ALCALDÍA MAYOR
DE BOGOTÁ D.C.
AMBIENTE
Instituto Distrital de Gestión de Riesgos
y Cambio Climático

Instructivo Backup de Bases de Datos ORACLE

TICS-IN-02
Versión 2

1. Objetivo. Proteger la información, base de datos y documentación critica para la entidad con el fin de que se conserven respaldados, así como permitir la restauración de la misma en el momento que se necesite.

2. Alcance. Inicia con la programación que se tiene definida en el área de tecnología para las copias de seguridad de la información y bases de datos y termina con la verificación del backup en medio de almacenamiento externo y la salvaguardia de esta información.

14/02/2018

3. Consideraciones generales

Es responsabilidad del administrador de la base de datos definir la manera de tomar los backups de las diferentes bases de datos para que estas copias sean guardadas en medio externo por parte de Administrador de Infraestructura Tecnológica.

En la actualidad el IDIGER cuenta con dos servidores en arquitectura RAC, los cuales incluyen 4 bases de datos en ambiente productivo. El RAC lo componen dos servidores ATLAS y FENIX.

Las bases de datos productivas son SIREDB, SICAP, SICAPITAL y SICAPDES. Este documento es expresamente sobre el backups de estas cuatro bases de datos,

Políticas Específicas para Servidores, base de datos, Código fuente de aplicaciones y Archivos de usuarios:

Las copias de seguridad o respaldo a cintas u otro medio magnético deben generarse al menos una vez al mes según lo determine el grupo TIC de IDIGER.

Los BackUp's a discos deben mantenerse al menos 15 días antes de pasarse a cintras u otro medio magnético.

Las copias de seguridad se administrarán mediante la herramienta de backup vigente licenciada por la entidad.

Las políticas de backup aplican así

Backup de configuración de servidores: Incluyen la configuración del sistema operativo, políticas, reglas configuradas y despliegue de aplicaciones. Debe hacerse al menos una vez por semana (martes) en días de menos carga operativa o antes de una tarea de mantenimiento ya sea preventivo o correctivo y sin afectar la operación de los usuarios de la entidad. Se deben etiquetar como SVR_DDMMYYYY. Aplica para los servidores de Directorio Activo, Firewall, PANDORA.

Bases de datos: Incluyen Backups completos de toda la data, deben hacerse al menos dos veces por semana, los días lunes y jueves o antes de una tarea de mantenimiento preventivo o correctivo. Deben etiquetarse como nombre-bd_DDMMYYYY.bkp Aplica para los servidores de Bases de datos.

Código Fuente de aplicativos desarrollados: Será responsabilidad del grupo de desarrollo, los cuales deberán notificar la periodicidad y forma de Acorde a lo determinado por el grupo de desarrollo, Deben etiquetarse como: APL_DDMMYYYY. Para este BackUp se asignará un espacio en el NAS. En caso de que no se encuentre información actualizada para el BackUp se notificará por correo electrónico al supervisor del responsable

Archivos de usuarios: Es responsabilidad de cada usuario y de su supervisor almacenar sus archivos en el NAS siendo igualmente responsable de la calidad del

backup. Se sugiere etiquetarse como \\vnas1\home\nombre_usuario\numero_contrato. No se podrán almacenar archivos de carácter personal, solo debe estar almacenado lo concerniente a las funciones y productos de su objeto contractual. En caso de encontrar archivos que no corresponden a las funciones específicas estos serán borrados

Backup de correo electrónico: Es responsabilidad del grupo de infraestructura tecnológica hacer un backup de la cuenta de correo electrónico una vez que se requiera suspender la cuenta. Deben etiquetarse con el mismo nombre de usuario, inicialmente se enviará a archivado desde la URL suministrada por el proveedor del servicio de correo electrónico y descargarse en un archivo PST de Outlook o en otro formato que sea fácilmente configurable por el usuario

Para la restauración de los datos se debe solicitar directamente al grupo de apoyo a la infraestructura tecnológica con la justificación correspondiente indicando la información qué se requiere. La solicitud debe hacerse mediante la herramienta de HelpDesk o en su defecto vía correo electrónico.

Control de acceso a sistemas de información y recursos de red

El acceso a plataformas, sistemas de información y recursos de red será asignado por el equipo de administración tecnológica acorde a los requerimientos de cada usuario y/o grupo de trabajo siempre y cuando sea para contribuir al normal desarrollo de sus obligaciones contractuales, y sin hacer uso indebido o para fines personales de la información respaldada en los sistemas de información.

Cualquier usuario interno o externo que requiera acceso a la red dentro de las instalaciones de la entidad debe estar previamente autenticado, si el acceso es de manera remota, ésta debe ser una conexión cifrada por el firewall-proxy de la entidad con certificado de vigencia máximo la duración del contrato

Control de acceso al centro de cómputo

Solo tendrá acceso al centro de cómputo el personal autorizado por el grupo de administración tecnológica de IDIGER, o personal que tenga responsabilidad directa en administración de algún servidor y/o planta telefónica, sistema de grabación, para el caso de IDIGER, el personal de los siguientes grupos:

a. Administración tecnológica
b. Redes y monitoreo
c. Comunicaciones

El acceso a la sala de monitoreo de servidores se hará mediante control biométrico, y solo tendrá acceso el grupo de administración tecnológica. El acceso a la sala de servidores se hará mediante tarjeta y clave.

Todos los funcionarios y/o contratistas que requieran acceso permanente al centro de cómputo deben estar registrados en el sistema de huellas o tener tarjeta de autorización con

su correspondiente clave. De igual manera debe estar autorizado por el administrador del centro de cómputo.

