BASE DE DATO II

¿QUÉ ES UN PLAN DE CONTINGENCIA DE BASE DE DATOS?

En el proceso de recuperación de datos y unificación de información en caso de presentarse una contingencia, se presentan diversos escenarios típicos y frecuentes de recuperación, donde el Director de Infraestructura Tecnológica procederá:

- Informar inmediatamente al DBA encargado de la Base de Datos.
- El DBA evaluará la naturaleza de la contingencia y procederá de acuerdo a los siguientes escenarios, es de aclarar, que las contingencias que se puedan presentar a nivel de base de datos son numerosas, razón por la cual se explican los casos más frecuentes y típicos.
- Si la contingencia es a nivel de Hardware (referente a todas las partes que componen el servidor.
- Si la contingencia esta en el Software de la BDD (debido a un daño físico del disco con información de la base de datos) se describen los posibles eventos:
    - Daños en archivos de control.
    - Daño en archivos de Redo se procede:
        - Si es un solo archivo, se borra el archivo dañado y se recrea
        - Si se dañan todos los archivos, se procede a recuperar la base de datos.
    - Daño de table spaces diferentes a los del system se procede:
        - Recuperar la base de datos con el backup del export, del día inmediatamente anterior.
    - Daño en alguno de los table space.
    - Daño en archivo temporal o de Undo se procede:
        - Crear nuevos archivos, desactivar el anterior y posteriormente borrarlo.
    - Daño o pérdida total de una de las bases de datos
        - El DBA encargado de la base de datos, notificará al Director de Infraestructura Tecnológica la solución correspondiente.
        - El Director de Infraestructura Tecnológica junto con el proveedor del aplicativo y los funcionarios de cada una de las unidades de negocio, entraran hacer las validaciones correspondientes de la funcionalidad del aplicativo, de tal manera que de llegar a encontrar inconsistencias en la funcionalidad de alguno de los aplicativos, le reportará al DBA encargado para que este a su vez la subsane.
        - En el evento de faltar el Director de Infraestructura Tecnológica, para solventar esta contingencia, el personal de Coordinación Plan Operativo, deberá contactar al DBA encargado de la Base de Datos, información que se encuentra en el ANEXO No. 4 de este documento, respecto a la restauración de los exports realizados a la base de datos.
        - Existen dos procedimientos diferentes para hacer la restauración total de la bases de datos, el primero es a partir de los backups hechos con la utilidad RMAN (“rman”), el segundo es usando los archivos exports hechos con la utilidad de Export (“exp”).

Ejemplo de un Plan de contingencia en base de datos

1. OBJETIVO Y CAMPO DE APLICACIÓN

El Centro de Cómputo -Nivel Central, se encargará de proteger y garantizar que los recursos del sistema de información (Aplicaciones y Bases de Datos) de la Superintendencia de Notariado y Registro, se mantengan respaldados y sean fácilmente recuperables en el momento que se necesite.
Los clientes del proceso son la Superintendencia de Notariado y Registro -Nivel Central- incluyendo las aplicaciones asignadas para su administración de los entes externos.

2. ALCANCE:

Inicia: Inicia con la programación que se tiene definida en el Centro de Cómputo de la SNR para hacer copias de seguridad de las bases de datos de los sistemas de información.
¿Qué hace?: Ejecutar procedimiento para cada base de datos y diligenciar bitácora de Backup de acuerdo a su periodicidad.
Termina: Con la verificación del Backup y posterior custodia de dichas copias de seguridad.

3. RESPONSABLES:

Responsable estratégico: Jefe Oficina de Informática
Responsable operativo: Coordinador de Grupo Centro de Cómputo, Profesional especializado, Profesional Universitario y Analista de sistemas.

4. DEFINICIONES:

BACK-UP: Copia de seguridad de los archivos, aplicaciones y/o bases de datos disponibles en un soporte magnético (generalmente discos o CD`s), con el fin de poder recuperar la información en caso de un daño, borrado accidental o un accidente imprevisto. Es conveniente realizar copias de seguridad a intervalos temporales fijos (diario o semanal, por ejemplo), en función del trabajo y de la importancia de los datos manejados.

Copia de Respaldo o Seguridad: Acción de copiar archivos o datos de forma que estén disponibles en caso de que un fallo produzca la pérdida de los originales. Esta sencilla acción evita numerosos, y a veces irremediables, problemas si se realiza de forma habitual y periódica.

Base de Datos: Conjunto de datos que pertenecen al mismo contexto almacenados sistemáticamente. En una base de datos, la información se organiza en campos y registros. Los datos pueden aparecer en forma de texto, números, gráficos, sonido o vídeo.

Copias de Seguridad: copias de la información en un medio magnético que se almacena en un lugar seguro.
Contingencia: Conjunto de procedimientos de recuperación. Las acciones a contemplar aplican para Antes- Durante- Después con el fin de reducir las pérdidas.
Plan de Contingencia: procedimientos alternativos de una entidad cuyo fin es permitir el normal funcionamiento de esta y/o garantizar la continuidad de las operaciones, aún cuando alguna de sus funciones se vean afectadas por un accidente interno o externo.

