	Responsable del Proceso	**Dirección de Planeación**
	Aprobación	**Revisión Técnica**
Firma:		
Nombre:	CARMEN ROSA MENDOZA SUÁREZ	GABRIEL HERNÁN MÉNDEZ CAMACHO
Cargo:	Directora Técnica.	Director Técnico.
Dependencia:	Dirección de Tecnologías de la Información y las Comunicaciones.	Dirección de Planeación.
R.R. Nº 019		**Fecha: 21 de septiembre de 2020**

OBJETIVO:

Establecer las actividades para hacer copias de respaldo de la información institucional de la Contraloría de Bogotá D.C., para proteger la información de la entidad contra pérdida o daño de datos y disponer de un medio externo para recuperar la información en un momento determinado.

2. ALCANCE:

Inicia con las actividades para la realización de las copias de respaldo de la información institucional de la Contraloría de Bogotá, D.C., y termina con la devolución de las cintas utilizadas para el proceso de restauración al sitio de almacenamiento, diligenciando la Bitácora Gestión de Copias de Respaldo.

3. BASE LEGAL:

Definir el entorno normativo externo e interno sobre el cual se basa o afecta el procedimiento, bajo la estructura siguiente:

NORMA	FECHA (dd/mm/aaaa)	DESCRIPCIÓN
Ley 1273	5-ene-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 información y las comunicaciones, entre otras disposiciones.

COPIA CONTROLADA

NORMA	FECHA (dd/mm/aaaa)	DESCRIPCIÓN
Ley 1437	18-ene-2011	Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo, Título III Capitulo IV- Utilización de medios electrónicos en el procedimiento administrativo.
Ley 1581	17-oct-2012	Por la cual se dictan disposiciones generales para la protección de datos personales, en lo referente a la regulación vigente para la protección del derecho fundamental que tienen todas las personas naturales a autorizar la información personal que es almacenada en bases de datos o archivos, así como su posterior actualización y reglamentada parcialmente por el Decreto Nacional No. 1377 de 2013.
Ley 1712	06-mar-2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Decreto 1008	14-jun-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.
Resolución 305 de la Secretaría General Alcaldía Mayor de Bogotá D.C. - Comisión Distrital de Sistemas – CDS	20- oct-2008	Por la cual se expiden las Políticas Públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre", la cual fue modificada por la Resolución 004 del 28 de noviembre de 2017.
Norma NTC-ISO/IEC COLOMBIANA 27001:2013	11-dic-2013	Norma Técnica Colombiana - Requisitos del Sistema de Gestión de la Seguridad de la Información.
Norma GTC-ISO/IEC 27002:2015	22-jul-2015	Guía Técnica Colombiana ISO - Tecnologías de la Información. Técnicas de Seguridad. Código de Práctica para Controles de Seguridad de la Información.
Norma NTC ISO 22301: 2019	30-oct-2019	Seguridad y resiliencia. Sistemas de gestión de la continuidad del negocio. Requisitos.

COPIA CONTROLADA

4. DEFINICIONES:

ACTIVO (Inglés: Asset)**:** Cualquier cosa que tenga valor para un individuo, una organización o un gobierno[1].

ACTIVO DE INFORMACIÓN: Conocimiento o datos que tienen valor para el individuo u organización[2].

En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la organización[3].

APLICATIVO: Programa informático que facilita las tareas de procesamiento, consulta, modificación, eliminación o reportes sobre las bases de datos de información de la Contraloría de Bogotá y que es manejado por usuarios específicos.

HERRAMIENTA PARA COPIA DE RESPALDO: Software para la realización automática de copia de respaldo, la cual automatiza los procesos de respaldo de la información desde disco o cinta para permitir la restauración de la información en caso de presentarse una contingencia sobre la información.

BASE DE DATOS: Conjunto de datos que son almacenados y organizados de acuerdo con el tipo de información que maneja un proceso.

COPIA DE RESPALDO: Es un respaldo de los datos y la información de un usuario o entidad que están almacenados en un ordenador[4], con el propósito de disponer de un medio para recuperarlos ante una eventual pérdida.

DATACONTRABOG (\\Datacontrabog): Espacio el servidor, asignado a las diferentes dependencias de la entidad, para almacenar la información institucional en forma electrónica conforme a la serie y subserie establecida en la TRD – Tabla de Retención Documental vigente, cuya responsabilidad de la administración corresponde a cada dependencia. El usuario lo visualiza en el explorador de archivos o directorio de archivos, en la carpeta, que se identifica con un icono que simboliza un disco con el nombre (\\Datacontrabog) (X:)".

La Dirección de Tecnologías de la Información y las Comunicaciones, realizará las copias de respaldo a la información institucional que las dependencias almacenen en Datacontrabog.

[1] Tomado de la Norma ISO/IEC 27032:2012 (definición 4.6, traducida al español), disponible en Internet en: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en.
[2] Ibídem (definición 4.27, traducida español).
[3] Tomado del Portal de ISO 27001 en español, Gestión de Seguridad de la Información. En http://www.iso27000.es/glosario.html#section10a.
[4] Roa Buendía, José Fabián. Seguridad Informática. Madrid: MacGraw-Hill España, 2013. p. 94.

