Informe de Backup de Base de Datos

Fecha de Elaboración: 15 de noviembre de 2024

Responsable del Backup: DBA

Versión: 1.0

1. Propósito de las Políticas de Backup

- **Objetivo**: El objetivo principal de este backup es asegurar la protección de los datos contenidos en la base de datos [Com5600G09] ante posibles incidentes de pérdida o corrupción. La copia de seguridad se realizará de forma completa para garantizar la continuidad del negocio y cumplir con los requisitos de recuperación ante desastres (DRP). Ya que es de vital importancia que no se pierda los detalles de ventas.

2. Frecuencia de los Backups

- **Tipos de Backup**:
  - **Completo**: Mensualmente se debe guardar los datos de ventas para guardarlo en el histórico de ventas.
  - **Diferencial**: Cada día se debe guardar las ventas totales realizadas por cada empleado.
  - **Incremental**: Cada vez que se realiza una venta se registra y se guarda.
- **Cronograma de Backup**:

  - **Completo:** Al finalizar cada mes desde que cierra la última venta del ultimo día del Mes se debe comenzar a hacer el Backup. Hora aproximada 23HS
  - **Diferencial:** Cada vez que se finalice el día se debe comenzar a hacer el Backup. Hora aproximada 23HS.
  - **Incremental:** Luego de oficializar la venta se realiza un Backup.

3. Ubicación de Almacenamiento de los Backups

- **Ubicación Primaria**: Almacenamiento en servidores locales.
- **Ubicación Secundaria (Off-site)**: Almacenamiento externo en la nube, Microsoft Azure
- **Retención de Backups**: Se debe mantener las copias diarias durante un mes y las mensuales durante un año.

4. Restauración de Backups

- **Frecuencia de Pruebas de Restauración**: Pruebas Mensuales, Pruebas Trimestrales, Pruebas Anuales, Pruebas de Restauración después de Cambios Críticos.
- **Tiempo de Recuperación Objetivo (RTO)**: Al ser un supermercado, el tiempo máximo de recuperación no puede ser mayor a un día.

5. Seguridad de los Backups

- **Cifrado**: Todos los backups deben estar cifrados utilizando algoritmos de cifrado de alto nivel, como AES-256, para proteger los datos sensibles durante su almacenamiento y transferencia.
- **Motivo del Cifrado**: El cifrado es una medida esencial para evitar que los datos de los backups sean accesibles en caso de pérdida, robo o acceso no autorizado. Es especialmente importante si los backups se almacenan en ubicaciones externas, como la nube o unidades físicas fuera del sitio.
- **Control de Acceso**: Los Backups solo puede ser accedidos por el DBA a cargo
- **Registro de Accesos:**
    - Todos los accesos a los backups deben ser registrados en un log de auditoría detallado. Estos registros deben incluir la identidad del usuario, el tipo de acceso realizado (lectura, escritura, restauración), y la fecha y hora de acceso.
    - Los logs deben almacenarse de forma segura y ser accesibles solo por personal autorizado para evitar manipulaciones o accesos indebidos.

6. Gestión de Errores y Alertas

- **Registro de Errores**: Se llevará un registro de los errores durante los procesos de backup y su resolución.
- **Notificaciones de Fallo**: Alertas inmediatas para los administradores en caso de fallos durante la copia de seguridad.
- **Plan de Acción ante Errores**: Procedimientos para identificar y resolver problemas con los backups fallidos.

7. Revisión y Actualización de Políticas

- **Revisión Regular**: Las políticas de backup deben ser revisadas y actualizadas anualmente o tras cambios significativos en el sistema.
- **Documentación de Cambios**: Registrar cualquier modificación en las políticas y el motivo de estos cambios.