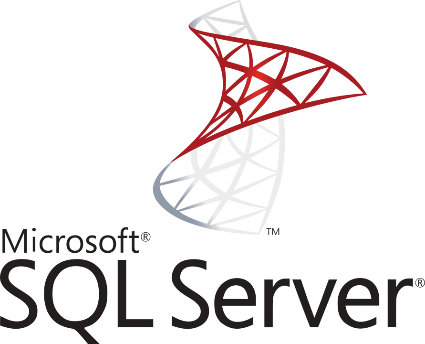
*“Año de la universalización de la salud”*

**Centro de Extensión y Proyección Social   
UNIVERSIDAD NACIONAL DE INGENIERÍA**



**Practica Calificada – 2**

**Trabajo:** **Plan de backup and Restore de una Base de Datos**

**Asignatura :** SQL Server 03 – Administración

**Docente :** Gustavo Coronel

**Integrantes :**

|  |  |
| --- | --- |
| Apellidos y Nombres | DNI |
| 1. Agip Mercedes , Hans Manuel | 40503113 |
| 1. Chumioque Gonzales, Luigui Brando | 75074906 |
| 1. Perfecto Diaz, Klaren Mercedes | 71279086 |

**Lima, 20 de diciembre del 2020**

**1. OBJETIVO Y ALCANCE**

**Objetivo:**

* El objetivo de este documento es describir los requisitos mínimos de respaldo y recuperación para todas las bases de datos alojados en el entorno de TI de la Compañía y administrados por los Servicios de TI.

**Alcance:**

* Estos estándares se aplican a los procesos continuos de copia de seguridad en disco y recuperación para todas las bases de datos de TI de la empresa.
* Es fundamental comprender que la copia de seguridad de bases de datos es un proceso que no debe confundirse con el uso de copias instantáneas con fines de archivos. Esta naturaleza significa que los medios de almacenamiento utilizados tienen un período de retención específico después del cual no se hace ningún esfuerzo para retener los datos. El medio simplemente se reutiliza y se sobrescribe con la copia de seguridad de datos más reciente.

**No es un alcance:**

* El archivo y los procesos asociados con la protección de los archivos no están sujetos a los estándares corporativos básicos.
* El uso de copias de seguridad para fines de control de versiones no está incluido y es inapropiado para estos estándares. Los procesos de control de versiones deben incluirse en los estándares de gestión de la información.
* El suministro de copias de los datos de respaldo para los procedimientos de replicación al sitio de recuperación de aplicaciones principales se rige únicamente por el estándar de objetivo de punto de recuperación. Se hace referencia a cómo se aplica la replicación al proceso de planificación de recuperación ante desastres de TI.
* El uso de cintas con el fin de realizar copias de seguridad continuas ya no es un proceso estándar de servicios de TI y está fuera del alcance de estos estándares. Se debe hacer todo lo posible en todas las ubicaciones para reemplazar los procesos de respaldo en cinta con respaldo en procesos de disco usando el kit de herramientas estandarizados de servicios de recuperación de datos.

**2. DEFINICIONES Y TÉRMINOS**

Estos estándares han sido desarrollados de acuerdo con los requisitos del sistema integrado de resiliencia de la Compañía: 'Ready, Response and Recovery', comúnmente conocido como Sistema R3, que incorpora Gestión de Crisis, Emergencias, Seguridad y Continuidad del Negocio.

Términos de recuperación (R3)

Interrupción máxima aceptable (MAO）

Objetivo de punto de recuperación (RPO)

Objetivo de tiempo de recuperación (RTO)

* 2.1.1 Ciclo activo

La etapa activa del ciclo de vida de la información para datos estructurados (bases de datos) se aplica cuando los datos experimentan cambios y desarrollos frecuentes. Esta es la etapa a la que se aplica la protección continua de copia de seguridad y recuperación definida en este documento.

* 2.1.2 Ciclo de referencia

La etapa de referencia del ciclo de vida de la información se relaciona con el momento en que los datos ya no se cambian, pero pueden continuar leyéndolo de manera regular, como los datos históricos del Proyecto. Estos datos se pueden migrar a dispositivos de almacenamiento secundarios y se pueden realizar copias de seguridad en intervalos poco frecuentes y se pueden restaurar en raras ocasiones. El estándar de Interrupción Máxima Aceptable (MAO) se aplica a esta fase del ciclo de vida, sin embargo, el RPO y los ciclos continuos no.

