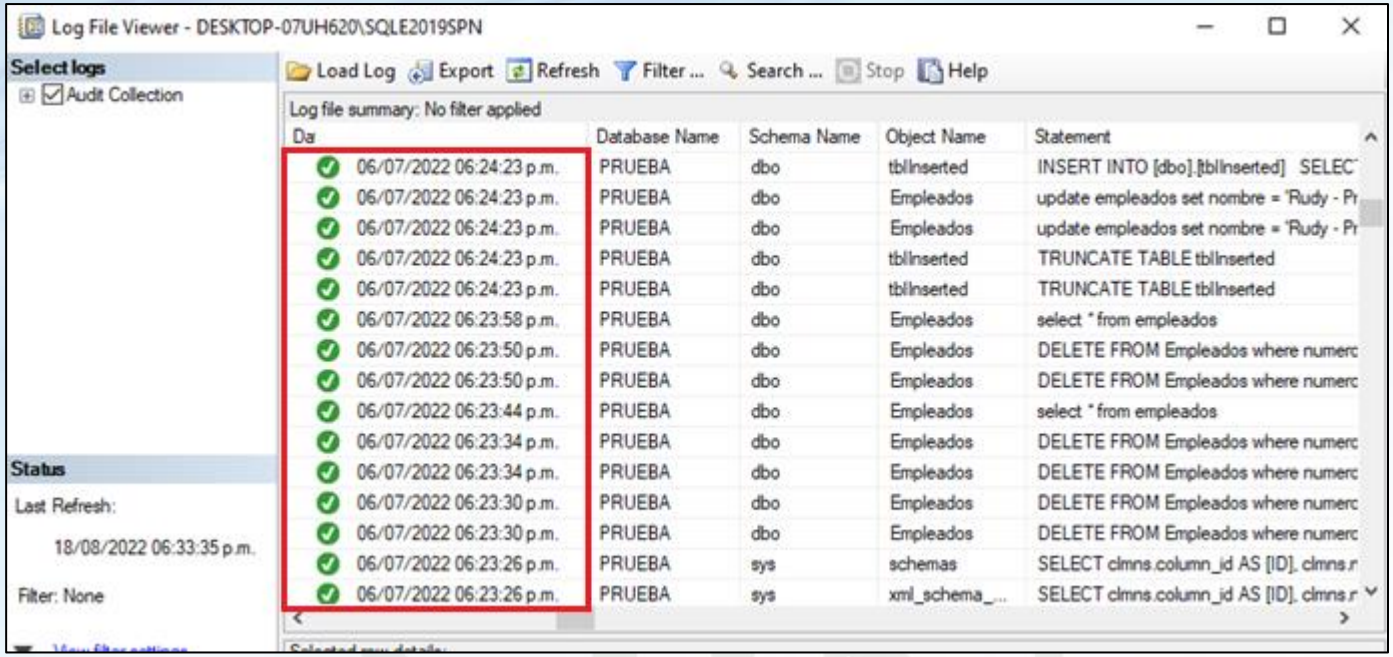
- En el **Explorador de objetos** de **Microsoft SQL Management Studio**, expanda la carpeta **Seguridad**.
- Luego expanda la carpeta **Auditorías**, haga clic con el botón derecho en la auditoría que desea consultar y seleccione **Ver registros de auditoría.**



Auditoría SQL Server

4. Consultar la auditoría en SQL Server:

Esta pantalla le muestra los eventos en la base de datos que han sido registrados por la auditoría:



***Nota**: SQL Server registra el evento usando el horario **UTC** y no la hora local del equipo. Por lo tanto, al momento de consultar la auditoría hay que hacer la conversión para ver la fecha y hora exacta del evento.

Auditoría SQL Server

5. **Ejemplo de modificaciones de datos y su verificación en la Auditoría:**

   Vamos a presentar 3 ejemplos de cambios en los datos:

