1. Objetivo:

Asegurar la información contenida en los sistemas de información de la Administración Central a través de la generación de copias de respaldo de archivos, programas, sistemas operativos y bases de datos, garantizando su recuperación ante posibles pérdidas, su integridad y la continuidad de los procesos de la Entidad.

2. Alcance:

Inicia desde la planeación de la generación de los respaldos hasta la custodia a través de un tercero.

3. Convenciones

Convenciones	Punto de Control	Decisión	Nota	Evidencias	Interacción con otros procesos
					

4. Definiciones:

Almacenamiento en la nube: El almacenamiento en la nube es un servicio que permite almacenar datos transfiriéndolos a través de Internet o de otra red a un sistema de almacenamiento externo que mantiene un tercero

Backup: Procedimiento informático para el almacenamiento y aseguramiento de la información. Es una copia de los datos originales que se realiza con el fin de disponer de un medio de recuperarlos en caso de su pérdida.

Backup en frio: implica parar la Base de Datos en modo normal y copiar todos los ficheros sobre los que se asienta (datafile, controlfile y logfile). Antes de parar la Base de Datos hay que parar también todas las aplicaciones que estén trabajando con la Base de Datos. Una vez realizada la copia de los ficheros, la Base de Datos se puede volver a arrancar.

Backup en caliente: se realiza mientras la Base de Datos está abierta y funcionando en modo ARCHIVELOG. Habrá que tener cuidado de realizarlo cuando la carga de la Base de Datos sea pequeña.

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.

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

Copia de Seguridad Completa: Contiene todos los datos de las carpetas y archivos que se han seleccionado para la copia de seguridad.

Copia de Seguridad Diferencial: Consiste en copiar todos los datos nuevos o modificados desde la última copia completa

Copia de Seguridad Incremental: solo realiza la copia de los archivos que hayan sido modificados desde la última copia, sea ésta completa o diferencial.

Integridad: Propiedad de Salvaguardar la exactitud y estado completo de los activos de información

Medio Externo: Dispositivo capaz de leer y escribir información con el propósito de almacenarla como CD, DVD, cintas magnéticas, USB, etc.

Restauración de los datos (en inglés ***restore***), es la acción de leer y grabar en la ubicación original u otra alternativa los datos requeridos.

5. Base legal:

Ver Normograma, código NOR-SIG-01.

6. Condiciones generales:

La generación de copias de seguridad, se realizarán de conformidad con el plan de copias de seguridad y por requerimientos específicos de las dependencias de la Alcaldía, y se aplicarán las políticas y controles establecidos en el manual de políticas de seguridad de la Información 12.3 Copias de Respaldo.

Para la recepción de las copias de seguridad se requiere que el memorando de entrega contenga las fechas de elaboración de las copias de seguridad y ´se referencie la información que contiene.

Cuando se requiera tener una copia de la base de datos completa se hace el Backup en frio, y cuando se requiere copiar todos los ficheros correspondientes a un tablespace determinado, los ficheros redo log archivados y los ficheros de control, se hace el backup en caliente, el tipo de Backup dependerá de lo que se establezca en el plan de copias de seguridad.

El plan de copias contendrá como mínimo la siguiente información: Elemento Respaldado, Periodicidad, número de copias según periodicidad, Tipo de copia (Completa, Incremental, Diferencial), Medio de Almacenamiento, Responsable, periodicidad pruebas de restauración, observaciones.

El almacenamiento Externo podrá ser en la NUBE, dependiendo de la disponibilidad de recursos para la contratación de este Servicio y la capacidad de almacenamiento contratado. Las copias de respaldo que no se alojen en la nube, deben reposar en sitio externo definido por la Secretaría de las TIC.

EL Reemplazo de los medios de almacenamiento y su disposición final estarán contemplados en el plan de preservación digital.