COPIA CONTROLADA

DOCUMENTO ELECTRÓNICO: Es la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares. Se encuentran documentos ofimáticos (Word, Excel, etc.), cartográficos (mapas y planos), correos electrónicos, imágenes, videos, audio, mensajes de datos de redes sociales, formularios electrónicos, bases de datos, páginas WEB, entre otros.

FRECUENCIA DE COPIA DE RESPALDO: Periodo definido para realizar una copia de respaldo, el cual puede ser diaria, semanal, mensual, o como se defina.

INFORMACIÓN: Es un activo que, como otros activos importantes del negocio, es esencial para el negocio de una organización y, por consiguiente, necesita ser debidamente protegida[5].

LIBRERÍA O GRUPO DE MEDIOS: Es el nombre dado a un conjunto de cintas que se agrupan lógicamente y se utilizan exclusivamente para un trabajo de copia de seguridad, el cual no puede sobrescribirse hasta que se cumplan ciertos criterios especificados en las políticas de retención y rotación.

MEDIOS DE ALMACENAMIENTO DE INFORMACIÓN: Son dispositivos capaces de leer y escribir información con el propósito de almacenarla permanentemente. Actualmente existen muchas clases y categorías de unidades de almacenamiento, encontrando en el mercado una gran variedad de dispositivos internos o externos capaces de almacenar una gran cantidad de datos.

SISTEMA DE INFORMACIÓN: Se refiere a aplicaciones, servicios, activos de tecnologías de la información, y otros componentes para manejar la información.

RECURSOS TECNOLÓGICOS: Son aquellos componentes de hardware y software tales como: servidores virtuales, bases de datos, archivos, carpetas, aplicativos, repositorios electrónicos, configuraciones, entre otros, los cuales tienen como finalidad apoyar las tareas misionales y administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de la entidad.

[5] Tomado de la Norma Técnica Colombiana NTC-ISO/IEC 27000:2017 (pág.13).

COPIA CONTROLADA

5. DESCRIPCIÓN DEL PROCEDIMIENTO:

5.1 Realización de Copias de Respaldo.

Nº	RESPONSABLE	ACTIVIDAD	REGISTRO	PUNTOS DE CONTROL / OBSERVACIONES
1	Profesional o Técnico de la Dependencia (Administrador del recurso tecnológico)	Diligencia el reporte del recurso tecnológico para copia de respaldo (Anexo 1), con las solicitudes de creación y actualización de copias de respaldo que se requieran y solicita el servicio en la mesa de servicios.	Reporte del recurso tecnológico para copia de respaldo (PGTI-03-01)	**Observación:** Establecer los aspectos requeridos para respaldo de la información, establecidos en el Anexo 1. Esta actividad se realiza cada vez que se generen novedades de creación, modificación, o eliminación de copias de respaldo de un recurso tecnológico.
2	Profesional o Técnico de la Dirección TIC (Responsable de copias de respaldo)	Consolida la información Reporte del recurso tecnológico para copia de respaldo (Anexo 2), en el Reporte consolidado de los recursos tecnológicos para copia de respaldo.	Reporte consolidado del recurso tecnológico para copia de respaldo (PGTI-03-02)	**Punto de Control:** Verificar que las copias de respaldo se realicen conforme a los aspectos establecidos en el Reporte del recurso tecnológico para copia de respaldo y la herramienta vigente. **Observación:** Configura y realiza la tarea de copia de respaldo de acuerdo con lo descrito en el Anexo No. 6 - Lineamientos para las copias de respaldo y los recursos disponibles para esta actividad.

COPIA CONTROLADA

Nº	RESPONSABLE	ACTIVIDAD	REGISTRO	PUNTOS DE CONTROL / OBSERVACIONES
				La copia de respaldo se realiza de acuerdo con las configuraciones establecidas en la herramienta utilizada para la realización de estas copias de respaldo.
3	Profesional o Técnico de la Dirección TIC (responsable de copias de respaldo)	Monitorea y comprueba diariamente la ejecución de la copia de respaldo para asegurar que se realiza de manera completa y de acuerdo con las especificaciones establecidas.	Reporte de monitoreo generado por la herramienta utilizada para la realización de las copias de respaldo.	**Observación:** En caso de falla de la tarea de copia de respaldo, identificar la causa, realizar diagnóstico, establecer las acciones a ejecutar para su solución y volver a realizar la copia de respaldo. En los casos en que el responsable de copias de respaldo no pueda dar solución a la falla presentada, informa a los responsables del recurso tecnológico, para establecer medidas tendientes a mitigar el evento y tomar medidas alternativas.
4	Profesional o Técnico de la Dirección TIC (Responsable de copias de respaldo)	Replica mensualmente las copias de respaldo en un medio diferente al normalmente utilizado (Librería de cintas, discos externos, almacenamiento en la nube, entre otros). Rotula el medio de almacenamiento con el Rótulo para identificar medios de almacenamiento (Anexo 5).	Rótulo para identificar medios de almacenamiento PGTI-03-05	**Punto de Control:** Para asegurar y garantizar que los medios de respaldo estén en perfectas condiciones y que se puede depender de ellos ante emergencias, se pondrán a prueba regularmente, para lo cual el Subdirector de Recursos Tecnológicos