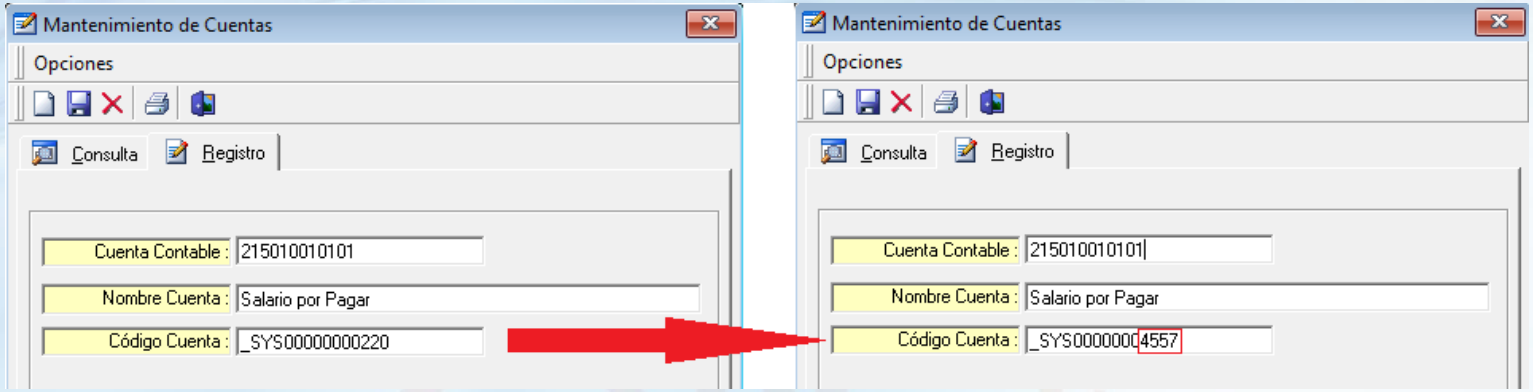
   - ***Actualización***
   - ***Inserción***
   - ***Eliminación***

   Lo realizaremos desde diferentes aplicaciones y vamos a observar como estos cambios se registran en la auditoría.

Auditoría SQL Server

5.1. Actualización de datos.

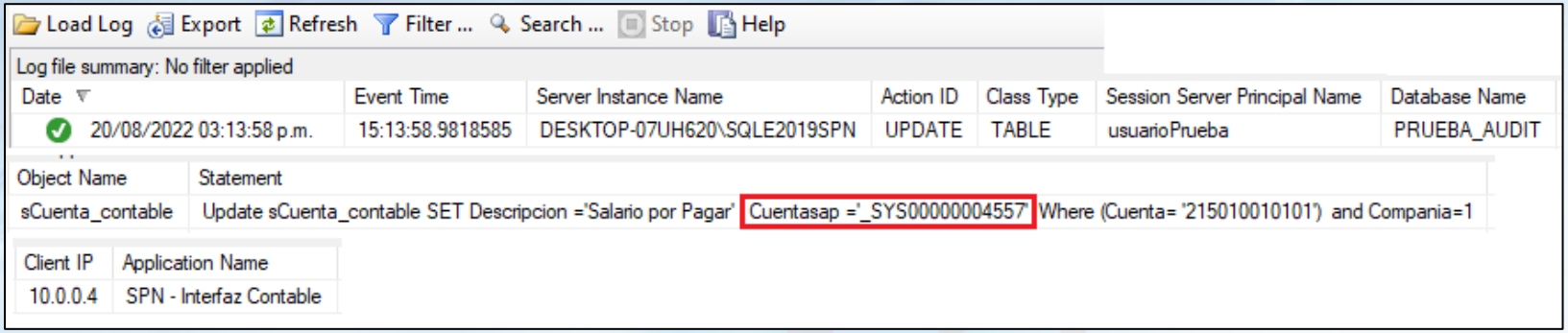
Se realizó un cambio en el campo Código Cuenta mediante este módulo:



Auditoría SQL Server

5.1.Actualización de datos.

Al consultar la auditoría, podemos ver:

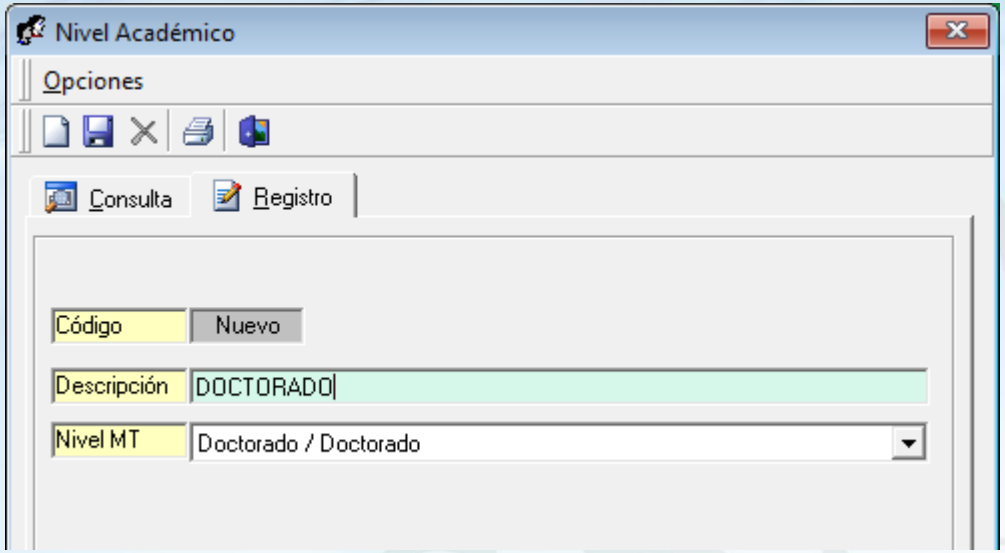


- Fecha y hora del evento
- Instancia de SQL
- Tipo de acción: **UPDATE**
- Tipo de objeto afectado: **TABLA**
- Usuario de la DB: **usuarioPrueba**
- Base de datos afectada: **PRUEBA_AUDIT**
- Nombre de la tabla afectada: **sCuenta_contable**
- **Sentencia SQL** completa donde vemos el cambio realizado.
- IP del equipo: **10.0.0.4**
- Nombre del aplicativo desde donde se realizó el cambio: **SPN – Interfaz Contable**

Auditoría SQL Server

5.2.Inserción de datos.

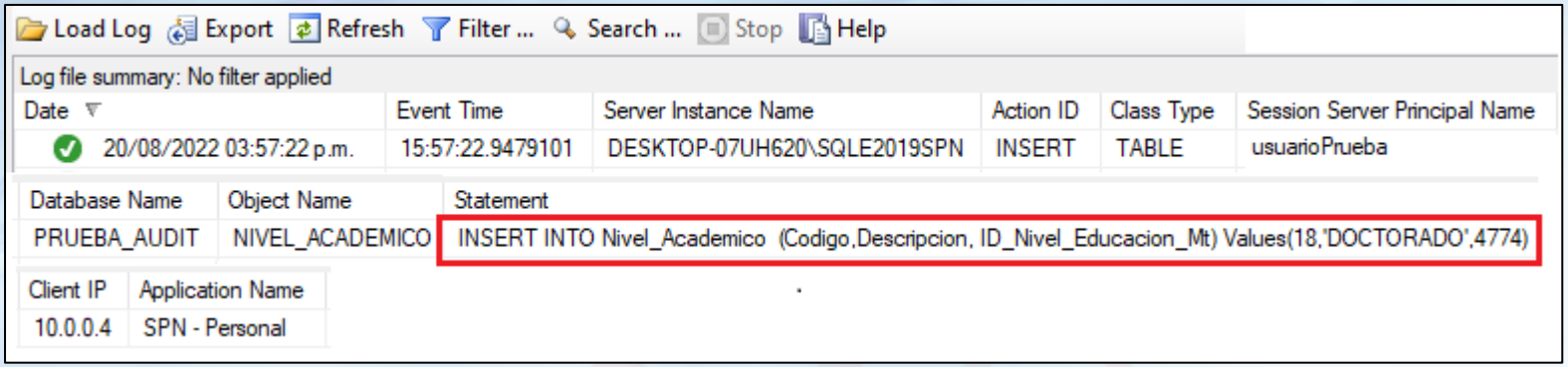
Para este ejemplo agregamos un nuevo Nivel Académico usando el módulo de *Personal*:



Auditoría SQL Server

5.2.Inserción de datos.

