


# MANUAL DE COPIAS DE SEGURIDAD Y RECUPERACIÓN

| CÓDIGO: | 2310200-MA-002 | VERSIÓN: | 03 | PÁGINA: | 1 de 23 |
|---|---|---|---|---|---|

# HOSPITAL DONALDO SAUL MORON MANJARREZ MUNICIPIO DE LA JAGUA DEL PILAR – LA GUAJIRA.

# MANUAL DE POLÍTICA DE

# COPIAS DE SEGURIDAD Y RECUPERACIÓN

# MANUAL DE COPIAS DE SEGURIDAD Y RECUPERACIÓN



## CONTENIDO


Pág.

1. INTRODUCCIÓN 4
2. OBJETIVOS 4
2.1. Objetivo General 4
3. DEFINICIONES 4
4. COPIAS DE SEGURIDAD Y RECUPERACIÓN EN DESASTRES 7
4.1. Pruebas de Restauración de Backup 7
5. HERRAMIENTA DE BACKUP 8
6. TIPOS DE BACKUP 8
6.1. Estrategias de Backup 9
7. CONSIDERACIONES AL PLAN DE BACKUP 11
8. INFORMACIÓN QUE SE DEBE RESPALDAR 12
9. BACKUP DE DATOS DEL SYSTEM STATE, CONTROLADORES DE DOMINIO, APLICATIVOS, SITIO WEB INSTITUCIONAL Y BASES DE DATOS DE APLICATIVOS 12
9.1. Controladores de dominio 14
9.2. Bases de Datos 14
9.3. Aplicativos Web 15
9.4. Repositorio de Información de las áreas de la Entidad 15
9.5. Portal Web e Intranet 15
10. PROCESO DE COPIA A CINTA 16
11. PLAN DE COPIAS DE SEGURIDAD

11.1. Backup Bases de Datos (Oracle) 17
11.2. Backup de la configuración de los Servidores 19
11.3. Backup de Buzones 19
11.4. Backup de Aplicaciones WEB 20
11.5. Repositorio de Información de las áreas 20
12. ESQUEMA DE BACKUPS
12.1. Realización de Backups y tipo 21
21
13. PROCESO DE ALMACENAMIENTO DE LOS BACKUPS DE BASE DE DATOS, APLICATIVOS Y REPOSITORIO 22

# MANUAL DE COPIAS DE SEGURIDAD Y RECUPERACIÓN



## 1. INTRODUCCIÓN

Los capítulos que conforman este documento corresponden al esquema de copias de respaldo y restauración de información, que posee el Hospital Donaldo Saul Morón Manjarrez del Municipio de La jagua del pilarla Guajira en sus actuales servidores y servicios que corren sobre estos.

La Oficina de Tecnologías de la Información y las Comunicaciones de ESE Hospital Donaldo Saul Moron Manjarrez, se encargará de proteger y garantizar que los recursos del sistema de información (Aplicaciones y Bases de Datos) de la entidad, se mantengan respaldados y sean fácilmente recuperables en el momento que se necesite.

## 2. OBJETIVOS

### 2.1. Objetivo General

Se tiene un esquema de copias de seguridad de los Servicios, Aplicaciones y Bases de Datos de ESE Hospital Donaldo Saul Moron Manjarrez, que vayan de la mano con el Plan de contingencia para evitar un posible desastre que llegase a ocurrir y que de alguna manera la entidad pueda recuperase a tal eventualidad.

### a. Objetivos Específicos

- Diseñar el esquema de backups que debe poseer ESE Hospital Donaldo Saul Moron Manjarrez.
- Explicar cómo funciona el esquema de backups dentro ESE Hospital Donaldo Saul Moron Manjarrez.
- Explicar los diferentes backups que se dan al interior ESE Hospital Donaldo Saul Moron Manjarrez.
- Explicar a qué se le debe realizar respaldo.
- Cómo funciona el esquema de respaldos y de custodia.




## 3. DEFINICIONES

**Backup (Copia de Respaldo o Seguridad):** Copia de seguridad de los archivos, aplicaciones y/o bases de datos disponibles en un soporte magnético (generalmente discos extraíbles, unidades de cinta), 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 y verificación de las mismas a intervalos temporales fijos (diario o semanal, por ejemplo), en función del trabajo y de la importancia de los datos manejados.

**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.

**Cinta LTO7-FC:** Linear Tape-Open es una tecnología de cinta magnética (unidad de cinta) de almacenamiento de datos, se creó como una tecnología de "formato abierto" para que los usuarios tuviesen múltiples fuentes de productos y media.

**Contingencia:** Conjunto de procedimientos de recuperación. Las acciones a contemplar aplican para Antes- Durante- Después con el fin de reducir las pérdidas.

**DataSet**: es una representación de datos residente en memoria que proporciona una modelo de programación relacional coherente independientemente del origen de datos que contiene. El DataSet contiene en sí, un conjunto de datos que han sido volcados desde el proveedor de datos.

**Hosting**: Alojamiento web (en inglés web hosting) es el servicio que provee a los usuarios de Internet un sistema para poder almacenar información, imágenes, vídeo, o cualquier contenido accesible vía Web.

**Librería de Cintas Sun Storagetek SL150**: La biblioteca de cintas modular SL150 está diseñada para funcionar automáticamente, bajo el control de una aplicación de gestión de copia de seguridad, archivo, almacenamiento o residente en host, como Oracle Secure Backup. En circunstancias normales, la biblioteca SL150 requiere poca o ninguna intervención del operador. Las unidades robóticas de la biblioteca controlan todo el movimiento de los cartuchos dentro de la biblioteca bajo el control de la aplicación. Los catálogos de almacenamiento de la aplicación host permanecen constantes y rara vez requieren auditorías físicas del contenido de la biblioteca.