Recuperación: Hace referencia a las técnicas empleadas para recuperar archivos a partir de una copia de seguridad (medio externo); esto se aplica para archivos perdidos o eliminados por diferentes causas como daño físico del dispositivo de almacenamiento, borrado accidental, fallos del sistema, ataques de virus y hackers.

Restauración: Volver a poner algo en el estado inicial. Una Base de Datos se restaura en otro dispositivo después de un desastre.

PHVA

- **Planeación:** Garantizar la realización de respaldo.
- **Hacer:** Desarrollar cada una de las actividades contempladas en el proceso de Backup. Realizar recuperación de información cuando sea necesario.
- **Verificación:** Registrar en la bitácora de control de Backup's.
- **Actuar**: Hacer seguimiento proceso de Backup`s.

5. **CONTENIDO:** Se describe la actividad y se establecen los link con formatos, documentos, instructivos, protocolos, normas y actas.

ACTIVIDAD ESENCIAL	DESCRIPCIÓN. ¿CÓMO?
Proceso de Backup	**Descripción de actividades:** 1. Determinar o identificar el número de aplicativos y/o bases de datos para respaldo. 2. Determinar los mecanismos de copias de respaldo según la base de datos a respaldar: manual o automático. 3. Verificar si el Backup es automático el sistema asigna fecha de creación de la base de datos, si no se debe cambiar la fecha de creación de la misma. 4. Verificar los archivos log del servidor. 5. Comprimir los archivos en formato .zip o .rar si la copia se realiza correctamente. 6. Verificar las copias comprimidas, para verificar que se pueden descomprimir cuando se necesiten. 7. Volver a realizar copia por segunda vez, si el archivo log del servidor indica un error. 8. Grabar diaria, semanal y anualmente, en un dispositivo de almacenamiento (CD) todas las copias y guardar en la Oficina de Informática. 9. Grabar mensualmente en un dispositivo de almacenamiento (CD) todas las copias se guarda una en la oficina de Informática y se envía otra a un ente externo. 10. Diligenciar en los formatos de control las copias realizadas con sus respectivas bases de datos y fecha de creación. **Nota:** Las copias de Backup de las Bases de Datos realizadas en el Centro de Cómputo se generan de dos formas: manual y automática ejecutando

	Scripts de Backup's. **Responsable:** Coordinador Centro de Cómputo, Profesional Universitario, Analista de Sistema y Técnico. **Conocimiento:** Aplicaciones y Bases de Datos. **Recursos esenciales:** Sistema de información, instructivos y equipos. **Normatividad:** • NTC-ISO/IEC 27001 Sistema de Gestión de Seguridad de la Información. • Ley 23 de 1982: Sobre Derechos de Autor • Decretos y normatividad aplicable a la SNR. **Herramientas de control:** Bitácora de Control y Formulario de Solicitud de Gestión de Usuarios **Frecuencia:** Diaria, semanal y/o mensual **Tecnología (M.A.S):** Manual, automatizado y sistematizado.

Seguimiento a la bitácora de control	**Descripción de actividades:** 1. Revisión y verificación sobre el diligenciamiento completo. 2. Cumplimiento de las políticas de seguridad de la Entidad. **Responsable:** Coordinador Centro de Cómputo, Profesional Universitario, Analista de Sistema y Técnico. **Conocimiento:** Aplicaciones y Bases de Datos. **Recursos esenciales:** Sistema de información, instructivos y equipos. **Normatividad:** • NTC-ISO/IEC 27001 Sistema de Gestión de Seguridad de la Información. • Ley 23 de 1982: Sobre Derechos de Autor • Decretos y normatividad aplicable a la SNR (Políticas de Seguridad en los Sistemas de Información). **Herramientas de control:** Bitácora de Control y Formulario de Solicitud de Gestión de Usuarios **Frecuencia:** Diaria, semanal y/o mensual **Tecnología (M.A.S):** Manual, automatizado y sistematizado.

6. **DOCUMENTOS DE REFERENCIA**.
   - ISO/IEC: 17799 e ISO/IEC: 27001. Seguridad Informática.

7. NOTAS DE CAMBIO.

VERSIÓN	FECHA	NATURALEZA DEL CAMBIO
01	10- 06- 07	Se creó el proceso
02	23-12-09	Se hizo ajustes al procedimiento acorde con los resultados de la auditoría interna
03	03-05-10	Se hizo ajustes al procedimiento acorde con los resultados de la Preauditoria, se incluyeron los formatos

Formatos de Novedades

Código	Nombre
GT-GRT-PR-07-FR-03	Bitácora control de Backups (anual)
GT-GRT-PR-07-FR-04	Bitácora control de Backups (diaria)
GT-GRT-PR-07-FR-05	Bitácora control de Backups (mensual)
GT-GRT-PR-07-FR-06	Bitácora control de Backups (Semanal)
GT-GRT-PR-07-FR-07	Recuperación Base de Datos
GT-GRT-PR-07-FR-08	Restauración Backups Base de Datos
GT-GRT-PR-07-FR-09	Copias de Seguridad
GT-GRT-PR-07-FR-10	Copias de Seguridad Redologs
GT-GRT-PR-07-FR-11	Copia Recepción Backups