Al consultar la auditoría, tenemos:

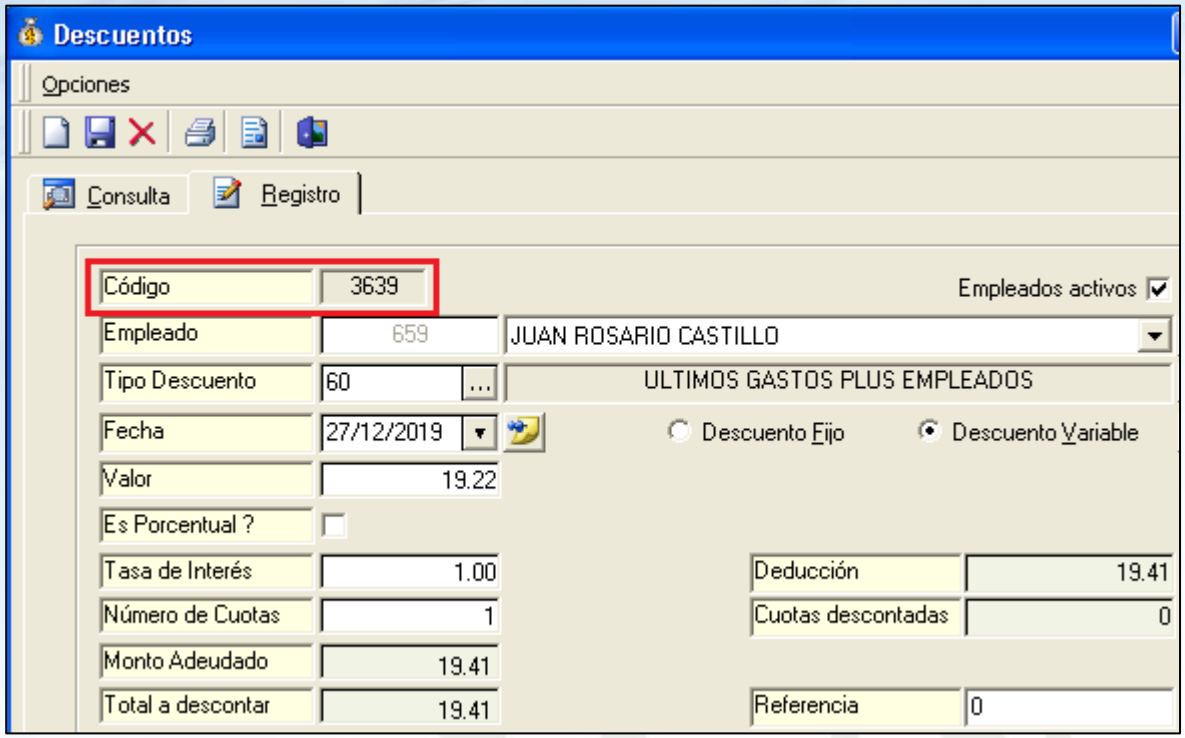


- Fecha y hora del evento
- Instancia de SQL
- Tipo de acción: **INSERT**
- Tipo de objeto afectado: **TABLA**
- Usuario de la DB: **usuarioPrueba**
- Base de datos afectada: **PRUEBA_AUDIT**
- Nombre de la tabla afectada: **NIVEL_ACADEMICO**
- **Sentencia SQL** completa donde vemos la inserción realizada.
- IP del equipo: **10.0.0.4**
- Nombre del aplicativo desde donde se realizó la inserción: **SPN – Personal**

Auditoría SQL Server

5.3.Eliminación de datos.

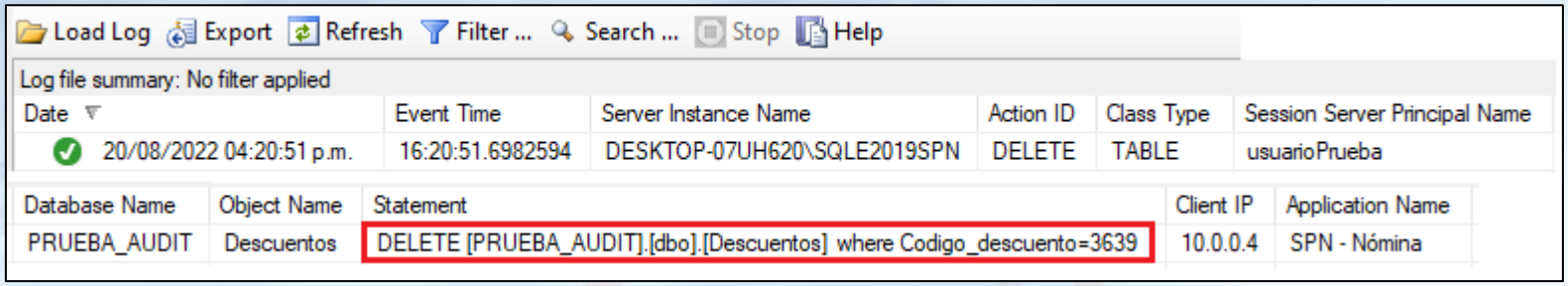
En este caso eliminamos un descuento usando el módulo de *Nómina*:



Auditoría SQL Server

5.3.Eliminación de datos.