Tal como lo establece la política de seguridad de la información, el propietario de la información es el responsable de definir el periodo de retención de las copias de seguridad, para lo cual debe tener en cuenta las TRD y las disposiciones de la ley general de archivo

7. Actividades

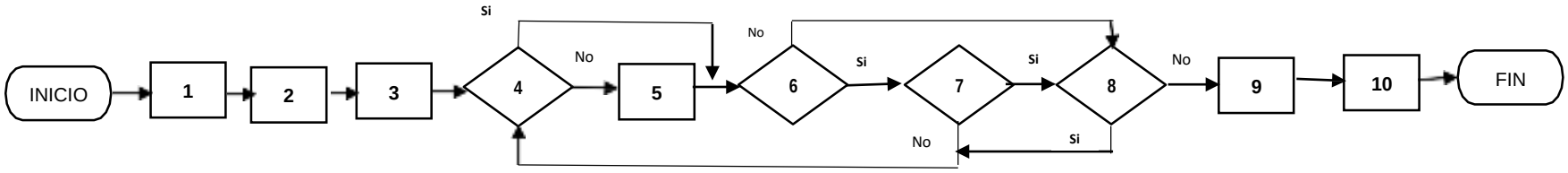
Descripción del Procedimiento			
No.	**Descripción de la actividad**	**Responsable**	**Evidencia**
1	**Elaborar el plan de copias de Seguridad:** Identificar los sistemas de información automatizados que se encuentran en producción de la administración central e información que requiere tener copia de respaldo y elaborar el plan de copias de seguridad, teniendo en cuenta el volumen de información, periodicidad de la copia, responsable, proceso, tipo de copia, medio de almacenamiento y periodicidad de restauración El responsable del control y ejecución del procedimiento de creación y custodia de copias de seguridad cuando elabora el plan de copias, y con una periodicidad semestral, verifica que todos los sistemas de información que apoyan los procesos de la Entidad registrados en el inventario estén incluidos en el plan de copias de seguridad, El registro de las adiciones o modificaciones, quedan registradas en el plan de copias. En caso de detectar sistemas de sistemas de información no incluidos en el plan de Backups, remitir comunicación interna registrada en PISAMI – Gestión Documental, al líder del proceso solicitando la información necesaria para ser incluido en el plan de copias. Aplica la política de seguridad 12.3 Copias de respaldo.	Profesional Universitario de la Secretaría de las TIC	PISAMI-Gestión Documental, Plan de Backup
2	**Realizar Copia de Seguridad** Los administradores de los Sistemas de Información o a quien se le delegue esta responsabilidad programan la copia automática de acuerdo a la periodicidad establecida o en su defecto la genera manualmente y la remite a la Secretaría de las TIC, en el medio y periodicidad establecido en el plan de copias Todo medio de almacenamiento se rotula con el nombre de la base de datos, servidor o sistema de información y la fecha en formato dd-mm-aaaa.	Servidor Público responsable según Plan de Copias en cada Área Administrativa	Medio de almacenamiento

Descripción del Procedimiento			
No.	**Descripción de la actividad**	**Responsable**	**Evidencia**
	EL Responsable de realizar la copia de seguridad verifica el estado del backup, teniendo entre otros parámetros el tamaño de la copia, el tiempo de generación, contenido, cantidad de archivos o carpetas. En caso de observar inconsistencias, analizar las causas, tomar correctivos y generar nuevamente la copia de seguridad. Aplica la política de seguridad 12.3 Copias de respaldo:		
3.	**Recepcionar copias de Seguridad** Acceder a las copias de respaldo remitidas por las Dependencias, por los diferentes medios. El encargado de la ejecución y seguimiento del plan de copias, adscrito a la Secretaría de las TIC, diariamente verifica las copias de respaldo remitidas por las diferentes Dependencias y confronta la periodicidad del envío con lo establecido en el plan de copias y el tamaño de la copia con las copias anteriores. Cuando se detecte un incumplimiento solicita por escrito al líder del proceso mediante comunicación interna registrada en PISAMI-Gestión Documental, o cuando advierta una variación significativa en el tamaño de la copia, lo comunica de manera inmediata al responsable de la realización de la copia, por medio de correo electrónico. Aplica la política de seguridad 12.4.2 Protección de la información de registro	Profesional o técnico de Secretaría de las TIC	PISAMI-Gestión Documental Medio de almacenamiento
4	**Realizar almacenamiento externo** Asegurar las copias de respaldo en un lugar de almacenamiento diferente al servidor primario. El almacenamiento es en la nube? **Si:** cargar las copias de seguridad en el repositorio indicado para la correspondiente transmisión. Continúa con la actividad 6 **No: Continúa con la actividad 5**	Profesional o técnico de Secretaría de las TIC	Medio de Almacenamiento

