**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.

# 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:

* + - 1. de qué hacer copia,
      2. el tipo de copia,
      3. la periodicidad,
      4. la vigencia,
      5. su ubicación,
      6. y las pruebas de restauración, entre otros datos requeridos en el formato PGTI-03-01 Reporte del recurso tecnológico para copia de respaldo.

# 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.

# Los datos que son críticos para la entidad deben ser definidos por las áreas propietarias y encargadas y deben ser respaldados.

# Las copias de seguridad almacenarse en una ubicación que sea físicamente diferente de su ubicación original de creación y uso.

# Las restauraciones de datos deberán probarse mínimo una vez cada semana.

# 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.

# 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.

# Todo el material de respaldo requerido para procesar la información, también debe ser respaldado. Esto incluye software, hardware y documentación de procesos y procedimientos.

# Se deben considerar los siguientes tipos de copias de seguridad:

1. Copia de seguridad completa: se realiza una copia de todos los datos a una unidad de almacenamiento.
2. Respaldo incremental: se realiza una copia de los datos que han sido modificados desde la última copia de seguridad.
3. Copia de seguridad diferencial: se realiza una copia de los datos que han cambiado desde la última copia de seguridad completa.

# 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.

# 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

# Las versiones de las vigencias anteriores deberán conservarse en una ubicación de almacenamiento fuera del sitio y por un mínimo de 10 años.

# 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.

# Las pruebas de recuperación deben ser documentadas y revisadas por el Subdirector de Recursos Tecnológicos.

# Los lineamientos descritos en este procedimiento son complementarios a los detallados en el numeral 7.7., del documento PGTI-16 POLITICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA CONTRALORIA DE BOGOTA, D.C.