



**ALCALDÍA MAYOR
DE BOGOTÁ D.C.**
Secretaría Distrital de Seguridad,
Convivencia y Justicia

Proceso:

Gestión de Tecnologías de la
Información

Código:

PD-GT- 11

Versión:

1

Fecha Aprobación:

30/08/2019

Documento:

Generación de Backup Bases de
Datos

Fecha de Vigencia:

30/08/2019

Página 1 de 12

OBJETIVO

Asegurar la información de las bases de datos de la Secretaría de Seguridad, Convivencia y Justicia a través de la generación de copias de respaldo, garantizando su recuperación ante posibles pérdidas, su integridad y la continuidad de los procesos de la Entidad.

ALCANCE

Inicia con la definición de la información de bases de datos que se debe respaldar en el Plan de Backup BD, continua con su configuración, y finaliza con la verificación del resultado final con base en el Plan.

NORMATIVIDAD


- Ley 1273 de 2009 – De La Protección de la Información y de los datos.
- ISO/IEC 27001:2013 – Sistemas de Gestión de Seguridad de la Información (SGSI)
- ISO/IEC 27002:2005 – Código para la Práctica de la Gestión de la Seguridad de la Información.
- ISO 22301:2012 – Seguridad de la Sociedad: Sistemas de Continuidad del Negocio y la Norma Técnica Colombiana NTC- ISO: 9001.
- Resolución 541 del 04 de diciembre de 2017 de la SCJ por la cual se adopta la Política de Seguridad de la Información y se definen lineamientos para su uso, actualización y aplicación”

DOCUMENTOS DE REFERENCIA

EXTERNOS

INTERNOS

Política de Seguridad y Privacidad de la Información PO-GT-1

 ALCALDÍA MAYOR DE BOGOTÁ D.C. Secretario Distrital de Seguridad, Convivencia y Justicia	Proceso:	Gestión de Tecnologías de la Información	Código:	PD-GT- 11
	Documento:	Generación de Backup Bases de Datos	Versión:	1
			Fecha Aprobación:	30/08/2019
			Fecha de Vigencia:	Página 2 de 12
			30/08/2019	

DEFINICIONES

BACKUP/ Copia de Seguridad: En tecnologías de la información e informática es una copia de los datos originales que se realiza con el fin de disponer de un medio de recuperación consistente, el cual puede ser usado en caso de un desastre, fallo o pérdida de Bases de Datos.

Base de Datos: Conjunto de datos relacionados que se almacenan de forma ordenada pudiéndose acceder a ellos de manera sencilla, con la posibilidad de relacionarlos y acomodarlos basados en diferentes criterios, etc.

Confidencialidad: Es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.

Copia de seguridad Completa (full): Una copia de seguridad en línea y fuera de línea incluye la totalidad de archivos previamente seleccionados de un sistema informático.


Copia de seguridad (Backup) Diferencial: Respaldar los archivos que han cambiado desde el más reciente bajo nivel, por ejemplo, un nivel 5 respalda los archivos que han cambiado desde el más reciente nivel 4,3,2,1 y 0 (Full). Los niveles se incluyen desde el 0 al 9.

Copia de seguridad incremental: Una copia de seguridad que respalda los archivos creados o modificados desde la última copia de seguridad completa. La restauración de los datos debe realizarse con la última copia de seguridad completa y las copias de seguridad incrementales posteriores.

Crontab: Es un demonio (proceso en segundo plano usado para programación de tareas), configurado en un archivo con contenido especial. Posee una lista con todos los scripts a ejecutar, su periodicidad y ubicación en el sistema para ejecución.

Dabas: Servicio SaaS, donde la base de datos se ofrece como servicio. La infraestructura se aloja en el proveedor de nube y sirve para múltiples clientes.

Disponibilidad: Es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. Secretaría Distrital de Seguridad, Convivencia y Justicia	Proceso:	Gestión de Tecnologías de la Información	Código:	PD-GT- 11
	Documento:	Generación de Backup Bases de Datos	Versión:	1
			Fecha Aprobación:	30/08/2019
			Fecha de Vigencia:	Página 3 de 12
			30/08/2019	

IaaS: Infraestructura como servicio por sus siglas en inglés. Se trata de servicios de computación en la nube a través de la red de redes (internet).

Integridad: Es la protección de la exactitud y estado completo de los activos.


Recursos tecnológicos: Son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de la Secretaría Distrital de Seguridad, Convivencia y Justicia.

Recuperación y Restauración: Hace referencia a las técnicas empleadas para recuperar la información (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.

RMAN: Administrador de recuperación, por sus siglas en inglés. Es un cliente de base de datos Oracle que permite realizar Backup y recuperación de tareas en la Base de Datos, automatizando la administración y estrategias de Backup.