COPIA CONTROLADA

Nº	RESPONSABLE	ACTIVIDAD	REGISTRO	PUNTOS DE CONTROL / OBSERVACIONES
				solicitará trimestralmente la restauración aleatoria de una copia de respaldo de cualquier recurso tecnológico (servidores virtuales, bases de datos, archivos, carpetas, aplicativos, repositorios electrónicos, configuraciones, entre otros) **Observación:** Realiza la tarea de replica mensual de las copias de respaldo de acuerdo con lo descrito en el Anexo 6 - Lineamientos para las copias de respaldo.
5	Profesional o Técnico de la Dirección TIC (Responsable de copias de respaldo)	Relaciona los medios de almacenamiento que van para custodia externa en la Bitácora Gestión de Copias de Respaldo (Anexo 3).	Bitácora Gestión de Copias de Respaldo. (PGTI-03-03)	
6	Subdirector de Recursos tecnológicos	Revisa y aprueba la Bitácora Gestión de Copias de Respaldo (Anexo 3).	Bitácora Gestión de Copias de Respaldo. (PGTI-03-03)	
7	Secretario o Técnico de la Dirección TIC	Traslada las réplicas relacionadas en la Bitácora para la sede destinada para custodia externa del medio de almacenamiento.	Bitácora Gestión de Copias de Respaldo. (PGTI-03-03)	**Punto de control:** El formato debe ser revisado y firmado por las personas que entregan y reciben los medios en la sede externa.

COPIA CONTROLADA

5.2 Restauración de Copias de Respaldo.

Nº	RESPONSABLE	ACTIVIDAD	REGISTRO	PUNTOS DE CONTROL / OBSERVACIONES
1	Profesional o Técnico de la Dependencia (Administrador del recurso tecnológico) o Jefe de la dependencia	Solicita a través de la mesa de servicios, la restauración de la copia de respaldo, diligenciando y anexando la solicitud de restauración de copias de respaldo (Anexo 4).	Solicitud de restauración de copias de respaldo (PGTI-03-04)	**Observación:** El formato PGTI-03-04 - Solicitud de restauración de copias de respaldo deberá contener la autorización por parte del responsable del recurso tecnológico o jefe de la dependencia. La solicitud mesa de servicios debe provenir del responsable del recurso tecnológico o jefe de la dependencia. Para la restauración de los archivos del Datacontrabog, la solicitud la realiza el Jefe de la dependencia solicitante.
2	Profesional o Técnico de la Dirección TIC (responsable de copias de respaldo)	Revisa la completitud de la solicitud de restauración de copias de respaldo. Si el requerimiento está incompleto, devuelve la solicitud para los ajustes requeridos.	Registro en la mesa de servicios	**Observación:** Se debe documentar la novedad en el caso de la mesa de servicios.
3	Profesional o Técnico de la Dirección TIC (responsable de copias de respaldo)	Identifica en la herramienta utilizada para la realización de las copias de respaldo la información a restaurar de acuerdo con lo solicitado.		**Observación:** En caso de que la información este en resguardo externo, se diligencia el formato PGTI-03-03 - Bitácora Gestión de Copias de Respaldo solicitando el medio.

COPIA CONTROLADA

Nº	RESPONSABLE	ACTIVIDAD	REGISTRO	PUNTOS DE CONTROL / OBSERVACIONES
4	Profesional Dirección TIC (Administrador Centro de Cómputo) Profesional o Técnico de la Dirección TIC (Responsable de copias de respaldo)	Verifica en conjunto con el Administrador del Centro de Computo los recursos necesarios (como espacio en disco, máquinas virtuales, configuraciones especificas entre otros) para la restauración y en caso de requerir más recursos (ejemplo especio o disco) los deberán solicitar al Subdirector de Recursos Tecnológicos.		**Observación:** El administrador del centro de cómputo informa y apoya los detalles técnicos de la configuración requerida para que el responsable de copias de respaldo continúe con la actividad de restauración.
5	Profesional Dirección TIC (Administrador Centro de Cómputo) Profesional o Técnico de la Dirección TIC (responsable de copias de respaldo)	Realiza las configuraciones, adecuaciones y cambios requeridos para efectuar la restauración solicitada.		**Observación:** El administrador del centro de cómputo deberá revisar las hojas de vida de los recursos tecnológicos para validar las configuraciones normales requeridas.
6	Profesional o Técnico de la Dirección TIC (Responsable de copias de respaldo)	Ejecuta las verificaciones respectivas de la información restaurada y se documenta en la Bitácora Gestión de Copias de Respaldo (Anexo 3).	Bitácora Gestión de Copias de Respaldo. (PGTI-03-03)	**Observación:** Se documenta el resultado de las verificaciones conforme a las pruebas realizadas con el Administrador de centro de cómputo.