Descripción del Procedimiento			
No.	**Descripción de la actividad**	**Responsable**	**Evidencia**
5	**Remitir copias a custodia en medio físico** Remitir con oficio registrado en PISAMI, la copia en un medio removible a la entidad externa responsable de la custodia. Aplica la política de seguridad 12.3 Copias de respaldo 13.2 Transferencia de información 12.4.2 Protección de la información de registro	Profesional o técnico de Secretaría de las TIC	PISAMI-Gestión Documental
6	**Gestionar el acceso a la copias de seguridad externas** Solicitar las copias de seguridad a la Entidad que las tenga en custodia o acceder a las que se encuentran almacenadas en la nube. Esto se puede originar por dos razones: 1. Por solicitud Escrita de los Entes de Control Externo 2. Por necesidad de restauración por medio de ticket o Comunicación interna registrada en PISAMI –Gestión Documental 3. Por prevención en cumplimiento de la política de seguridad Es por solicitud de los Entes de Control Externo? **Si:** Continúa con la actividad 7 **No:** Continúa con la actividad 8	Profesional o técnico de Secretaría de las TIC	PISAMI-Gestión Documental, Ticket
7	**Suministrar copia de Seguridad al Ente de Control** Realizar una copia adicional, cuando la copia va a quedar en poder del Ente de Control y hacer la entrega dejando registro en PISAMI-Gestión Documental. El ente de Control Externo solicita soporte para la restauración? **Si:** Brindar el soporte técnico para la restauración de la copia en sitio, para lo cual ejecuta la actividad 8 **No:** Continúa con la actividad 4	Profesional o técnico de Secretaría de las TIC	Acta.

Descripción del Procedimiento			
No.	**Descripción de la actividad**	**Responsable**	**Evidencia**
8	**Restaurar copias de seguridad** Restaurar las copias de seguridad con la base de datos en frio o en ambiente de pruebas. La restauración fue exitosa? **Si:** Dejar constancia en el acta o en el ticket. Continúa con la actividad 4 **No:** Continúa con la actividad 9 En ambiente de pruebas se debe realizar la restauración de copias con periodicidad mínima cuatrimestral, para verificar su integridad y disponibilidad o cuando se requiere reemplazar datos para hacer alguna verificación de información o proceso especial. En frio cuando se requiere reemplazar los datos de producción como acción del plan de gestión de incidente.	Administradores de los Sistemas de información	PISAMI-Módulo de Tickets, Gestión Documental o actas.
9	**Analizar fallas en la restauración** Analizar posibles fallas ocasionadas en la restauración y tomar acciones correctivas para garantizar la efectividad de las copias de respaldo. Registrar constancia de la actuación en acta.	Responsable de los sistemas de información	Acta
10	**Archivar documentación** Archivar los documentos físicos y digitales originados en el desarrollo del proceso **y finaliza el procedimiento**. Proceso de Gestión Documental, Procedimiento Oorganización de documentos de archivo de gestión.	Auxiliar Administrativo	Expediente de archivo según TRD

8. Flujograma



9. Control de cambios

VERSIÓN	VIGENTE DESDE	DESCRIPCIÓN DEL CAMBIO
01	11/12/2015	PRIMER VERSIÓN
02	31/07/2018	SEGUNDA VERSION
03	25/04/2018	TERCERA VERSION
04	10/07/2019	CUARTA VERSION
05	30/10/2019	QUINTA VERSION
06	30/12/2021	Cambio nombre de Dependencia en el flujograma, de Dirección de informática a Secretaría TIC Actualización base legal remitiendo al normograma. Inclusión en las actividades del flujograma de la actividad 10 Modificación punto de control y adición de registro en la actividad 16
07	25/02/2022	Se actualiza el formato de conformidad con la versión 11 del procedimiento control de documentos del SIGAMI Se actualizaron los puntos de control, y las actividades del procedimiento, Se relacionaron las actividades donde aplican políticas de seguridad. Se actualizó el flujograma, el normograma, y conceptos

10. Ruta de aprobación

Elaboró	Revisó	Aprobó
Profesional Especializado Profesional Universitario Grupo Infraestructura Tecnológica	Asesor	Secretaria de las TIC