1. OBJETIVO

Determinar las acciones que garanticen la administración de las copias de seguridad y las restauraciones de copias de información, con el fin de salvaguardar la integridad, confiabilidad y confidencialidad de la información institucional.

2. ALCANCE

El procedimiento inicia con las solicitudes de respaldo de información, las estrategias y estándares de respaldo establecidos en los sistemas de información de la Entidad, incluye la programación de las actividades, ejecución, registro y restauración de las copias de la información. Este procedimiento cubre las necesidades de respaldo de información Lógica:

- Servidores
- Aplicaciones
- Bases de datos.

3. RESPONSABLES

La Oficina de Tecnología de la Información y las Comunicaciones, junto con el grupo de Profesionales del área, son los responsables de la ejecución y monitoreo de este procedimiento.

Elaboró	Revisó	Aprobó
Jorge Ramírez Contratista Oficina TIC.	Camilo Augusto Ramos Profesional Universitario Oficina TIC Andres Briceño Diaz Jefe Oficina TIC	Andres Briceño Diaz Jefe Oficina TIC Javier de Jesús Cruz Jefe de la Oficina Asesora de Planeación.
Fecha: 09/08/2019	Fecha: 12/08/2019	Fecha: 21/08/2019

4. NORMATIVIDAD

Norma	Titulo	Origen			Articulo
		Nacional	Distrital	Interna	
Ley 527 de 1999	Ley 527 Por medio de la cual se define y reglamenta, el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales	X			Utilización de medios electrónicos
Ley 1266 de 2008	Por la cual se dictan las disposiciones generales del Habeas data y se regula el manejo de la información contenida en bases de datos personales en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.	X			ARTÍCULO 1. OBJETO. La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información establecido en el artículo 20 de la Constitución Política, particularmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países.
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la	X			CAPITULO I De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

	información y las comunicaciones, entre otras disposiciones.				
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales	X			Todo su contenido.
Decreto 235 de 2010	Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones publicas	X			Artículo 2. Para efectos del intercambio de Información, las entidades a que hace referencia el artículo anterior deberán establecer mecanismos magnéticos, electrónicos o telemáticos para integrar, compartir y/o suministrar la información que por mandato legal se requiere, o permitir el acceso total dentro del marco de la Constitución y el derecho fundamental a la intimidad, a las bases de datos completas que requieran otras entidades para el ejercicio de sus funciones.
Decreto 1008 de 2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones	X			Todo su contenido.
Decreto 1377 de 2013	Tiene como objeto reglamentar parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de	X			Todo su contenido.

	datos personales.				
Decreto 1078 de 2015	Decreto único reglamentario del sector de tecnologías de la información y las comunicaciones.	X			Todo su contenido.
Resolución 4664 de 2016	Por la cual se adopta la Política de Seguridad Informática de la Caja de la Vivienda Popular			X	Todo el documento
Norma Técnica Internacional ISO 27001 ; 27002 ; 27005 de 2013	Norma internacional emitida por la Organización Internacional de Normalización (ISO) para gestionar la seguridad de la información en una organización pública o privada.	X			Es la norma estándar para la implementación del Sistema de Gestión de Seguridad de la Información expedida por la Organización Internacional de Normalización que describe cómo gestionar la seguridad de la información en una organización.

5. DOCUMENTOS DE REFERENCIA

Tipo de documento	Título del documento	Código	ORIGEN	
			Nacional	Distrital
NORMA	Norma Técnica Internacional ISO 27001; 27002; 27005 de 2013	N/A	X	

6. DEFINICIONES

- ✓ **Base de Datos:** Conjunto de datos relacionados que se almacenan de forma que se pueda acceder a ellos de manera sencilla, con la posibilidad de relacionarlos, ordenarlos en base a diferentes criterios, etc. Las Bases de Datos son uno de los grupos de aplicaciones de productividad personal más extendidos.
- ✓ **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 porque un evento ocurre para un dispositivo en particular o aplicación.