**Log ("registro", en español):** es un archivo de texto en el que constan cronológicamente los acontecimientos que han ido afectando a un sistema informático (programa, aplicación, servidor, etc.), así como el conjunto de cambios que estos han generado.

**Oracle RAC (Real Application Cluster):** Es una arquitectura de base de datos de "uso compartido global" en la que dos o más nodos de Oracle RAC se agrupan en clúster y comparten el mismo almacenamiento.

**Oracle Secure Backup 12.1**: Software de respaldo configurado para operar hacia una librería de cintas Sun StorageTek SL150 con dos unidades de cinta tipo LTO7-FC.

**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, aun cuando algunas de sus funciones se vean afectadas por un accidente interno o externo.

**RMAN:** Herramienta de copia de seguridad de Oracle, para entornos de BBDD en clúster y muy eficaz en entornos de instancia única. En este artículo conoceremos sus políticas de retención.

**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.

**Repositorio de información:** Un repositorio es un espacio centralizado donde se almacena, organiza, mantiene y difunde información digital, habitualmente archivos informáticos, que pueden contener información importante de una entidad.

**Respaldo**: Es la copia de información a un medio del cual se pueda recuperar y restaurar la información original.

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

**Servidor**: Se utiliza para referirse al ordenador físico en el cual funciona ese software, una máquina cuyo propósito es proveer datos de modo que otras máquinas puedan utilizar esos datos.

**Sistemas de Información**: Es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad u objetivo.

**Snapshot (foto instantánea):** Es una instantánea del estado de un sistema en un momento determinado. El término fue acuñado como una analogía a la de la fotografía

## 4. COPIAS DE SEGURIDAD Y RECUPERACIÓN EN DESASTRES

Una de sus funciones más esenciales es asegurar que nunca se pierdan la información de la entidad y que las aplicaciones estén disponibles, a pesar de caídas del servidor, apagones o desastres naturales. No sólo se debe hacer copia de seguridad de la información, también se debe verificar que dichas copias son "recuperables" y, además, que se pueda hacer en un intervalo concreto de tiempo.
La entidad dispone de una plataforma web que permite consultar el informe de las copias de seguridad para verificar que el backup que se ha llevado a cabo correctamente. De esta manera nos aseguramos de que todo ha ido bien, y que si le pasa algo a nuestros datos (un borrado accidental, una infección por virus/troyanos/malware) podamos recuperar una versión reciente de nuestros datos.

### 4.1. Pruebas de Restauración de Backup

Como medida de protección durante el año se harán pruebas de las cintas de backup que se resguardan al interior de Oficina de Tecnologías de la Información y las Comunicaciones de ESE Hospital Donaldo Saul Moron Manjarrez.

Las pruebas de Restore se realizan mensual y se ha definido los siguientes periodos:

- Se realizarán pruebas de restore cada mes para las bases de datos en un servidor de pruebas.
- Cuando sea necesario restaurar información para la implementación de ambiente de pruebas.

Se verificará posteriormente que el respaldo a cinta se esté ejecutando de forma correcta y/o que la restauración de la información se haya ejecutado, revisando el log que genera la restauración de información en bases de datos, para verificar que se haya ejecutado satisfactoriamente, en caso de no restaurar correctamente, se deberá tomar el backup anterior a la fecha del restaurado.

Con el fin de verificar las copias de respaldo cada mes, se realizarán pruebas de restauración de la información almacenada en las cintas. Se escogerá de forma aleatoria una cinta de backup de bases de datos y se restaurará para validar que la información almacenada se registre de forma correcta en un servidor de pruebas para tal fin, posteriormente será validada por el responsable funcional.

En cuanto a la Copia Diaria de las aplicaciones web, esta copia todos los archivos seleccionados que han sido modificados en el día que se haya realizado, permitiendo que la copia este sincronizada con los

aplicativos de producción, en caso de que estos presenten algún inconveniente técnico, se activa la copia de los aplicativos sin interrumpir el servicio.
En caso de presentarse inconvenientes se debe revisar directamente el servidor desde el que se realizó el backup.

## 5. HERRAMIENTA DE BACKUP

La herramienta a utilizar cuenta con una librería (Robot) Sun StorageTek SL150 y un software de copias de respaldo (backups) Oracle Secure Backup 12.1, para la realización de los respaldos de información de la entidad. Esta herramienta se utiliza con el fin de realizar backups a las Bases de Datos Oracle.

La biblioteca de cintas modulares StorageTek SL150 de Oracle es la primera biblioteca de cintas escalables diseñado para negocios en crecimiento. Construido a partir del software Oracle y la biblioteca StorageTek tecnología, ofrece una combinación líder en la industria de facilidad de uso y escalabilidad. Ideal para aplicaciones de copia de seguridad y archivado, la biblioteca de cintas modulares StorageTek SL150 ahorra tiempo y dinero, estableciendo el nuevo estándar para la automatización de cintas de entrada.
Oracle Secure Backup 12.1 Software de respaldo configurado para operar hacia una librería de cintas Sun StorageTek SL150 con dos unidades de cinta tipo LTO7-FC.

En cuanto a la copia de respaldo de las aplicaciones se realiza desde el S.O. sincronizando los servidores de aplicaciones con el servidor de backup en el Centro de Cómputo.
Para los servidores se realizará un backup de la configuración inicial o snapshot del sistema o de una parte que permiten recuperar en un estado que se sabe que es correcto.

## 6. TIPOS DE BACKUP

Los backups se pueden dividir en varios tipos como son los siguientes:

- Un ***Backup Normal,*** copia todos los archivos seleccionados y marca cada uno como un backup normal. Para la restauración es solamente necesario el más reciente backup realizado.