COPIA CONTROLADA

Nº	RESPONSABLE	ACTIVIDAD	REGISTRO	PUNTOS DE CONTROL / OBSERVACIONES
7	Profesional o Técnico de la Dirección TIC (Responsable de copias de respaldo)	Registra la información del resultado de la restauración en la solicitud de Restauración de Copia de respaldo (Anexo 4), en la sección identificada para uso del Responsable de copias de respaldo. Actualiza el estado de la solicitud en la mesa de servicio a “solucionado” y adjuntar el formato diligenciado. En caso de que no se logre la restauración, se informa al Subdirector(a) de Recursos Tecnológicos y/o a Director(a) para establecer las acciones a seguir y el caso en la mesa de servicios se modifica a estado “suspendido”, relacionando las causas que lo genera, hasta dar solución al requerimiento.	Solicitud de Restauración de Copia de respaldo (PGTI-03-04) Registro en la mesa de servicios	**Punto de Control:** Verificar con el área solicitante la conformidad de la restauración, antes de cerrar el caso.
8	Profesional o Técnico de la Dirección TIC (Responsable de copias de respaldo)	Devolver las cintas utilizadas para el proceso de restauración al sitio de almacenamiento, diligenciando la Bitácora Gestión de Copias de Respaldo (Anexo 3).	Bitácora Gestión de Copias de Respaldo (PGTI-03-03)	**Observación:** En caso de realizar la restauración desde las copias almacenadas en el servidor de copias de respaldo, se documentará en el formato PGTI-03-04 - Solicitud de Restauración de Copia de respaldo.

COPIA CONTROLADA

6. ANEXOS

ANEXO No. 1 Reporte del recurso tecnológico para copia de respaldo.

	REPORTE DEL RECURSO TECNOLÓGICO PARA COPIA DE RESPALDO.	Código formato: PGTI-03-01 Versión: 2.0
		Código documento: PGTI-03 Versión: 8.0
		Página 1 de 1

PARA SER DILIGENCIADO POR EL ADMINISTRADOR DEL RECURSO TECNOLÓGICO

FECHA SOLICITUD (DD/MM/YYYY)	NOMBRE DEL RECURSO TECNOLÓGICO QUE REQUIERE COPIA DE RESPALDO	TIPO	SERVIDOR	RUTAS DE DIRECTORIOS O NOMBRES DE RECURSOS A RESPALDAR	FUNCIONARIO ADMINISTRADOR DEL RECURSO TECNOLÓGICO	PERIODICIDAD	HORARIO DE RESPALDO (Hora en la cual se debe hacer la copia)	TIPO DE COPIA DE RESPALDO	RETENCIÓN (Tiempo de permanencia en custodia)	OBSERVACIÓN
14/06/2019	Ejemplo: APLICATIVO SIGESPRO	Carpeta	vmsever05	C:.... e:\Datos D: PDF FIRMADOS.	MANUEL	Diaria	11 p.m	Full		Son los archivos que corresponden a la configuración del aplicativo.
14/06/2019	Ejemplo: BASE DE DATOS SIGESPRO	Base de Datos	VmServer03	SigesPro	MANUEL	Diaria	11 p.m	Incremental		Base de datos del Sistema SIGESPRO
NOMBRE DEL RESPONSABLE DEL RECURSO TECNOLÓGICO:										

INSTRUCCIONES DE DILIGENCIAMIENTO	
PARA SER DILIGENCIADO POR EL SOLICITANTE	
Nombre campo	**Descripción del campo**
FECHA SOLICITUD (DD/MM/YYYY)	Fecha en la cual se realiza el reporte de recursos tecnológicos para copia de respaldo (Día/Mes/Año).
NOMBRE DEL RECURSO TECNOLÓGICO QUE REQUIERE COPIA DE RESPALDO	Nombre del recurso tecnológico que requiere copia de respaldo. Nota: Si un recurso tecnológico tiene más de un tipo, cada uno de los tipos se debe colocar en una fila y se establecerán las especificaciones en forma individual (ver ejemplo en el formato para el caso SIGESPRO).
TIPO	Registre el nombre del tipo de recurso tecnológico que requiere copia de respaldo. Para identificar los tipos tengan en cuenta los siguientes: Archivo; Carpeta; Base de Datos; Máquina Virtual; Configuración Switch; Logs; snapshot; otros.
SERVIDOR	Registre el nombre del servidor o la dirección IP del servidor donde se ubica el recurso tecnológico que requiere copia de respaldo.