Al consultar la auditoría, tenemos:



- Fecha y hora del evento
- Instancia de SQL
- Tipo de acción: **DELETE**
- Tipo de objeto afectado: **TABLA**
- Usuario de la DB: **usuarioPrueba**
- Base de datos afectada: **PRUEBA_AUDIT**
- Nombre de la tabla afectada: **Descuentos**
- **Sentencia SQL** completa donde vemos la eliminación realizada.
- IP del equipo: **10.0.0.4**
- Nombre del aplicativo desde donde se eliminó el registro: **SPN – Nómina**

Auditoría SQL Server

6. **Impacto en el espacio en disco al activar la auditoría SQL:**

   Es importante tomar en cuenta que estas auditorías almacenan toda esa información en disco, y su crecimiento va a depender de cuánta información estemos recolectando.

   Para evitar almacenar información innecesaria, se recomienda identificar con cada proveedor cuáles son esos objetos (tablas, vistas, etc.) críticos de la aplicación y auditar "**Acciones**" específicas tales como: **INSERT**, **UPDATE**, **DELETE** y **EXECUTE**.

   **Pueden consultar la documentación de MS SQL Server para ver las Acciones y los Grupos de Acciones y que implican cada uno.*

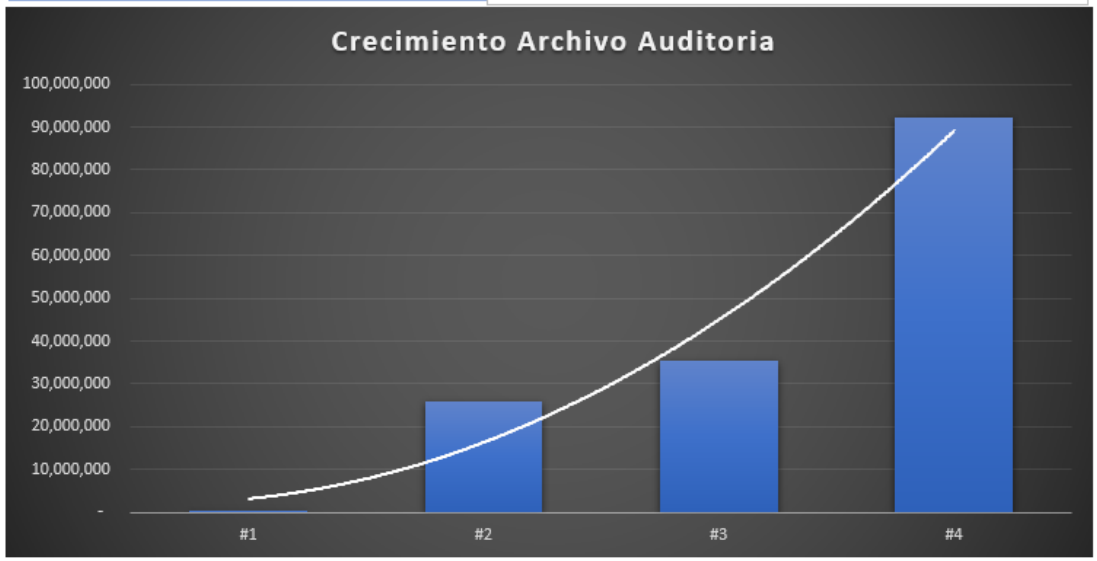
Auditoría SQL Server

6. Impacto en el espacio en disco al activar la auditoría SQL:

Este resultado fue con una muestra de 10 empleados y activando la auditoría para todos los objetos de la base de datos y para todos los tipos de acciones (DDL y DML):

Detalle	Peso en Bytes	Peso en MB
#1	16,384	0.02
#2	25,755,648	24.56
#3	35,520,512	33.88
#4	92,274,688	88.00

#1 Cuando activamos auditoria.
#2 Al importar empleados.
#3 Creamos 10 acciones de incorporacion y aumento de sueldo.
#4 Luego de procesar y postear nominas.



Auditoría SQL Server

FIN