- Un ***Backup Incremental***, realiza backup solamente a los archivos que fueron creados o modificados desde el último backup normal o incremental. Esta marca solamente los archivos que se les ha realizado backup. Al utilizar una combinación de backups normales e increméntales es necesario

para la restauración tener el último backup normal y todo el set de backups increméntales hasta la fecha.

- Un ***Backup Diferencial***, copia los archivos creados o modificados desde el último backup normal o incremental. Este no marca los archivos como si se le hubiera realizado backup. Si se tiene una combinación de backups normales y diferenciales; para la restauración es necesario tener el último backup normal y el set de backups diferenciales.

- Un ***Backup Copia***, copia todos los archivos seleccionados, pero no marca los archivos como si se le hubiera hecho backup. Este backup no afecta otros tipos de backup.

- Un ***Backup Diario***, copia todos los archivos seleccionados que han sido modificados en el día que se haya realizado el backup. Los archivos no son marcados.

Con la herramienta de software se posee más flexibilidad con los backups ya que se envían a cinta.

**6.1. Estrategias de Backup**

Una buena estrategia de backup es la mejor defensa contra la perdida de datos. Las tres estrategias comunes de backup son las siguientes:

- **Copia de seguridad completa o normal:** Una copia normal no es más que un backup completo de todos los archivos seleccionados en el plan de copias. Cada vez que se realiza una copia normal, el sistema operativo pone el bit de copia del archivo salvaguardado (también llamado bit de modificación) a 0, para identificar que se le ha realizado un respaldo, o que el archivo no ha sido modificado desde la última copia de seguridad que se le realizó. Este bit volverá a 1 en el momento en que el archivo sea modificado.

- **Copia completa semanal y una incremental diaria:** Se trata del tipo de copia que menos capacidad necesita, por volumen de copia, ya que solo almacenará la información que haya sido modificada desde la última copia de seguridad realizada, ya sea completa, diferencial o incremental, da lo mismo. Además, evidentemente, también se trata del proceso de backup más rápido en realizarse. El principal inconveniente que tiene este mecanismo es que, para lograr una restauración en un momento determinado, se necesitarán todos los conjuntos de medios incrementales hasta llegar a la última copia diferencial o completa realizada, además de éstas últimas. Igualmente, será el propio software de backup el que nos pida los diferentes volúmenes y los catalogue antes de proceder a su restauración,

por lo que el proceso será bastante transparente para el administrador, antes de disponer de nuevo de toda la información.

- **Copia completa semanal y una diferencial diaria:** Se realiza una copia de seguridad de todos los cambios realizados desde la última copia de seguridad completa. Es mucho más rápida y requiere menos espacio de almacenamiento que una copia de seguridad completa, pero más que una copia de seguridad incremental. Las restauraciones son más lentas que con una copia de seguridad completa, pero más rápidas que con copias de seguridad incrementales.

Para el caso de ESE Hospital Donaldo Saul Moron Manjarrez, donde la estructura de la red y la administración es centralizada, se deberá realizar una copia completa semanal y una diferencial diaria, donde se encuentre la información de los sistemas misionales y administrativos de la entidad.

Se contará con las siguientes estrategias de copias de seguridad, dependiendo de la función que realice cada uno de los servidores miembros del dominio de ESE Hospital Donaldo Saul Moron Manjarrez.

La estrategia de Copias de Seguridad, es fundamental para mantener la disponibilidad de la información, y en Windows 2012 Server y Centos Linux release 7, no es la excepción.

En esta sección se describirá la estrategia de Copias de Seguridad propuesta para la infraestructura de Windows 2012 Server y Centos Linux release 7.

Se realizarán las copias de seguridad diarias diferenciales y los sábados son backups Full para las bases de datos.

Esta estrategia permitirá realizar una recuperación de inmediato cuando se presente un daño, por motivos muy diversos, desde infecciones del sistema por virus y malware, fallos de hardware (cortes de corriente y picos de tensión, excesos de temperatura y daños en los dispositivos), apagados incorrectos del equipo, problemas motivados por algún programa, daños del usuario al borrar archivos por error, etc.

Es por eso, que la Secretaria Jurídica Distrital cuenta con 3 capas de backup así: Un PC con cuatro discos duros de 4 Teras, Servidor en Secretaría General, el Sun StorageTek SL150 (Robot) y un software de copias de respaldo (backups) Oracle Secure Backup 12.1.

Por lo tanto, en el PC con cuatro discos duros de 4 Teras se almacena los backups de Base de datos, SIGA (imágenes), Aplicativos Misionales y Administrativos.

La entidad cuenta con un servidor denominado “bogotajuridica”, el cual se encuentra ubicado en el datacenter de la Secretaría General de la Alcaldía Mayor de Bogotá y está amparado ante un convenio entre las dos Entidades y posee un disco de 6TB en el cual se realizan backups de base de datos, base de datos históricas, contenedor de expedientes y contenedor de Imágenes de Gestión documental, como un plan alterno en caso de presentarse algún evento que pueda afectar el Datacenter de la Secretaria Jurídica Distrital y poder recuperar y dar disponibilidad de la información en corto tiempo, en este servidor se tiene una tarea programada que se encarga de sincronizar las siguientes actividades:

- Contenedor del servidor de aplicaciones misional y administrativas.
- Imágenes de SIGA.
- Backups de Oracle.

Los backups se realizan todos los días en distintos horarios y son de tipo incremental para ser eficientes en el uso del espacio de disco duro.En el caso de la base de datos se toman los backups del servidor principal en el directorio /u03/backups. Para el caso del aplicativo de SIGA (Sistema de Gestión Documental) se sincronizan la data del directorio
/imágenes, para hacer la copia de las imágenes que se almacenan en el aplicativo.