* 2.1.3 Ciclo de archivo

La etapa de archivo del ciclo de vida de la información es cuando el uso de los datos disminuye significativamente o se aplica al período después del cual un proyecto se cerró y ya no se hace referencia y se requiere que se mantenga durante un período de tiempo específico para cumplir con los requisitos de cumplimiento. Cuando se requiera replicar estos datos, el estándar MAO se aplica al proceso de replicación; sin embargo, el RPO y los ciclos continuos no lo hacen.

* 2.2.0 Condiciones de los servicios de recuperación de datos (DRS)
* 2.2.1 Ciclo continuo de protección de datos

Se refiere al número de intervalos (días) secuenciales y consecutivos en los que se realizan copias de seguridad antes de que se reinicie el ciclo. Este término no se debe confundir con la toma de instantáneas de sincronización, que se refiere a un proceso de administración de datos utilizado por DPM. El ciclo mínimo para los servicios de TI es de siete días y el estándar recomendado es de 30 días.

Estos estándares se basan en estadísticas de recuperación de la industria que muestran la siguiente frecuencia de solicitudes de recuperación:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **PLAN DE BACKUP** | | | | | | | |
| **HORA** | **SÁBADO** | **DOMINGO** | **LUNES** | **MARTES** | **MIÉRCOLES** | **JUEVES** | **VIERNES** |
| 08:00 | OK |  | OK | OK | OK | OK | OK |
| 09:00 |
| 10:00 |
| 11:00 |
| 12:00 | BK LOG | BK LOG | BK LOG | BK LOG | BK LOG |
| 13:00 | OK |  | OK |  | OK |
| 14:00 | **ERROR** |  |
| 15:00 | OK |  |
| 16:00 |  |
| 17:00 |  |
| 23:00 | **BK FULL** | BK DIF | BK DIF | BK DIF | BK DIF | BK DIF |

**3. TÉRMINOS DE RECUPERACIÓN**

* 3.3.1 Recuperación de base de datos

La recuperación de datos requiere un sistema de respaldo que pueda guardar y posteriormente restaurar archivos desde el disco en base a un punto de recuperación dentro del RPO definido. Esto debería abarcar la recuperación de una base de datos por etapas o completa. Los eventos de recuperación del sistema pueden ser tan simples como una falla en un disco físico o tan complejos como una falla completa del servidor y podría resultar en múltiples interrupciones.

Los servicios de TI deben dar prioridad al desarrollo de un mapa de servicios que describa todas las relaciones relevantes necesarias para la disponibilidad de cada servicio de modo que, en caso de una operación de reconstrucción después de una interrupción importante, todos los elementos se recuperen. Los procedimientos de reconstrucción deben incluirse o mencionarse en el Plan IT-DR porque esta tarea deberá llevarse a cabo mientras se proporciona acceso alternativo a las aplicaciones. El incumplimiento de este requisito expone a la empresa a una pérdida total de la capacidad operativa si los sistemas no pueden reconstruirse a tiempo o proporcionarse en una ubicación alternativa.

La estrategia de TI corporativa claramente pone énfasis en reducir el riesgo de pérdida física al abstraer la mayor cantidad posible de dependencia de la capa física y reemplazar los sistemas con entornos virtuales que están protegidos regularmente y disponibles para iniciarse rápidamente en otra ubicación. Esto es mucho más adecuado que mantener alternativas de capa física dual y proporciona un grado mucho mayor de agilidad en la protección de los procesos comerciales que dependen de la presencia de TI.

* 3.3.2 Recuperación ante desastres

La recuperación ante desastres se define como el proceso, las políticas y los procedimientos relacionados con la preparación para la recuperación o continuación de los Servicios de TI críticos para el negocio de la Compañía después de un desastre natural o inducido por el hombre. La planificación de la recuperación ante desastres de TI es un requisito de los procesos de planificación de la continuidad del negocio de R3 y puede invocar los estándares descritos en este documento. Es fundamental que el Plan IT-DR contenga los detalles señalados en estas normas y que los procedimientos y condiciones para la coordinación de reconstrucción y cambio con R3 estén incluidos en la documentación.