- ✓ **BACK-UP (COPIA DE RESPALDO):** Copia de seguridad de los archivos, aplicaciones y/o bases de datos disponibles en un soporte magnético (generalmente discos o CD), con el fin de poder recuperar la información en caso de un daño, borrado accidental o un accidente imprevisto.
- ✓ **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.
- ✓ **Plan de Pruebas de Recuperación**: pruebas de recuperación de copias de respaldo programadas con el fin de verificar la consistencia e integridad de las copias de respaldo.
- ✓ **Recuperación (Restauración):** 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, realizar pruebas, entre otros.
- ✓ **Integridad**: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- ✓ **Periodicidad copias de seguridad**: Hace referencia a la frecuencia con la que se realizan las copias de seguridad de la información institucional, la entidad tiene definida la frecuencia en tres tipos de periodicidad los cuales diarias, semanales y mensuales.
- ✓ **NAS (Network Attached Storage):** define todo sistema que permita compartir almacenamiento de data en un punto central a través de la red. Este punto central se le conoce como el servidor NAS (NAS server). El servidor NAS puede incluir uno o más discos duros, y tiene la capacidad de almacenar y compartir data proveniente de diferentes fuentes (computadoras, servidores, servicios en el web, entre otros).
- ✓ **Backups completos:** Como su propio nombre indica, este tipo de backup copia la totalidad de los datos en otro juego de soportes, que puede consistir en cintas, discos. La ventaja principal de la realización de un backup completo en cada operación es que se dispone de la totalidad de los datos en un único juego de soportes. Esto permite restaurar los datos en un tiempo mínimo, lo cual se mide en términos de objetivo de tiempo de recuperación (RTO). No obstante, el inconveniente es que lleva más tiempo realizar un backup completo que de otros tipos (a veces se multiplica por un factor 10 o más), y requiere más espacio de almacenamiento.
- ✓ **Backups incrementales**: Una operación de backup incremental sólo copia los

datos que han variado desde la última operación de backup de cualquier tipo. Se suele utilizar la hora y fecha de modificación estampada en los archivos, comparándola con la hora y fecha del último backup. Las aplicaciones de backup identifican y registran la fecha y hora de realización de las operaciones de backup para identificar los archivos modificados desde esas operaciones. Como un backup incremental sólo copia los datos a partir del último backup de cualquier tipo, se puede ejecutar tantas veces como se desee, pues sólo guarda los cambios más recientes. La ventaja de un backup incremental es que copia una menor cantidad de datos que un backup completo. Por ello, esas operaciones se realizan más deprisa y exigen menos espacio para almacenar el backup.

- ✓ **Niveles de respaldo de información**: Hace referencia a los diferentes ambientes en los cuales las copias de seguridad se guardan de manera oportuna con el fin de tener varios niveles de recuperación de la información en caso de desastre. Actualmente la entidad cuenta con dos niveles de respaldo, las unidades de cinta y replicación de las bases de datos en el datacenter externo con el cual cuenta la entidad.

7. CONDICIONES GENERALES

- La Oficina TIC debe asesorar al propietario de la información para aplicar el procedimiento de las copias de seguridad de la información
- La Oficina TIC debe contar con un servidor donde se aloje la información que se va a respaldar
- La Oficina TIC definirá los tipos de copia de seguridad que se va a realizar de información institucional contenida en los servidores de la Entidad.
- La Entidad debe contar con un repositorio robusto para almacenamiento de información institucional.
- Todos los usuarios deben almacenar la información institucional en la unidad Z: asociada a la cuenta de usuario del dominio de la Entidad.
- Para las solicitudes de copias de respaldo y de restauración de copias debe ser solicitado mediante el email dirigido a soporte@cajaviviendapopular.gov.co indicando nombre de usuario y fecha de validación de la información en la unidad Z:.

8. DESCRIPCION DEL PROCEDIMIENTO

No.	Actividad	Responsable	Documentos/Registros
	¿El procedimiento inicia con una copia de seguridad o restauración? - Copia de Seguridad, ir a la actividad 1. - Restauración. Ir a la actividad 8.		
COPIAS DE SEGURIDAD			
1	Definir mediante una política de seguridad en el controlador de dominio la ejecución automática de la copia de toda información alojada en la carpeta *Documentos_CVP* o en la unidad Z: de cada uno de los usuarios de la entidad con los parámetros establecidos por los responsables de la información; la cual será respaldada en un servidor *serv_cv11*	Profesional de la Oficina TIC	Políticas de seguridad de dominio
2	Definir que todo equipo de cómputo unido al controlador de dominio de la CVP y autenticado con una cuenta de la misma, realizara una copia automática de seguridad.	Profesional de la Oficina TIC	
3	Revisar los archivos de log de auditoria del servidos utilizado para el alojamiento de copias de seguridad	Profesional de la Oficina TIC	Log Aplicación. Registro de copia realizada
4	Verificar que las copias de seguridad realizadas queden almacenadas en el primer nivel de respaldo	Profesional de la Oficina TIC	Log de auditoria de Windows.
5	Verificar que las copias de seguridad de bases de datos realizadas queden guardadas en el segundo nivel de respaldo DATA CENTER EXTERNO con el proveedor de servicio de alojamiento en la nube	Proveedor de servicio de alojamiento en la nube	Log Aplicación.
6	Revisar periódicamente la disponibilidad de espacio en el repositorio y DATA CENTER EXTERNO.	Profesional de la Oficina TIC Proveedor de servicio de alojamiento en la nube	