Para el caso de los aplicativos misionales, contenedor del servidor de aplicaciones misional y administrativas /contenedor/* /backups/contenedor.

## 7. CONSIDERACIONES AL PLAN DE BACKUP

Cuando se desarrolla un plan de backup se debe tener en cuenta lo siguiente:

- Determinar el tipo de información a ser resguardada, lo que indica que cada copia debe estar debidamente identificada respecto a la información que debe contener.

- Prever los aspectos relacionados con la fiabilidad de la copia, ya que se debe garantizar la integridad de los archivos a ser copiados y de los soportes a utilizar.

- Incluir una prueba de tensión del hardware de backup (unidades de almacenamiento, unidades ópticas y controles) y del software (programas de backup y unidades de dispositivo).

- Establecer las políticas de seguridad con los responsables para el acceso a las copias, así como la protección física del lugar donde están almacenados.

## 8. INFORMACIÓN QUE SE DEBE RESPALDAR

- Los servidores que manejan aplicaciones web.
- Las bases de datos de los que soporten aplicaciones de ESE Hospital Donaldo Saul Moron Manjarrez.
- Los Controladores de Dominio y de DHCP.
- Repositorio de información asignado a las áreas para el almacenamiento de información.
- Portal Web y cuentas de correo

**Nota:**
En los casos en que ESE Hospital Donaldo Saul Moron Manjarrez contrate la provisión o infraestructura que soporte alguna de la información mencionada anteriormente, se deberá asegurar que el TERCERO cumpla con la política descrita en el presente manual.

## 9. BACKUP DE DATOS DEL SYSTEM STATE, CONTROLADORES DE DOMINIO, APLICATIVOS, SITIO WEB INSTITUCIONAL Y BASES DE DATOS DE APLICATIVOS

ESE Hospital Donaldo Saul Moron Manjarrez, cuenta con una librería (Robot) y un software de copias de respaldo Oracle Secure Backup 12, para la realización de los respaldos de la información crítica de la entidad, almacenada en los servidores de la red de datos. Estos se realizarán todos los días, mediante una tarea programada a través del software de copias de respaldo instalado y configurado en la entidad para este propósito.

### a. Frecuencia de las Copias de Respaldo

Se deben realizar todos los días ya que se cuenta con una librería (robot) de última generación, ya que estas cuentan con un magazine (slots) que permiten guardar varias cintas y si se requiere cambio de una cinta o varias se puede hacer en horas laborables.

Para la base de datos misional, se genera un Backup Full todos los jueves a la 1:21 a.m., y los backup de archives (backups diferenciales) todos los días a las 9:20 a.m., 12:20 a.m., 14:20 p.m. y 7:20 p.m.

Para la base de datos administrativa (aplicativos administrativos) se genera un Backup Full todos los sábados a las 10:32 a.m. y backup de archives (backups diferenciales) todos los días a las 9:43 a.m., 12:43 a.m., y 18:43 p.m. el nombre de la tarea de agendamiento es: Agenda-Full_Admjurup.

**b. Configuración de la Copia de Respaldo**

Será realizada por el administrador de la red de datos y este a su vez será el responsable directo de la recuperación de la información en caso que se requiera. Para tal fin, debe utilizar el software de copias de respaldo adquirido por la entidad.

El System State es la configuración del sistema; este varía dependiendo del rol de la máquina Windows 2012 Server y Centos Linux releáse 7 (si es DC, Cluster entre otros). Es muy importante el backup del System State, ya que sobre él se encuentra la configuración de los servidores y estaciones.

Los datos del System State están comprendidos por los siguientes archivos:

- Los archivos Boot, incluyendo los archivos del sistema, y todos los archivos protegidos por Windows File Protección (WFP).
- El Directorio Activo (en un controlador de dominio solamente).
- Sysvol (en un controlador de dominio solamente).
- Servicio de Certificados (en autoridades de certificación solamente).
- Base de datos Cluster (en un nodo del Cluster, solamente donde se encuentre el servicio).
- El registro.
- Información del contador de configuración del desempeño.
- Base de datos de registro de las clases de servicio del Componente.

A los datos del System State se les puede realizar backup en cualquier orden. La restauración del System State remplaza los archivos de Boot primero y confía en la carga del registro del sistema como paso final en el proceso.

La operación de Backup y Restore del System State incluye todos los datos del sistema: No se le puede seleccionar al backup o al Restore componentes individuales debido a la dependencia entre los componentes del System State. Sin embargo, se puede restaurar los datos del System State en una localización alterna en la cual solamente los archivos de registro, el directorio de archivos del Sysvol, y el sistema de archivos de Boot son restaurados.

La base de datos del Directorio Activo, la base de datos del servicio de certificado, y la base de datos de los componentes de servicios de clases registradas no son restauradas en una localización alterna.

Se recomienda hacer una copia de seguridad del System State sobre un archivo en el disco duro, para que desde un servidor que tenga unidad de cinta a través de la red se realice el backup a este archivo.

### 9.1. Controladores de dominio

Dada la funcionalidad que tienen el servidor como Controlador de Dominio, de la entidad se recomienda para proteger el directorio activo, realizar copias de seguridad regulares del “System State”, adicionalmente antes de instalar un nuevo driver o una nueva aplicación se debe actualizar el disco de reparación de sistema, una vez comprobada la correcta funcionalidad del servidor se debe actualizar nuevamente el disco de reparación.