**4. TÉRMINOS DE RESTAURACIÓN**

La restauración de base de datos debe ser un proceso documentado para cada uno de los principales servicios de aplicaciones que brindan los servicios de TI, que incluyen: bases de datos SQL (tanto de tipo único como de grupo). Los procedimientos para la recuperación completa de los sistemas deben describirse e incluirse dentro de los Planes IT-DR. El tiempo de recuperación del sistema no está definido porque la recuperación de los sistemas originales para volver a funcionar como de costumbre después de una interrupción importante es indeterminada.

Todas las solicitudes de restauración que no estén directamente relacionadas con un evento de interrupción declarada deben pasar por uno de los siguientes procesos:

• La mesa de servicio de TI.

• El proceso de gestión de cambios de TI.

• El proceso de gestión de incidentes de TI.

**5. PRUEBA DE RESTAURACIÓN**

Los servicios de TI son responsables de probar los procesos de recuperación de acuerdo con los requisitos descritos en el Plan IT-DR luego de la implementación exitosa de un proceso de respaldo. El alcance y la profundidad de la prueba de recuperación deben coincidir con los requisitos de la empresa y debe realizarse según los procedimientos R3.

Las pruebas de restauración deben realizarse con datos de respaldo de producción en vivo en sistemas de prueba adecuados u otro sistema apropiado que proteja la integridad de los sistemas de producción y la información. Una vez completada la prueba, el entorno de prueba debe estar totalmente limpio de todos los datos. Esta prueba debe documentarse y los resultados deben informarse al Coordinador de R3.

Los usuarios del sistema deberán participar en la prueba para garantizar que el sistema funcione según lo previsto.

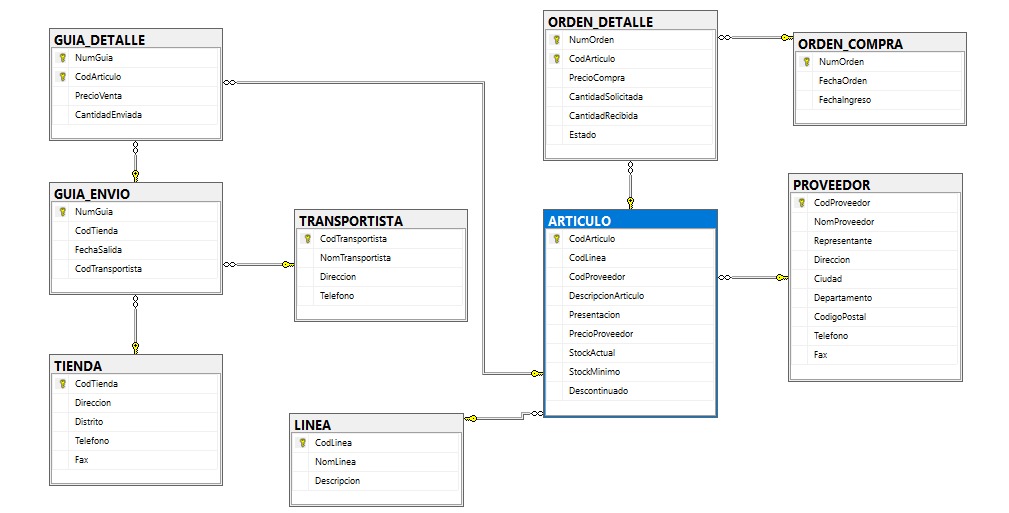
Los servicios de TI deben tener procedimientos para abordar cualquier debilidad del proceso descubierta mediante la prueba del Plan IT-DR. Una vez que se han identificado estas debilidades, se deben documentar, diseñar planes de remediación y luego implementarlos. La verificación de la implementación se incluirá en los programas periódicos de auditoría interna y como parte del ciclo de prueba R3, cuando corresponda.

**6. EJECUCIÓN DE LA PRUEBA**

**Desarrollo:**

DB objeto de estudio: QhatuPeru

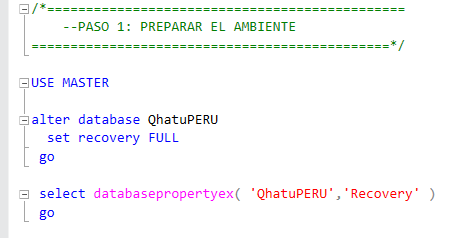
Contexto: la DB de QhatuPeru está compuesta por 08 tablas, las cuales están relacionadas de la siguiente manera:



Para la demostración del BACKUP y Restauración debemos de seguir los siguientes pasos

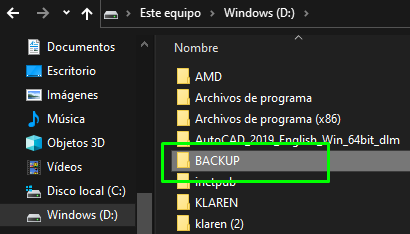
**PASO 01: Preparación del ambiente**

Es importante que la DB QhatuPeru esté en modo recuperación, para ello vamos a ejecutar el siguiente Script.