SaaS: Software como servicio por sus siglas en inglés. Se trata de aplicaciones completas ofrecidas como servicio, bajo demanda y vía multitenan, lo que significa una sola instancia de software que corre en la infraestructura del proveedor de nube y sirve para múltiples clientes.

Sistema de información: Es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. Secretaría Distrital de Seguridad, Convivencia y Justicia	Proceso:	Gestión de Tecnologías de la Información	Código:	PD-GT- 11
	Documento:	Generación de Backup Bases de Datos	Versión:	1
			Fecha Aprobación:	30/08/2019
			Fecha de Vigencia:	Página 4 de 12
			30/08/2019	

POLÍTICAS DE OPERACIÓN

- La política y estrategia de backup de la Secretaria de Seguridad Convivencia y Justicia está alineada a la naturaleza del negocio y los componentes que lo soportan: Networking, Procesamiento, servicios, aplicaciones e Interoperatividad. El presente procedimiento está enfocado en la política y estrategia de backup de bases de datos.
- Como parte de las buenas prácticas y acorde a la ISO 27001, se programan actividades orientadas a la obtención de Backup de bases de datos relevantes en la operación de la Entidad.
- Cada funcionario y contratista de la Secretaria de Seguridad, Convivencia y Justicia es responsable de salvaguardar la información propia de su trabajo almacenada en los equipos de cómputo asignados, ubicándolos en el repositorio de información virtual destinado por la Entidad para tal fin.
- El encargado de la administración de copias de seguridad deberá realizar pruebas de los elementos más críticos, validando su efectividad.

PARÁMETROS DE MEDICIÓN

Ver Matriz de Indicadores



ALCALDÍA MAYOR
DE BOGOTÁ D.C.

Secretaría Distrital de Seguridad,
Convivencia y Justicia

Proceso:

Gestión de Tecnologías de la
Información

Documento:

Generación de Backup Bases de
Datos

Código:

PD-GT- 11

Versión:

1

Fecha Aprobación:

30/08/2019


Fecha de Vigencia:

30/08/2019

Página 5 de 12

DESCRIPCIÓN DEL PROCEDIMIENTO

Nº	Entrada o Insumo	Actividad	Descripción de la Actividad	Dependencia	Responsable	Punto de Control	Salida (Registro)
1.	Planeación del Año	Programar reunión con equipo de Infraestructura	El coordinador de infraestructura convoca una reunión con el equipo de trabajo dedicado servicios en la nube y onpremise	Dirección de Tecnologías y Sistemas de la Información	Profesional - Líder de infraestructura		Agendamiento por correo electrónico
2.	Agendamiento por correo electrónico	Evaluar Tecnologías de susceptibles de backup	El equipo de infraestructura administrador de recursos de red de datos, determina a que Base de Datos se les realizará BackUp, y bajo qué métodos, tiempos, riesgos y responsables de ejecución del procedimiento.	Dirección de Tecnologías y Sistemas de la Información	Profesionales - Equipo de Backup		Definición de tipo de información a respaldar
3.	Definición de tipo de información a respaldar	Decidir tipo de respaldo y herramientas	Definir el tipo de Backup y su frecuencia según la naturaleza del servicio y su impacto en la operación. Así mismo se define el uso de herramientas dependiendo de si se trata de una Base de Datos en la nube u onpremise.	Dirección de Tecnologías y Sistemas de la Información	Profesionales - Equipo de Backup		Definición de tecnología de backup apropiada

 ALCALDÍA MAYOR DE BOGOTÁ D.C. Secretaría Distrital de Seguridad, Convivencia y Justicia	Proceso:	Gestión de Tecnologías de la Información	Código:	PD-GT- 11
			Versión:	1
	Documento:	Generación de Backup Bases de Datos	Fecha Aprobación:	30/08/2019
			Fecha de Vigencia:	Página 6 de 12 30/03/2019

4.	Definición de tipo de información a respaldar y tecnología de backup adecuada	Definir el plan de trabajo	Una vez planeado el sistema de backup a realizar, se genera un plan de trabajo con definiciones, un cronograma detallado de tareas, responsables, tiempos y actividades a desarrollar; lo cual queda establecido en el plan anual de Backup.	Dirección de Tecnologías y Sistemas de la Información	Profesionales - Equipo de Backup		Plan de Backup Bases de Datos
5.	Plan Anual de Backup Continuación Ejecución Plan Anual de Backup	Revisar tipo de backup en Plan de trabajo	Revisar en el plan de trabajo la forma cómo está establecido la ejecución del Backup, teniendo en cuenta lo siguiente: - Backup de Base de Datos debe realizarse para servicios basados en nube pública o privada (onpremise). - Si el Backup se planea realizar en nube privada (onpremise), se debe definir el tipo de servidor: si se trata de un servicio basado en software (SaaS-DBaS) o uno basado en infraestructura (IaaS). - Cuando se trata de software como servicio (SaaS-DBaS), existen dos tipos de herramienta para generar BackUps:	Dirección de Tecnologías y Sistemas de la Información	Profesional de Backup		Tareas de backup