Las copias de seguridad en el servidor donde se encuentran el Controlador de Dominio se deberán realizar de acuerdo a la siguiente plantilla:

| Backup | System State (Controladores de Dominio) |
|---|---|
| **Cada 15 días** | **X** |

### 9.2. Bases de Datos

El Plan de Backups diarios se efectuarán de forma automática, agendándolos por horas de acuerdo a los criterios definidos por la Oficina de Tecnologías de la Información y las Comunicaciones así:

| Base de Datos | Tipo de backup | Días | Horario |
|---|---|---|---|
| **Misional** | Diferencial | Todos los días | 9:20 a.m.<br>12:20 a.m.<br>14:20 p.m.<br>7:20 p.m. |
| | Full | Jueves | 1:21 a.m. |
| **Administrativa** | Diferencial | Todos los días | 9:43 a.m.<br>12:43 a.m.<br>18:43 p.m. |
| | Full | Sábados | 10:32 a.m. |

ESE Hospital Donaldo Saul Moron Manjarrez, cuenta con una librería (Robot) Sun StorageTek SL150, tape externos y un software de copias de respaldo (backups) Oracle Secure Backup 12, para la realización de los respaldos de la información crítica de la entidad, almacenada en los servidores de la red de datos. Estos se realizarán todos los días, mediante una tarea programada a través del software de copias de respaldo instalado y configurado en la entidad para este propósito.

### 9.3. Aplicativos Web

La entidad posee aplicativos web, los cuales son programas diseñados para o por los usuarios para facilitar la realización de tareas específicas en la computadora, sistemas de gestión de base de datos como los misionales y administrativos.

Se posee un plan de backup diario que se generan automáticamente a partir de las 2:00 a.m., se realiza un backup full, el cual se guarda en el servidor de backups.

### 9.4. Repositorio de Información de las áreas de la Entidad

La entidad provee a las áreas una cuota de almacenamiento para estas con capacidad de 20 Gb, este espacio asignado es para almacenar los datos y archivos relevantes para el funcionamiento de las áreas, dicho repositorio se suministra a través de una unidad de RED almacenada en un Servidor creado para este fin.

Se posee un Plan de Backups diarios diferenciales para la base de datos Misional que se generan automáticamente en los siguientes horarios 9:20 a.m., 12:20 a.m., 14:20 p.m. y 7:20 p.m., y el Backup Full que se genera el el jueves a las 1:21 a.m., para la base de datos Administrativa se generan backups diferenciales todos los días a las 9:43 a.m.,12:43 a.m. y 18:43 p.m., y backup Full todos los sábados a las 10:32 a.m.

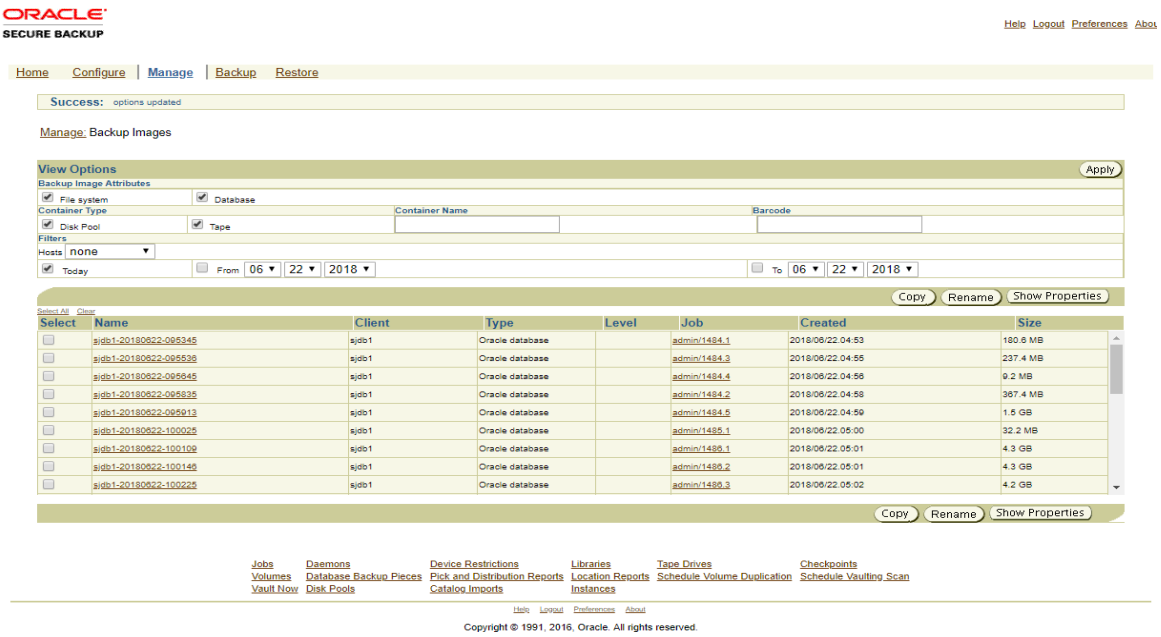
### 9.5. Portal Web e Intranet

Generar respaldos semanales (backup) del Portal Institucional e Intranet de la Secretaria Jurídica Distrital los cuales se deben almacenar en un repositorio de información.

## 10. PROCESO DE COPIA A CINTA

Los Backups que se generan de las bases de datos se almacena en cintas tipo LTO7-FC, proceso que se debe configurar en el software de respaldo Oracle Secure Backup 12.1, para la automatización de las tareas de respaldo de las Bases de Datos, la cual opera hacia la librería de cintas.

Desde el software de respaldo Oracle Secure Backup 12.1, se asigna a cada cinta LTO7-FC un código para su identificación, además el software cuenta con un reporte denominado Backup Images, que permite identificar el nombre del backup, cliente, tipo, fecha y hora de creación y peso.