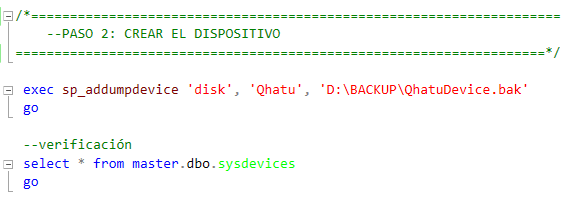


**PASO 02: Crear el dispositivo de almacenamiento**

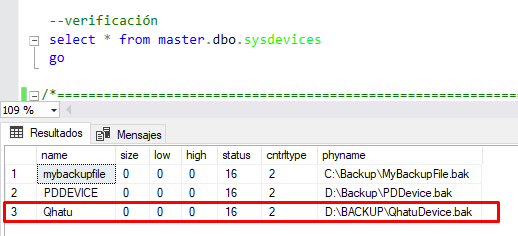
Para ello primero debemos de elegir la carpeta donde se guardará nuestro dispositivo



Luego, procedemos a crear el dispositivo Qhatu.

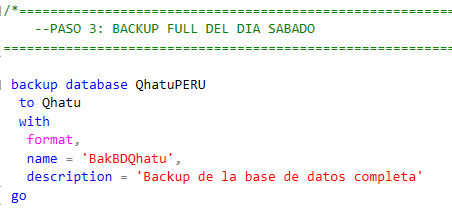


luego verificamos la creación del dispositivo

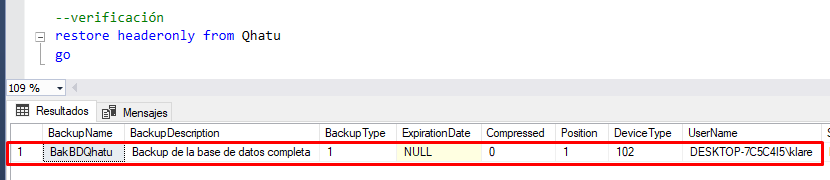


**PASO 03: BACKUP Full el día Sábado**

Para efectos de la simulación, partiremos desde el día sábado y acorde al cronograma ese día se realiza un backup completo

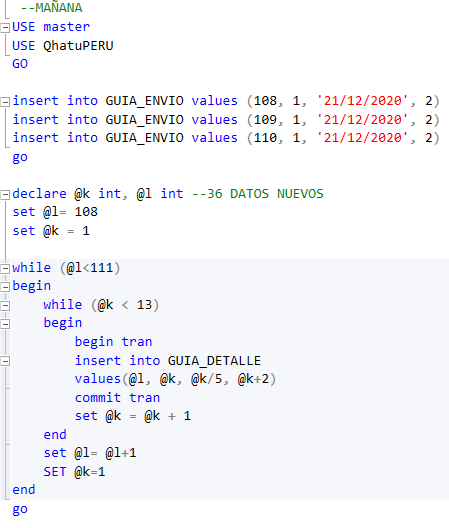


Para verificar seguimos la siguiente sentencia:

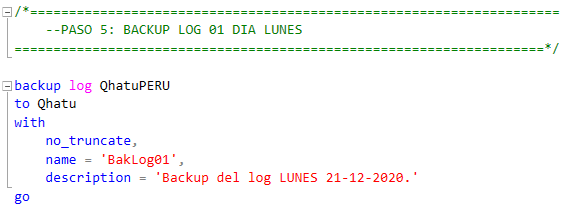


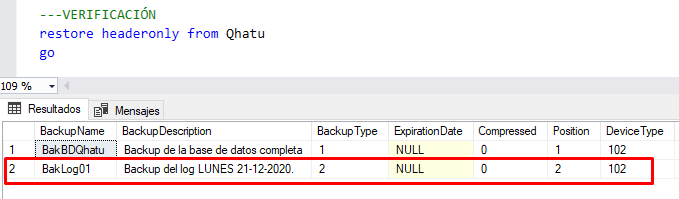
**PASO 04: Insertar datos del día LUNES 21/12/2020**

Se procede a hacer la simulación de insertar nuevos datos a las siguientes tablas GUIA\_ENVIO y GUIA\_DETALLE, hasta el mediodía.