**ALCALDÍA MAYOR
DE BOGOTÁ D.C.**

Secretaría Distrital de Seguridad,
Convivencia y Justicia

Proceso:

**Gestión de Tecnologías de la
Información**

Código:

PD-GT- 11

Versión:

1

Fecha Aprobación:

30/08/2019

Documento:


**Generación de Backup Bases de
Datos**

Fecha de Vigencia:

30/08/2019

Página 7 de 12

			herramienta automatizada basada en servicio y herramienta manual. - Cuando se trata de un servicio basado en infraestructura (IaaS), se debe realizar el procedimiento mediante la herramienta manual				
Tareas de backup	¿Generación del Backup en nube o físico?	Backup en nube: Continua en punto de decisión "Tipo de servicio en la nube" Backup Físico: Continúa con actividad 10	Dirección de Tecnologías y Sistemas de la Información	Profesional de Backup			Medio de generación del backup
Tareas de backup Medio de generación del backup	¿Tipo de Servicio en la nube?	Servicio Dabas: Continua en punto de decisión "Tipo de Herramienta" Servicio IaaS: Continua en la actividad No. 8	Dirección de Tecnologías y Sistemas de la Información	Profesional de Backup			Tipo de Servicio a generar backup
Tareas de backup Tipo de Servicio a generar backup	¿Tipo de Herramienta?	Herramienta Automática: Continúa en actividad 6. Herramienta Manual: Continúa en actividad 8	Dirección de Tecnologías y Sistemas de la Información	Profesional de Backup			Tipo de herramienta para backup

 ALCALDÍA MAYOR DE BOGOTÁ D.C. Secretaría Distrital de Seguridad, Convivencia y Justicia	Proceso:	Gestión de Tecnologías de la Información	Código:	PD-GT- 11
			Versión:	1
	Documento:	Generación de Backup Bases de Datos	Fecha Aprobación:	30/08/2019
			Fecha de Vigencia:	Página 8 de 12
			30/08/2019	

6.	Tareas de backup Tipo de herramienta para backup	Configurar y ejecutar herramienta de Backup de Oracle	Si se ha decidido ejecutar la herramienta suministrada por el proveedor. Se debe configurar tiempos (políticas de retención), tipo (full o incremental) y alcances.	Dirección de Tecnologías y Sistemas de la Información	Profesional de Backup		Backup en Oracle
7.	Backup en Oracle	Verificar Backup Oracle	La verificación de los BackUps programados se debe realizar mediante la revisión de logs, la existencia del archivo en el repositorio destinado para tal fin, la frecuencia seleccionada y la consistencia en cuanto al tamaño del archivo. Si el backup es coherente de acuerdo a los requerimientos planeados, se da por terminado el procedimiento. De no ser exitoso, se debe reconfigurar la herramienta, regresa a la actividad 6.	Dirección de Tecnologías y Sistemas de la Información	Profesional de Backup	Verificación de la ejecución del backup en oracle	Backup en Oracle Verificado
	Backup en Oracle Verificado	¿Backup Correcto?	Si: Fin del Procedimiento No: Regresa a la actividad 6	Dirección de Tecnologías y Sistemas de la Información	Profesional de Backup		Backup Correcto Backup erróneo



ALCALDÍA MAYOR
DE BOGOTÁ D.C.
Secretaría Distrital de Seguridad,
Convivencia y Justicia

Proceso:

Gestión de Tecnologías de la
Información

Código:

PD-GT- 11

Versión:

1

Fecha Aprobación:

30/08/2019

Documento:


Generación de Backup Bases de
Datos

Fecha de Vigencia:

30/08/2019

Página 9 de 12

8.	Tareas de backup Tipo de herramienta para backup	Configurar y ejecutar herramienta RMAN y CronTab en servidores donde se aloja la Base de Datos	Cuando se trata del uso de Backup de tipo manual, se debe configurar la herramienta CronTab y RMAN para sistemas operativos Linux, la cual programa tareas de manera periódica y bajo las condiciones de archivos a guardarse. El equipo de infraestructura de red conoce de antemano los archivos que deben guardarse de acuerdo al Plan de Backup BD. El repositorio utilizado es tipo SaaS.	Dirección de Tecnologías y Sistemas de la Información	Profesional de Backup		Backup en repositorio de Oracle.
9.	Backup en repositorio de Oracle.	Verificar Backup en repositorio alojado en la nube de Oracle	La verificación de los BackUps de Bases de Datos realizados por "Cron Tab", deben realizarse mediante la validación de logs, es decir, verificar la existencia del archivo en el repositorio destinado para tal fin, la frecuencia seleccionada y la consistencia en cuanto al tamaño del archivo. Si el backup es coherente de acuerdo a los requerimientos planeados, se da por terminado el procedimiento. De no ser exitoso, se debe reconfigurar la herramienta, regresa a la actividad 8.	Dirección de Tecnologías y Sistemas de la Información	Profesional de Backup	Verificación de la ejecución del backup en "Cron Tab"	Backup en repositorio de Oracle verificado