COPIA CONTROLADA

INSTRUCCIONES DE DILIGENCIAMIENTO	
PARA SER DILIGENCIADO POR EL SOLICITANTE	
Nombre campo	**Descripción del campo**
RUTAS DE DIRECTORIOS O NOMBRES DE RECURSOS A RESPALDAR	Registre las rutas de directorio o nombres de recurso a respaldar (pueden ser aplicaciones y/o configuraciones).
FUNCIONARIO ADMINISTRADOR DEL RECURSO TECNOLÓGICO	Registre el nombre y apellido de la persona encargada de custodiar la información.
PERIODICIDAD (Diaria, Semanal, Mensual, Anual)	Registre la periodicidad de realización de la copia de respaldo, que puede ser diaria, semanal, mensual o anual.
HORARIO DE RESPALDO (Hora en la cual se debe hacer la copia)	En caso de que se requiera el respaldo en una hora en particular.
TIPO DE COPIA DE RESPALDO (Full, Incremental)	Registre la forma de realización de la copia de respaldo, que puede ser full, e incremental.
RETENCIÓN (Tiempo de permanencia en custodia)	Registre el tiempo de permanencia en custodia, de acuerdo con la retención que debe permanecer normativamente o por las características del proceso, definiciones de tiempo establecidas en la TRD para la información que se encuentra relacionada con los recursos tecnológicos.
OBSERVACIÓN	Consideraciones adicionales que deben ser tenidas en cuenta.

COPIA CONTROLADA

ANEXO No. 2 Reporte consolidado del recurso tecnológico para copia de respaldo.

	REPORTE CONSOLIDADO DEL RECURSO TECNOLÓGICO PARA COPIA DE RESPALDO	Código formato: PGTI-03-02 Versión: 1.0
		Código documento: PGTI-03 Versión: 8.0
		Página 1 de 1

FECHA SOLICITUD (DD/MM/YYYY)	NOMBRE DEL RECURSO TECNOLÓGICO QUE REQUIERE COPIA DE RESPALDO	SERVIDOR	RUTAS DE DIRECTORIOS O NOMBRES DE RECURSOS A RESPALDAR	FUNCIONARIO ADMINISTRADOR DEL RECURSO TECNOLÓGICO	FECHA EN LA CUAL SE INICIA RESPALDO (DD/MM/YYYY)	HORARIO DE RESPALDO (Hora en la cual se debe hacer la copia)	TIPO DE COPIA DE RESPALDO	JOB	POOL	MEDIOS	OBSERVACIÓN

INSTRUCCIONES DE DILIGENCIAMIENTO	
Nombre campo	**Descripción del campo**
FECHA SOLICITUD (DD/MM/YYYY)	Fecha en la cual se realiza el reporte de recursos tecnológicos para copia de respaldo (Día/Mes/Año).
NOMBRE DEL RECURSO TENOLÓGICO QUE REQUIERE COPIA DE RESPALDO	Nombre del recurso tecnológico que requiere copia de respaldo. Nota: Si un recurso tecnológico tiene más de un tipo, cada uno de los tipos se debe colocar en una fila y se establecerán las especificaciones en forma individual (ver ejemplo en el formato para el caso SIGESPRO).
SERVIDOR	Registre el nombre del servidor o la dirección IP del servidor donde se ubica el recurso tecnológico que requiere copia de respaldo.
RUTAS DE DIRECTORIOS O NOMBRES DE RECURSOS A RESPALDAR	Registre las rutas de directorio o nombres de recurso a respaldar (pueden ser aplicaciones y/o configuraciones).
FUNCIONARIO ADMINISTRADOR RECURSO TENOLÓGICO	Registre el nombre y apellido de la persona encargada de custodiar la información.
FECHA EN LA CUAL SE INICIA RESPALDO (DD/MM/YYYY)	Registre día, mes y año desde la cual se ejecutará la actividad de copia de respaldo.
HORARIO DE RESPALDO (Hora en la cual se debe hacer la copia)	En caso de que se requiera el respaldo en una hora en particular.
TIPO DE COPIA DE RESPALDO (Full, Incremental)	Registre la forma de realización de la copia de respaldo, que puede ser full, e incremental.
JOB	Nombre de la tarea programada en la herramienta de copia de respaldo, de acuerdo con las especificaciones diligenciadas en el formato.
POOL	Nombre utilizado para la agrupación de las cintas de acuerdo con la periodicidad.
MEDIOS	Relacionar los códigos de identificación de las cintas que están relacionadas con cada pool.
OBSERVACIÓN	Consideraciones adicionales que son requeridas para la ejecución de la actividad de copia de respaldo.

COPIA CONTROLADA

ANEXO No. 3 Bitácora Gestión de Copias de Respaldo.

	BITÁCORA GESTIÓN DE COPIAS DE RESPALDO	Código formato: PGTI-03-03 Versión: 1.0
		Código documento: PGTI-03 Versión: 8.0
		Página 1 de 1

TIPO DE MEDIO (CINTA / OTRO MEDIO)	IDENTIFICACIÓN DEL MEDIO	ACTIVIDAD EN CENTRO DE RESGUARDO		FECHA INGRESO O RETIRO (AAAA/MM/DD)	SE UTILIZA EL MEDIO PARA REALIZAR UNA RESTAURACIÓN (SI / NO)	LA RESTAURACIÓN ES SATISFACTORIA (SI / NO)	DESCRIPCIÓN	UBICACIÓN FISICA	FIRMAS	
		INGRESO	RETIRO						ENTREGA	RECIBE
	CB0181L6	X					Backup Full Mensual VM (Blade11, Blade03) WinFS fileserver14 (H:\), WinFS datacontrabog (F:\)			