# MANUAL DE COPIAS DE SEGURIDAD Y RECUPERACIÓN



## 11. PLAN DE COPIAS DE SEGURIDAD

La estrategia de backups corresponde a los backups de la configuración de servidores, Aplicaciones Web y Bases de Datos; estos backup se hacen a través de una librería (Robot) y un software de copias de respaldo (backups).

### 11.1. Backup Bases de Datos (Oracle)

Inicialmente se debe configurar e implementar el sistema de respaldo Oracle Secure Backup con la librería de cintas Sun StorageTek SL150.

Para ello se debe realizar una configuración general de la Librería de cintas SL150, de la red de administración, la configuración de Unidades de cinta y cargar los cartuchos de cinta.
Una vez realizadas estas actividades se ingresa a la plataforma de Oracle Secure Backup para configurar los dispositivos y se configura la librería de cintas en Oracle Secure Backup, una vez realizada esta configuración se puede revisar el listado de cintas identificados por el sistema de respaldo.




Luego se configura el dataset que se respalda en la política “ASR-Backup”, el filesystem llamado “/backup” en el servidor de ASR Manager, este respaldo se almacena en un grupo de cintas (Media Family) llamado “Filesystems”.

El Filesystem es configurado para ser respaldado en cintas a la base de datos de Misional todos los jueves a las 1:21 a.m., y para la base de datos Administrativa se generan todos los sábados a las 10:32 a.m.
Después se configura el respaldado RMAN para RAC, configurando un Database Backup Storage Selector denominado “RAC_RMAN”, para el enlace de la librería Oracle Secure Backup SBT, en cada uno de los nodos del ORACLE RAC. Se realiza una prueba de conectividad hacia los dos nodos de la base de datos del ORACLE RAC desde Oracle Secure Backup.

Queda habilitado el respaldo automático del catálogo de indexación de respaldo de Oracle Secure Backup a unidades de cinta. Este respaldo permite una rápida recuperación del sistema de respaldo de Oracle Secure Backup y es adicional al respaldo de Filesystems del servidor.

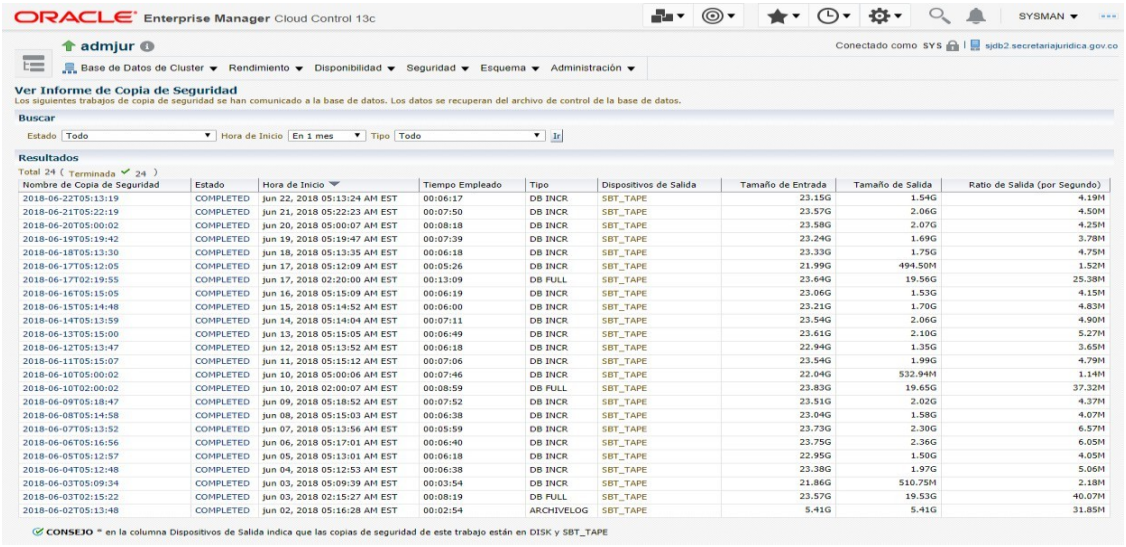
Para las Bases de Datos se genera una (1) cinta de backup respectivamente, todos los backups de Base de datos son Full backup.

Los backup son generados diariamente en el sistema de almacenamiento, pero solo se guarda como histórico el backup del día sábado para posterior restauración en caso de ser necesario.

| Backup | Normal | Histórico |
|---|---|---|
| **Lunes** | **X** | |
| **Martes** | **X** | |
| **Miércoles** | **X** | |
| **Jueves** | **X** | **X** |
| **Viernes** | **X** | |
| **Sábado** | **X** | **X** |
| **Domingo** | **X** | |
| **Nota** | **Todos los días se realiza backup diferenciales de la base de datos Misional todos los días a las 9:20 a.m., 12:20 a.m., 14:20 p.m., y 7:20 p.m., y de la base de datos administrativa se generan todos los días a las 9:43 a.m., 12:43 a.m., y 18:43 p.m.**<br><br>**El backup Full para la base de datos Misional se realiza todos los jueves a las 1:21 a.m., y para la base de datos administrativa los sábados a las 10:32 a.m.** | |

En la plataforma de Oracle Secure Backup en el menú Manage en la opción Backup Images, el administrador podrá generar un informe para verificar que se hayan realizado los backups en un periodo de tiempo determinado, además por la plataforma de Oracle Enterprise Cloud Control 13cen el menú Disponibilidad existe una opción denominada “Copia de Seguridad y Recuperación” la cual permite verificar que se hayan realizado los backups a diario en un mes determinado.