No.	Actividad	Responsable	Documentos/Registros
7	Validar de la conectividad entre el Datacenter externo y la CVP junto con la correcta ejecución de políticas de seguridad definidas en el controlador de dominio.	Profesional de la Oficina TIC Proveedor de servicio de alojamiento en la nube	
FIN DE PROCEDIMIENTO COPIAS DE SEGURIDAD			
RESTAURACION			
8	Solicitar por correo institucional soporte@cajaviviendapopular.gov.co la restauración de una copia de seguridad especificando: - Fecha - Usuario - Nombre de carpeta o archivo - Ubicación de la restauración :	Responsable de la información / supervisor / funcionario / contratista	Correo Institucional.
9	Verificar la existencia de la copia de seguridad en el primer nivel de respaldo teniendo en cuenta los criterios establecidos en el correo de solicitud.	Profesional de la Oficina TIC	Log Aplicación.
10	Realizar la restauración de la copia de seguridad solicitada.	Profesional de la Oficina TIC	Log Aplicación.
11	Enviar correo con respuesta informando la restauración de la copia de seguridad correspondiente.	Profesional de la Oficina TIC	Correo Institucional
12	Validar a satisfacción con el usuario solicitante la restauración de la copia de seguridad.	Profesional de la Oficina TIC Usuario solicitante	Caso o tiket en la herramienta de gestión de incidentes
13	Generar el reporte de restauración validando en la carpeta final de respaldo de la información que se encuentra la información solicitada.	Profesional de la Oficina TIC	Caso o tiket en la herramienta de gestión de incidentes
FIN DE PROCEDIMIENTO RESTAURACION			

9. PUNTOS DE CONTROL

N°	Actividad	¿Qué se controla?	¿Con qué frecuencia?	¿Quién lo controla?	Riesgos Asociados
1	Definir mediante una política de seguridad en el controlador de dominio la ejecución automática de la copia de toda información alojada en la carpeta Documentos_CVP o en la unidad Z: de cada uno de los usuarios de la entidad con los parámetros establecidos por los responsables de la información; la cual será respaldada en un servidor serv_cv11	La ejecución de las copias de seguridad y las restauraciones	Cada vez que se requiera a través de la herramienta de gestión de incidentes tecnológicos	Profesional de la Oficina TIC	Perdida de información
2	Definir que todo equipo de cómputo unido al controlador de dominio de la CVP y autenticado con una cuenta de la misma, realizara una copia automática de seguridad.	La cantidad de equipos para realizar copia de seguridad y restauraciones	Cada vez que se requiera a través de la herramienta de gestión de incidentes tecnológicos	Profesional de la Oficina TIC	Perdida de información
3	Revisar los archivos de log de auditoria del servidos utilizado para el alojamiento de copias de seguridad	La disponibilidad de las copia de seguridad	Según definido en la política	Profesional de la Oficina TIC	Continuidad del negocio
4	Verificar que las copias de seguridad realizadas queden almacenadas en el primer nivel de respaldo				
5	Verificar que las copias de seguridad de bases de datos realizadas queden guardadas en el segundo nivel de respaldo DATA CENTER EXTERNO con el proveedor de servicio de alojamiento en la nube				
6	Revisar periódicamente la disponibilidad de espacio en el repositorio y DATA CENTER EXTERNO.				

9	Verificar la existencia de la copia de seguridad en el primer nivel de respaldo teniendo en cuenta los criterios establecidos en el correo de solicitud.				
12	Validar a satisfacción con el usuario solicitante la restauración de la copia de seguridad.	La disponibilidad de las copia de seguridad	Cada vez que se requiera	Profesional de la Oficina TIC Usuario solicitante	Perdida de información

10. DIAGRAMA DE FLUJO

N.A.

11. ANEXOS

N.A.

12. CONTROL DE CAMBIOS

Versión	Fecha Aprobación (dd-mmm-aaaa)	Cambios	Revisó (Nombre y Cargo)
1	05-11-2015	Versión 1 del procedimiento	Martha Liliana González Directora de Gestión Corporativa y CID
2	21-08-2019	Se actualiza el procedimiento en los siguientes apartes: Responsable del Procedimiento Normatividad Documentos de Referencia Condiciones Generales Descripción de actividades del Procedimiento Se solicita la eliminación del Diagrama de Flujo del procedimiento	Andrés Briceño Díaz Jefe Oficina TIC