INSTRUCCIONES DE DILIGENCIAMIENTO

Nombre campo	Descripción del campo
TIPO DE MEDIO (CINTA / OTRO MEDIO)	Registre el tipo de medio el cual se ingresa o retira del centro de resguardo, cinta u otros medios (disco duro, cd, dvd, entre otros)
IDENTIFICACIÓN DEL MEDIO	Registre la identificación del medio a resguardar. Para cintas diligencie el código de barras.
ACTIVIDAD EN CENTRO DE RESGUARDO (INGRESO/SALIDA)	Registre el tipo de actividad que se realiza en el centro de resguardo, ingreso o salida de medios.
FECHA INGRESO O RETIRO (AAAA/MM/DD)	Registre día, mes y año de ingreso o retiro del medio en el centro de resguardo (AAAA/MM/DD).
SE UTILIZA EL MEDIO PARA REALIZAR UNA RESTAURACIÓN (SI / NO)	Registre si el medio retirado del centro de resguardo es utilizado para realizar restauración de copia de respaldo (SI / NO).
LA RESTAURACIÓN ES SATISFACTORIA (SI / NO)	Registre si la restauración realizada fue satisfactoria (SI / NO).
DESCRIPCIÓN	Diligencie la información contenida en el medio a trasladar.
UBICACIÓN FÍSICA	Diligencie la ubicación en la que quedara custodiado el medio (Bodega, estante, entre otros).
FIRMAS (ENTREGA / RECIBE)	Registre las firmas de la persona que entrega y recibe los medios.

COPIA CONTROLADA

ANEXO No. 4 Solicitud de restauración de copias de respaldo.

	SOLICITUD DE RESTAURACIÓN DE COPIAS DE RESPALDO	Código formato: PGTI-03-04 Versión: 2.0
		Código documento: PGTI-03 Versión: 8.0
		Página 1 de 1

FECHA DE LA SOLICITUD (DD/MM/YYYY	
NOMBRE DEL SOLICITANTE:	
DEPENDENCIA:	

PARA SER DILIGENCIADO POR EL SOLICITANTE						**PARA USO DEL ADMINISTRADOR DE BACKUP**	
NOMBRE DEL RECURSO TECNOLÓGICO A RESTAURAR	**TIPO**	**SERVIDOR**	**RUTAS DE DIRECTORIOS O NOMBRES DE RECURSOS A RESTAURAR**	**FECHA DE CORTE DEL RECURSO TECNOLÓGICO A RESTAURAR (DD/MM/YYYY)**	**OBSERVACIÓN**	**FECHA DE LA RESTAURACIÓN (DD/MM/YYYY)**	**UBICACIÓN O DESCRIPCIÓN DE LA RESTAURACIÓN**
APLICATIVO SIGESPRO	CARPETA	vmsever05	C:.... e:\Datos D: PDF FIRMADOS.	01/01/2019	Son los archivos que corresponden a la configuración del aplicativo.		
BASE DE DATOS SIGESPRO	CARPETA	VmServer03	SigesPro	01/01/2019	Base de datos del Sistema SIGESPRO		

INSTRUCCIONES DE DILIGENCIAMIENTO	
Nombre campo	**Descripción del campo**
FECHA DE LA SOLICITUD	Fecha en que se solicita la restauración de la copia de respaldo. (Día/Mes/Año).
NOMBRE DEL SOLICITANTE	Nombre del administrador del recurso tecnológico o jefe de la dependencia (Líder funcional) quien hace la solicitud. Nota: Para la restauración de los archivos del Datacontrabog, la solicitud la debe realizar el Jefe de la dependencia solicitante.
DEPENDENCIA	Nombre de la dependencia solicitante.
PARA SER DILIGENCIADO POR EL SOLICITANTE	
NOMBRE DEL RECURSO TECNOLÓGICO A RESTAURAR	Registre el nombre del recurso tecnológico que requiere restaurar. Nota: Si un recurso tecnológico tiene más de un tipo, cada uno de los tipos se debe colocar en una fila y se establecerán las especificaciones en forma individual (ver ejemplo en el formato para el caso SIGESPRO).
TIPO	Registre el nombre del tipo de recurso tecnológico que requiere restaurar. Para identificar los tipos tengan en cuenta los siguientes: Archivo; Carpeta; Base de Datos; Máquina Virtual; Configuración Switch; Logs; snapshot; otros.
SERVIDOR	Registre el nombre del servidor o la dirección IP del servidor donde se realiza la restauración.
RUTAS DE DIRECTORIOS O NOMBRES DE RECURSOS	Registre las rutas de directorio o nombres de recurso a restaurar (pueden ser aplicaciones y/o configuraciones).
FECHA DE CORTE	Registre día, mes y año del corte del activo a restaurar.
OBSERVACIÓN	Hace referencia a información adicional de la restauración que se considere registrar.
PARA USO DEL ADMINISTRADOR DE COPIA DE RESPALDO	
FECHA DE LA RESTAURACIÓN	Registre día, mes y año de la restauración de la copia de respaldo.
UBICACIÓN O DESCRIPCIÓN DE LA RESTAURACIÓN	Especifique la ubicación donde fue restaurado la copia de respaldo o describa los aspectos que considere sean requeridos o la información adicional que considere el administrador de copia de respaldo.