Se posee un Plan de Backups diarios que se generan automáticamente para la base de datos Misional todos los días a las 9:20 a.m.,12:20 a.m.,14:20 p.m., y 7:20 p.m., que es diferencial y el backup full que se genera el jueves a las 1:21 a.m., y para la base de datos administrativa se generan backups diferenciales todos los días a las 9:43 a.m.,12:43 a.m., y 18:43 p.m., y backup full todos los sábados a las 10:32 a.m.




| Nombre de Copia de Seguridad | Estado | Hora de Inicio | Tiempo Empleado | Tipo | Dispositivos de Salida | Tamaño de Entrada | Tamaño de Salida | Ratio de Salida (por Segundo) |
|---|---|---|---|---|---|---|---|---|
| 2018-06-22T05:13:19 | COMPLETED | jun 22, 2018 05:13:24 AM EST | 00:06:17 | DB INCR | SBT_TAPE | 23.15G | 1.54G | 4.19M |
| 2018-06-21T05:22:19 | COMPLETED | jun 21, 2018 05:22:23 AM EST | 00:07:50 | DB INCR | SBT_TAPE | 23.57G | 2.06G | 4.50M |
| 2018-06-20T05:00:02 | COMPLETED | jun 20, 2018 05:00:07 AM EST | 00:08:18 | DB INCR | SBT_TAPE | 23.58G | 2.07G | 4.25M |
| 2018-06-19T05:19:42 | COMPLETED | jun 19, 2018 05:19:47 AM EST | 00:07:39 | DB INCR | SBT_TAPE | 23.24G | 1.69G | 3.78M |
| 2018-06-18T05:13:30 | COMPLETED | jun 18, 2018 05:13:35 AM EST | 00:06:18 | DB INCR | SBT_TAPE | 23.33G | 1.75G | 4.75M |
| 2018-06-17T05:12:05 | COMPLETED | jun 17, 2018 05:12:09 AM EST | 00:05:26 | DB INCR | SBT_TAPE | 21.99G | 494.50M | 1.52M |
| 2018-06-17T02:19:55 | COMPLETED | jun 17, 2018 02:20:00 AM EST | 00:13:09 | DB FULL | SBT_TAPE | 23.64G | 19.56G | 25.38M |
| 2018-06-16T05:15:05 | COMPLETED | jun 16, 2018 05:15:09 AM EST | 00:06:19 | DB INCR | SBT_TAPE | 23.06G | 1.53G | 4.15M |
| 2018-06-15T05:14:48 | COMPLETED | jun 15, 2018 05:14:52 AM EST | 00:06:00 | DB INCR | SBT_TAPE | 23.21G | 1.70G | 4.83M |
| 2018-06-14T05:13:59 | COMPLETED | jun 14, 2018 05:14:04 AM EST | 00:07:11 | DB INCR | SBT_TAPE | 23.54G | 2.06G | 4.90M |
| 2018-06-13T05:15:00 | COMPLETED | jun 13, 2018 05:15:05 AM EST | 00:06:49 | DB INCR | SBT_TAPE | 23.61G | 2.10G | 5.27M |
| 2018-06-12T05:13:47 | COMPLETED | jun 12, 2018 05:13:52 AM EST | 00:06:18 | DB INCR | SBT_TAPE | 22.94G | 1.35G | 3.65M |
| 2018-06-11T05:15:07 | COMPLETED | jun 11, 2018 05:15:12 AM EST | 00:07:06 | DB INCR | SBT_TAPE | 23.54G | 1.99G | 4.79M |
| 2018-06-10T05:00:02 | COMPLETED | jun 10, 2018 05:00:06 AM EST | 00:07:46 | DB INCR | SBT_TAPE | 22.04G | 532.94M | 1.14M |
| 2018-06-10T02:00:02 | COMPLETED | jun 10, 2018 02:00:07 AM EST | 00:08:59 | DB FULL | SBT_TAPE | 23.83G | 19.65G | 37.32M |
| 2018-06-09T05:18:47 | COMPLETED | jun 09, 2018 05:18:52 AM EST | 00:07:52 | DB INCR | SBT_TAPE | 23.51G | 2.02G | 4.37M |
| 2018-06-08T05:14:58 | COMPLETED | jun 08, 2018 05:15:03 AM EST | 00:06:38 | DB INCR | SBT_TAPE | 23.04G | 1.58G | 4.07M |
| 2018-06-07T05:13:52 | COMPLETED | jun 07, 2018 05:13:56 AM EST | 00:05:59 | DB INCR | SBT_TAPE | 23.73G | 2.30G | 6.57M |
| 2018-06-06T05:16:56 | COMPLETED | jun 06, 2018 05:17:01 AM EST | 00:06:40 | DB INCR | SBT_TAPE | 23.75G | 2.36G | 6.05M |
| 2018-06-05T05:12:57 | COMPLETED | jun 05, 2018 05:13:01 AM EST | 00:06:18 | DB INCR | SBT_TAPE | 22.95G | 1.50G | 4.05M |
| 2018-06-04T05:12:48 | COMPLETED | jun 04, 2018 05:12:53 AM EST | 00:06:38 | DB INCR | SBT_TAPE | 23.38G | 1.97G | 5.06M |
| 2018-06-03T05:09:34 | COMPLETED | jun 03, 2018 05:09:39 AM EST | 00:03:54 | DB INCR | SBT_TAPE | 21.86G | 510.75M | 2.18M |
| 2018-06-03T02:15:22 | COMPLETED | jun 03, 2018 02:15:27 AM EST | 00:08:19 | DB FULL | SBT_TAPE | 23.57G | 19.53G | 40.07M |
| 2018-06-02T05:13:48 | COMPLETED | jun 02, 2018 05:16:28 AM EST | 00:02:54 | ARCHIVELOG | SBT_TAPE | 5.41G | 5.41G | 31.85M |

### 11.2. Backup de la configuración de los Servidores

Para proteger los controladores de dominio y el directorio activo se debe realizar la copia de seguridad del “System State” en el servidor (máquinas virtuales), con el fin de proteger la información de las cuentas de los usuarios vinculados a ESE Hospital Donaldo Saul Moron Manjarrez, se procederá a efectuar una copia completa de dicho repositorio (Directorio Activo) y, dada la baja actualización de información, se procederá a efectuar respaldos con una periodicidad quincenal.