 ALCALDÍA MAYOR DE BOGOTÁ D.C. Secretaría Distrital de Seguridad, Convivencia y Justicia	Proceso:	Gestión de Tecnologías de la Información	Código:	PD-GT- 11
	Documento:	Generación de Backup Bases de Datos	Versión:	1
			Fecha Aprobación:	30/08/2019
			Fecha de Vigencia:	Página 10 de 12
			30/08/2019	

	Backup en repositorio de Oracle verificado	¿Backup Correcto?	Si: Fin del Procedimiento No: Regresa a la actividad 8	Dirección de Tecnologías y Sistemas de la Información	Profesional de Backup		Backup Correcto Backup erróneo
10.	Tareas de backup Tipo de Sistema operativo del servidor en el que se encuentra la información a hacer backup	Configurar y ejecutar herramienta RMAN y CronTab en servidores donde se aloja la Base de Datos	Cuando se trata del uso de BackUp de tipo manual para equipos onpremise (físicos), se debe configurar la herramienta CronTab y RMAN para sistemas operativos Linux, la cual programa tareas de manera periódica y bajo las condiciones de archivos a guardarse. El equipo de infraestructura de red conoce de ante mano los archivos que deben guardarse de acuerdo al Plan de Backup BD. El repositorio se ubica en el Sistema Hiperconvergente	Dirección de Tecnologías y Sistemas de la Información	Profesional de Backup		Backup mediante CronTab y RMAN



ALCALDÍA MAYOR
DE BOGOTÁ D.C.

Secretaría Distrital de Seguridad,
Convivencia y Justicia

Proceso:

Gestión de Tecnologías de la
Información

Documento:

Generación de Backup Bases de
Datos

Código:

PD-GT- 11

Versión:

1

Fecha Aprobación:


30/08/2019

Fecha de Vigencia:

30/08/2019

Página 11 de 12

11.	Backup mediante CronTab y RMAN	Verificar Backup en repositorio alojado en sistema Hiperconvergente	La verificación de los BackUps de Bases de Datos realizados por Cron Tab y RMAN, deben realizarse mediante la validación de logs, es decir, verificar la existencia del archivo en el repositorio destinado para tal fin, la frecuencia seleccionada y la consistencia en cuanto al tamaño del archivo. Si el backup es coherente de acuerdo a los requerimientos planeados, se da por terminado el procedimiento. De no ser exitoso, se debe reconfigurar la herramienta, regresa a la actividad 10.	Dirección de Tecnologías y Sistemas de la Información	Profesional de Backup	Verificación de la ejecución del backup en Snapshot	Backup en repositorio alojado en sistema Hiperconvergente verificado
	Backup en repositorio alojado en sistema Hiperconvergente verificado	¿Backup Correcto?	Si: Continúa al punto de decisión "¿Falta ejecutar actividades del Plan anual? No: Regresa a la actividad 8	Dirección de Tecnologías y Sistemas de la Información	Profesional de Backup		Backup Correcto Backup erróneo
	Plan Anual de Backup Backup Correcto	¿Falta ejecutar actividades del Plan Anual de backup?	Si: Regresa a la actividad 5. No: Finaliza Procedimiento	Dirección de Tecnologías y Sistemas de la Información	Profesional de Backup		Fin del procedimiento Continuación Ejecución Plan Anual de Backup

 ALCALDÍA MAYOR DE BOGOTÁ D.C. Secretaría Distrital de Seguridad, Convivencia y Justicia	Proceso:	Gestión de Tecnologías de la Información	Código:	PD-GT- 11
	Documento:	Generación de Backup Bases de Datos	Versión:	1
			Fecha Aprobación:	30/08/2019
			Fecha de Vigencia:	30/08/2019
				Página 12 de 12

CONTROL DE CAMBIOS			
No. VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO	
1	30/08/2019	Documento Original	
ELABORÓ		REVISÓ	APROBÓ
NOMBRE	Sofía Elizabeth Gómez Muñoz	Jose Alejandro Suarez Cleves Marcela Senestrari Castro	Andres Javier Solorzano Ulloa
CARGO	Contratista – Ing. Calidad	Profesional Universitario Contratista Líder Operativo MIPG	Director de Tecnologías de Información
FIRMA	