COPIA CONTROLADA

ANEXO No. 5 Rótulo para identificar medios de almacenamiento.

	ROTULOS PARA MARCAR LOS MEDIOS DE ALMACENAMIENTO	Código formato: PGTI-03-05 Versión: 2.0
		Código documento: PGTI-03 Versión: 8.0
		Página 1 de 1

CONTRALORIA DE BOGOTA, D.C. - DIRECCION TIC. MEDIOS DE ALMACENAMIENTO			
CÓDIGO:		**POOL:**	
DESCRIPCIÓN:			
FECHA RETIRO ROBOT:		**FECHA RECIBO EN ARCHIVO:**	

Nota: El rótulo se debe ajustar de acuerdo al tamaño del sticker.

INSTRUCCIONES DE DILIGENCIAMIENTO	
Nombre campo	**Descripción del campo**
CÓDIGO	Relacionar el código de barras que identifica la cinta de copia de respaldo.
POOL	Registre el nombre en el cual se encuentra agrupada la cinta.
DESCRIPCIÓN	Registre brevemente la información almacenada en la cinta de copia de respaldo.
FECHA RETIRO ROBOT: (DD/MM/YYYY)	Fecha en la cual se realiza el reporte de recurso tecnológicos para copia de respaldo (Día/Mes/Año).
FECHA RECIBO EN ARCHIVO: (DD/MM/YYYY)	Fecha en la cual se realiza el reporte de recurso tecnológicos para copia de respaldo (Día/Mes/Año).
MEDIOS	Relacionar los códigos de identificación de las cintas que están relacionadas con cada pool.

COPIA CONTROLADA

ANEXO No. 6 Lineamientos para las copias de respaldo.

Los lineamientos que se describen a continuación proporcionan la documentación de las medidas tomadas para el respaldo de datos para la Entidad; Asimismo, sirven como evidencia de que el control aplicado para responder al cumplimiento de la disponibilidad de la información institucional se lleva a cabo correctamente y se tiene gestionado.

1. Todo el personal de la Dirección de Tecnologías de la Información y las Comunicaciones que administre o gestione un recurso tecnológico donde se almacene información institucional, debe realizar un inventario y clasificación de todo el software, configuraciones y datos imprescindibles, esto basado en la criticidad que representa su pérdida para la Entidad, el cual deberá ser relacionado en el formato PGTI-03-01 Reporte del recurso tecnológico para copia de respaldo. (Anexo 1 del procedimiento), el cual incluirá:
    a. de qué hacer copia,
    b. el tipo de copia,
    c. la periodicidad,
    d. la vigencia,
    e. su ubicación,
    f. y las pruebas de restauración, entre otros datos requeridos en el formato PGTI-03-01 Reporte del recurso tecnológico para copia de respaldo.

2. Si dentro de las copias de seguridad se incluye información personal, se tendrán que realizar las copias de seguridad basadas en la ley de protección de datos vigente y clausulas establecidas en contratos de terceros, para cumplir con dicha regulación.
3. Los datos que son críticos para la entidad deben ser definidos por las áreas propietarias y encargadas y deben ser respaldados.
4. Las copias de seguridad almacenarse en una ubicación que sea físicamente diferente de su ubicación original de creación y uso.
5. Las restauraciones de datos deberán probarse mínimo una vez cada semana.
6. Los procedimientos para hacer una copia de seguridad de los datos críticos y las pruebas de los procedimientos deberán documentarse y actualizarse según se requiera.
7. Todos los datos y software esenciales para la operación continua de la Contraloría de Bogotá, D.C, así como todos los datos que deben mantenerse para fines legislativos, deben ser respaldados.
8. Todo el material de respaldo requerido para procesar la información, también debe ser respaldado. Esto incluye software, hardware y documentación de procesos y procedimientos.
9. Se deben considerar los siguientes tipos de copias de seguridad:
    a. Copia de seguridad completa: se realiza una copia de todos los datos a una unidad de almacenamiento.
    b. Respaldo incremental: se realiza una copia de los datos que han sido modificados desde la última copia de seguridad.
    c. Copia de seguridad diferencial: se realiza una copia de los datos que han cambiado desde la última copia de seguridad completa.