### 11.3 Backup de Buzones

El esquema de backups corresponde a backups diarios lo realiza un tercero, toda vez que el servicio se contrata con un tercero, el cual debe garantizar que la información es respaldada, para que cuando sea necesario restablecer información esta se encuentre disponible.

Dentro del servicio que presta el tercero tiene como obligación la de respaldar la información de correos institucionales y el Portal Web de la entidad.
En este caso Google Vault permite conservar, retener, buscar y exportar datos para responder a las necesidades de archivado y descubrimiento electrónico de la entidad. Se puede utilizar Vault para gestionar la información de los siguientes elementos:

- Mensajes de correo electrónico.

- Chats de Hangouts que tengan el historial activado y chats de Google Talk con el registro habilitado.
- Grupos de Google.
- Archivos de Google Drive y de unidades de equipo.

Usos de Vault:

**Archivado:** puedes establecer reglas de retención para controlar durante cuánto tiempo se conservarán los datos hasta que se quiten de las cuentas de usuario y se eliminen de los sistemas de Google.

**Retenciones de datos con fines legales:** puedes aplicar retenciones a los usuarios para conservar sus datos de forma indefinida con el fin de cumplir tus obligaciones legales u otros requisitos de retención de datos.

**Búsqueda:** puedes buscar datos de tu dominio por cuenta de usuario, unidad organizativa, fecha o palabra clave. Vault admite búsquedas con operadores booleanos y comodín.
Exportación: puedes exportar datos para procesarlos y revisarlos con más detalle.

**Informes de auditoría:** utiliza los informes de auditoría de Vault para obtener información sobre las acciones que los usuarios de Vault han realizado durante un periodo especificado.

### 11.4 Backup de Aplicaciones WEB

Este Backup se realiza desde el S.O. sincronizando los servidores de aplicaciones con el servidor de backup en el Centro de Cómputo.

La Copia diaria Full de los Aplicativos Web, se encuentra en el Servidor de backup, el cual permite tener un espejo de la información, en caso de presentarse alguna catástrofe natural, o en caso de una pérdida material del hardware por cualquier otra causa siniestra, esta copia entra a reemplazar el servidor de producción y así no se interrumpe el servicio.

El backup es generado todos los días en el servidor de backup, la copia de seguridad se realiza a los archivos que se encuentran en el servidor que poseen configuradas las aplicaciones Web.

Se posee un plan de backup diario que se generan automáticamente a partir de las 2:00 a.m., se realiza un backup full, el cual se guarda en el servidor de backups.

### 11.5 Repositorio de Información de las áreas

Este Backup se realiza desde el S.O. Windows Server 2016 (Servidor IP 10.54.80.10) sincronizado con el servidor de backup en el Centro de Computo.

La Copia diaria de dicho repositorio, se encuentra en el Servidor de backup, el cual permite tener un espejo de la información, en caso de presentarse alguna catástrofe natural, o en caso de una pérdida material del hardware por cualquier otra causa siniestra, esta copia entra a reemplazar el servidor de producción y así no se interrumpe el servicio.

El backup es generado todos los días en el servidor de backup, la copia de seguridad se realiza a los archivos que se encuentran en la unidad (D:\).de almacenamiento del servidor.

Se posee un plan de backup diario que se generan automáticamente a partir de las 2:00 a.m., se realiza un backup full, el cual se guarda en el servidor de backups.

## 12. ESQUEMA DE BACKUPS

### 12.1. Realización de Backups y Tipo

| BACKUP TIPO DIFERENCIAL | | |
|---|---|---|
| | BDs Datos | Repositorio Áreas |
| Lunes | X | X |
| Martes | X | X |
| Miércoles | X | X |
| Jueves | X | X |
| Sábado | X | X |
| Domingo | X | X |

| BACKUP TIPO NORMAL (FULL) | | | | |
|---|---|---|---|---|
| | BDs Datos | Configuración Servidores | Aplicaciones Web | Repositorio Áreas |
| Lunes | | | X | |
| Martes | | | X | |
| Miércoles | | | X | |

| | | | | |
|---|---|---|---|---|
| **Jueves** | **X** | **Backup se realizará cada 15 días** | **X** | |
| **viernes** | | | | |
| **Sábado** | **X** | | **X** | |
| **Domingo** | | | **X** | **X** |

## 13. PROCESO DE ALMACENAMIENTO DE LOS BACKUP DE BASE DE DATOS, APLICATIVOS Y REPOSITORIO

Los backups diferenciales de base de datos son generados diariamente en el sistema de almacenamiento, estos se conservan en la cinta LTO 7 y el día ocho (8) se genera el backup diferencial y el backup full almacenados en la cinta.

En la plataforma de Oracle Enterprise Cloud Control 13c, en la opción denominada “Copia de Seguridad y Recuperación”, al consultar el informe de backups generados se puede identificar el nombre de la copia de seguridad, el estado del backup, la hora de inicio, tiempo empleado para la realización del backup, el tipo de backup diferencial o Full y el tipo de dispositivo de salida.

La Copia diaria Full de los Aplicativos Web, se encuentra en el Servidor de backup, la cual permite tener un espejo de la información, en caso de presentarse alguna catástrofe natural, o en caso de una pérdida material del hardware por cualquier otra causa siniestra, esta copia entra a reemplazar el servidor de producción y así no se interrumpe el servicio.