Ninguna persona externa a la entidad o visitante puede ingresar al centro de cómputo sin la debida autorización del administrador del centro de cómputo.

El visitante no necesita registrarse en el sistema de huellas pero debe diligenciar el formato Planilla de acceso al centro de cómputo.

4. Definiciones

BACKUP
Es la acción de copiar archivos de forma total o parcial de la información de archivos, carpetas, aplicaciones o bases de datos, esta copia de respaldo debe ser guardad en un dispositivo de almacenamiento externo como cinta,DVD,CD o discos duros externos.

BASES DE DATOS
Conjunto de datos perteneciente a un mismo contexto almacenados sistemáticamente.

.ZIP, .RAR
Formato para manejo de archivos comprimidos.

ARCHIVOS LOG
Es un registro oficial de eventos durante un rango de tiempo en particular, es usado para registrar datos o información sobre quién, que, cuando, donde y por qué (who,what,when,where y why).

5. Descripción de Actividades Realización del Backup

1. Identificación de Bases de Datos. El administrador de base de datos determina e identifican los archivos a generar para respaldar las diferentes bases de datos.

Se identifica el número de bases de datos para respaldo, en este caso se identifican SIREDB, SICAP, SICAPITAL y SICAPDES. Se utiliza el formato “Backup de base de datos Oracle””.

Determinar Tipo de Backup:
Se determinan los mecanismos de copias de respaldo según la base de datos a respaldar de forma manual.

Para cada una de las bases de datos se explica que tipo de backup se va agenerar:

SIREDB= Base de datos que está en modo NO Archivelog, por lo tanto se genera export full de la base de datos a manera de backup.

La ubicación de este archivo está en:
/exports2/siredb en el servidor de bases de datos.

1. Conectarse vía Mobaxterm o SSH con el usuario Oracle.

2. Una vez conectado teclear . ./.pro_db1

3. Se debe instanciar la base de datos SIREDB. Con el comando:

   Export PATH=$ORACLE_HOME/bin:$PATH
   Expd usuarios/clave@siredb schemas=.dmp logfile=$_sire_210418.log

4. Una vez instanciada la BD, se lanza el comando que genera el export de la base de datos.

   Export PATH=$ORACLE_HOME/bin:$PATH
   Expd usuarios/clave@siredb schemas=sire directory=EXPORT2 dumpfile==$_sire_210418 logfile=$_sire_210418.log

5. El archivo queda en la ubicación mencionada anteriormente..

SICAPDES= Base de datos que está en modo NO Archivelog, por lo tanto se genera export full de la base de datos a manera de backup.

La ubicación de este archivo esta en:
/exports2/sicapitaldes del servidor BD

Se genera con los siguientes pasos.

1. Conectarse vía Mobaxterm con el usuario de administración de las instancias.

2. Una vez conectado teclear . ./.pro_db1

3. Se debe instanciar la base de datos SICAPDES.

4. Una vez instanciada la BD, se lanza el comando que genera el export de la base de datos.

5. El archivo queda en la ubicación mencionada anteriormente.

SICAP= Base de datos que está en modo archive Archivelog, por lo tanto SI se genera backup consistente con RMAN.

La ubicación de este archivo esta en:
/exports2/sicapitaldes del servidor de base de datos

Se genera con los siguientes pasos.

1. Conectarse vía Mobaxterm con el usuario para administración de instancias.

2. Una vez conectado teclear . ./.pro_db1

3. Se debe instanciar la base de datos SICAP.

4. Se debe ingresa a RMAN y se conecta con la base SICAP.

5. Luego se lanza la instrucción del backup:

```
connected to target database: SICAP (DBID=2913207261)

RMAN> backup database format "/exports2/sicap/bckf_%sicap_%t" plus archivelog;
```

6. Una vez termine el backup de desconecta el usuario de RMAN, con la sentencia exit y entramos a SQL PLUS.

7. Estando en sql plus, lanzamos

```
Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.4.0 - 64bit Production
With the Partitioning, Real Application Clusters, Automatic Storage Management, Orac
le Label Security,
OLAP, Data Mining, Oracle Database Vault and Real Application Testing options

SQL>
SQL> ALTER DATABASE BACKUP CONTROLFILE TO '/exports2/sicap/ctr_sicap21042018.bkp';
```

Para estos se utiliza Bitácora Backups Bases de Datos.

Verificar los Archivos Resultado del Backup: Se verifica que los archivos se hayan generado bien y se actualiza la bitácora de control.

2. Revisa Archivos y Pasa a Medio Externo. El Administrador Infraestructura Tecnológica verifica el tamaño de los archivos y genera el paso a almacenamiento externo.

3. Verificación de Archivos OK en Medio Externo. El Administrador Infraestructura Tecnológica Realiza una copia de prueba del archivo externo a otro medio y se asegura que loa backups se puedan recuperar.

Control de Cambios.

Versión	Fecha	Descripción de la Modificación	Aprobado por
1		Elaboración inicial del instructivo	Margarita Buitrago - SDAI Nelson Rincon Martinez- CPL
2	21/04/2018	Se adicionan pantallazos.	Karen Cervantes

Aprobación.

Elaborado por	Validado por	Aprobado por
Alejandro Aguirre Álvarez Contratista	Karen Cervantes Líder Infraestructura Claudia Patricia Albornoz Jaque Profesional Oficina Asesora de Planeación	David Giovanni Flórez Reyes Jefe Oficina TIC Jorge Enrique Angarita López Jefe Oficina Asesora de Planeación

Nota: Para una mayor información referente a este documento comunicarse con la dependencia responsable.