COPIA CONTROLADA

10. Las copias de seguridad no deben interferir con las operaciones diarias; es posible que se requiera una ventana de operación para la generación de copias de seguridad, dependiendo de las condiciones requeridas por el responsable de copias de seguridad.
11. Las copias de seguridad deben realizarse con 30 puntos de restauración (uno por día), para garantizar que los datos puedan recuperarse en caso de una falla del sistema. Se tomará un punto de copia de seguridad completo y 29 incrementales. Finalizado cada mes, se realizará la copia de los 30 puntos de copias de seguridad a cinta, para conservar una copia de seguridad mensual
12. Las versiones de las vigencias anteriores deberán conservarse en una ubicación de almacenamiento fuera del sitio y por un mínimo de 10 años.
13. Las copias de seguridad anual y mensual deben conservarse en las instalaciones externas. Las copias de seguridad mensuales se pueden reutilizar para tomar nuevas copias de seguridad.
14. Las pruebas de recuperación deben ser documentadas y revisadas por el Subdirector de Recursos Tecnológicos.
15. Los lineamientos descritos en este procedimiento son complementarios a los detallados en el numeral 7.7., del documento PGTI-16 Versión 3.0 - POLITICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA CONTRALORIA DE BOGOTA, D.C.

COPIA CONTROLADA

7. CONTROL DE CAMBIOS

Versión	N° Acto Administrativo y Fecha	Descripción de la Modificación
1.0	R.R. No.001 24-ener-2003	Ver procedimiento, link normatividad.
2.0	R.R. No. 028 7-may-2003	Ver procedimiento, link normatividad.
3.0	R.R. No. 042 9-nov-2005	Ver procedimiento, link normatividad.
4.0	R.R. No. 035 30-dic-2009	Ver procedimiento, link normatividad.
5.0	R.R. No.018 12-jun-2017	Ver procedimiento, link normatividad.
6.0	R.R. No.007 16-feb-2018	Se actualiza la base legal, definiciones, actividades, responsables y puntos de control, lo anterior, teniendo en cuenta el objetivo técnico del procedimiento que es el proceso de copias de respaldo. Adicionalmente, se eliminaron las actividades y responsabilidades de la administración del espacio virtual (\\Datacontrabog) (X:)", dado que son propias de los Procedimientos para la Organización y Transferencias Documentales y para la Conservación, Seguridad y Recuperación de los Documentos en Archivo de Gestión y Archivo Central, dentro del Proceso Gestión Documental. La modificación del procedimiento es producto de la oportunidad de mejora de la Auditoría Interna al SGC de la vigencia 2019.
7.0	R.R. No.030 19-jul-2019	Se actualiza con las siguientes modificaciones: Se cambiar el nombre a "*Procedimiento para la Gestión de Copias de Respaldo*" – PGTI-03, en consideración a que las actividades establecidas abarcan toda la gestión de copias de respaldo, buscando su correcta administración y no solo la realización y control de las mismas. Se ajusta el objetivo, alcance, definiciones, base legal, numeración, actividades, responsables, observaciones, puntos de control y formatos, para actualizar y dar mayor claridad al procedimiento. Se ajusta el término Activo Informático por Recurso tecnológico, en todo el procedimiento y formatos, teniendo en cuenta que la definición establecida se ajusta al objeto de la copia de respaldo. Así mismo, incidente por situación y backup por copia de respaldo.

COPIA CONTROLADA

Versión	N° Acto Administrativo y Fecha	Descripción de la Modificación
		Se incluyó la actividad de envío a la custodia externa de los medios de respaldo utilizados en la restauración. Se ajusta el nombre del formato del anexo No.1 de Reporte de Activos Informáticos para Backup a "***Reporte del recurso tecnológico para copia de respaldo***". Así mismo, ajustar el formato eliminando los siguientes campos: fecha en la cual se inicia el respaldo (DD/MM/YYYY); para uso del administrador de backup (Job, Pool, Medios y Observaciones). Se elimina el formato No.2 "*Registro de Incidentes de copias de respaldo*" - PGTI-03-02, dado que la información será manejada en el nuevo formato de bitácora y debido a que el termino incidente se ajusta a falla. Se incluye en el anexo 2, un nuevo formato *"**Reporte consolidado del recurso tecnológicos para copia de respaldo***" - PGTI-03-02, con el consolidado para copia de respaldo. Se incluye el anexo 3 con un nuevo formato ***"Bitácora Gestión de Copias de Respaldo***" - PGTI-03-03, para hacer seguimiento y control a las copias y las restauraciones y donde se relacionan los medios de almacenamiento que van para custodia externa. Se ajustan los códigos de los formatos, de conformidad al orden que figuran en el procedimiento, en este sentido el formato Solicitud de restauración de copias de respaldo, cambia a PGTI-03-04. Se ajusta el nombre del formato del anexo No.5 Rótulo para marcar las cajas de las cintas de copias de respaldo de almacenamiento a "***Rótulo para identificar medios de almacenamiento***". Se incluye el ANEXO No. 6 Lineamientos para las copias de respaldo, con el fin de proporcionar la documentación de las medidas tomadas para el respaldo de datos para la entidad; Asimismo para que sirvan como evidencia de que el control aplicado para responder al cumplimiento de la disponibilidad de la información institucional se lleva a cabo correctamente y se tiene gestionado.
8.0	R.R. No. 019 del 21 de septiembre de 2020	

COPIA CONTROLADA