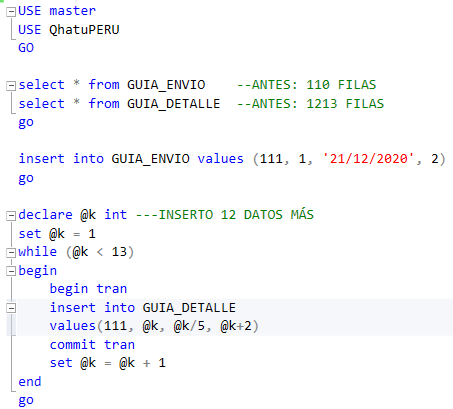
**PASO 05: BACKUP LOG del día LUNES 21/12/2020**





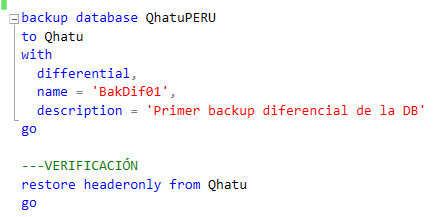
**PASO 06: Insertar más datos del día LUNES 21/12/2020 luego del mediodía**

Luego de realizar el Backup LOG del día lunes, se procederá a seguir insertando nuevos datos a las tablas, para ello ejecutaremos el siguiente Script:

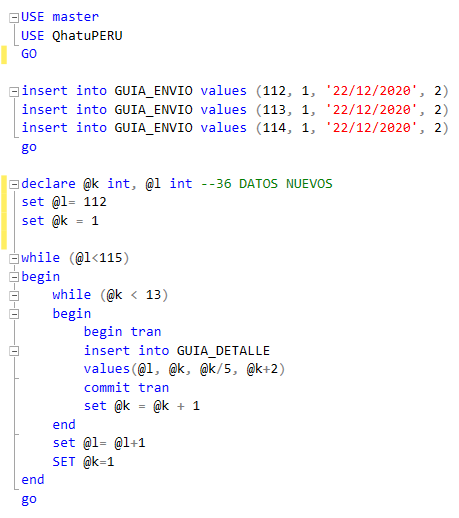


**PASO 07: BACKUP DIFERENCIAL del día LUNES 21/12/2020**

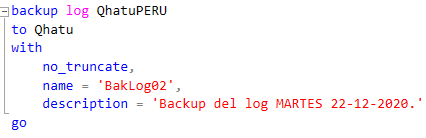
Al final del día se realiza un Backup DIFERENCIAL



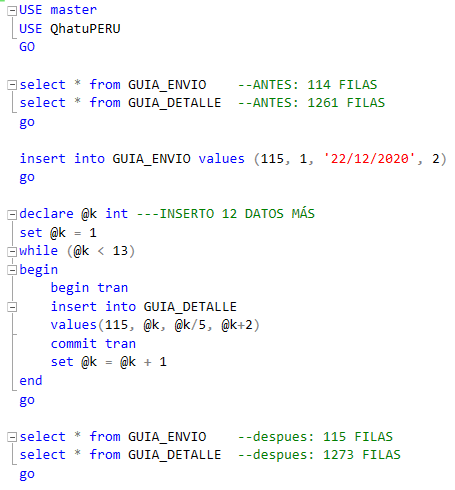
**PASO 08: Insertar datos del día MARTES 22/12/2020**



**PASO 09: BACKUP LOG del día MARTES 22/12/2020**



**PASO 10: Insertar más datos del día MARTES 22/12/2020 luego del mediodía**



A las 13 horas del día Martes, se presentó un **ERROR** en la DB QhatuPeru, esto debido a que se insertaron datos erróneos entre las 12 - 13 pm de ese mismo día.

Para solucionar este error se restaurará el BACKUP FULL + DIF LUNES + BACKUP LOG 02

**PASO 11: Restauración**

