Resolución Número 397
(Julio 10 de 2020)

"Por la cual se adopta el documento P-DT-019 Procedimiento para realizar copias de respaldo y restauración de información"

EL JEFE DE LA OFICINA ASESORA DE PLANEACIÓN DE LA EMPRESA DE TRANSPORTE DEL TERCER MILENIO "TRANSMILENIO S.A.", En uso de sus facultades conferidas mediante la Resolución 342 del 16 de junio de 2020, y

CONSIDERANDO:

Que de conformidad con lo señalado en el artículo segundo del Acuerdo 4 de 1999, corresponde a TRANSMILENIO S.A., la gestión, organización y planeación del servicio de transporte público masivo urbano de pasajeros en el Distrito Capital y su área de influencia, bajo la modalidad de transporte terrestre automotor.

Que cumpliendo con lo ordenado en el parágrafo único del artículo 1º de la Ley 87 de 1993, se adoptó el Manual de Procedimientos de TRANSMILENIO S.A.

Que, siendo TRANSMILENIO S.A., el ente gestor del Sistema Integrado de Transporte Público, considera necesario actualizar los Manuales de Procedimientos de las diferentes dependencias de la Entidad, con el objeto de ajustarlos a los nuevos parámetros documentales, necesidades y desarrollo del Sistema.

En mérito de lo expuesto,

RESUELVE:

ARTÍCULO 1°: Adoptar el siguiente documento con el nombre, código y versión que se registran a continuación:

CÓDIGO	VERSIÓN	NOMBRE
P-DT-019	0	Procedimiento para realizar copias de respaldo y restauración de información

ARTÍCULO 2°: La presente Resolución rige a partir de su publicación en la Gaceta Distrital.

PUBLÍQUESE Y CÚMPLASE

Dada en Bogotá, D.C., a los diez (10) días del mes de julio de dos mil veinte (2020).

SOFÍA ZARAMA VALENZUELA
Jefe de Oficina Asesora de Planeación

TABLA DE CONTENIDO

1. OBJETO

Establecer los responsables y las actividades a seguir para la realización de copias de respaldo de los sistemas de información y la información de los usuarios en TRANSMILENIO S.A.

2. ALCANCE

Este procedimiento es para aplicación y conocimiento de los funcionarios y contratistas de la Entidad.

De igual forma, el documento contempla los pasos que se deben seguir para la copia de respaldo de los sistemas de información (Bases de datos) e información de los usuarios, incluyendo la solución de hiperconvergencia, configuración de dispositivos de comunicación y redes e información vinculada a cuenta en plataforma office365.

3. RESPONSABLES

Los responsables por la elaboración y actualización de este procedimiento son el Profesional Especializado Grado 06 - Coordinador de Procesos Corporativos de TI y el Profesional Especializado Grado 06 - Seguridad Informática. Por su estricto cumplimiento, implementación y mantenimiento velará el(la) Director(a) de TIC.

Por su aplicación, serán responsables todos los usuarios funcionales que interactúen directa o indirectamente en el proceso de copias de respaldo de TRASMILENIO S.A.

La revisión y/o actualización de este procedimiento deberá realizarse cuando se considere pertinente por parte de los responsables de su aplicación y cumplimiento.

4. DOCUMENTOS DE REFERENCIA

- **Constitución Política de Colombia de 1991**

Artículo 2.	Fines Esenciales del Estado.
Artículo 6.	Responsabilidad de los servidores públicos.
Artículo 15.	Derecho a la Intimidad. Hábeas Data.
Artículo 20.	Derecho a la Información.

Artículo 74.	Libre Acceso a Documentos Públicos.
Artículo 122.	Desempeño de Funciones Públicas.
Artículo 123.	Desempeño de funciones de los Servidores Públicos.
Artículo 209.	Fines de la Función Administrativa.
Artículo 269.	Métodos y Procedimientos de Control Interno.
Artículo 284.	Acceso a Información Reservada.

- **Ley 23 de 1982:** Ley emitida por el Congreso de la República de Colombia, acerca de la Propiedad Intelectual y los Derechos de autor.

- **Ley 527 de 1999**: 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, se establecen las entidades de certificación y se dictan otras disposiciones.

- **Ley 603 del 2000:** Ley emitida por el Congreso de la República de Colombia, acerca del cumplimiento de las Normas de Propiedad Intelectual

- **Ley 1266 de 2008:** Por la cual se dictan las disposiciones generales del Habeas Data y se regula el manejo de la información contendida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

- **Ley 1273 de 2009.** Por medio del 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, el cual establece en su “Capítulo I De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos” así:
    - Artículo 269A: Acceso abusivo a un Sistema Informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático
    - Artículo 269B: Obstaculización Ilegítima de Sistema Informático o Red de Telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático.
    - Artículo 269C: Interceptación de Datos Informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático.

- Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos.
- Artículo 269E: Uso de Software Malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos.
- Artículo 269F: Violación de Datos Personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes
- Artículo 269G: Suplantación de Sitios Web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes.

- **Ley 1341 de 2009.** Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones acerca de la protección de los derechos de los usuarios.

- **Ley 1520 de 2012.** Por medio de la cual se implementan compromisos adquiridos por virtud del "Acuerdo de Promoción Comercial", suscrito entre la República de Colombia y los Estados Unidos de América y su "Protocolo Modificatorio, en el Marco de la Política de Comercio Exterior e Integración Económica"

- **Ley 1581 de 2012.** Por la cual se dictan disposiciones generales para la protección de datos personales, habeas data

- **Decreto 1360 de 1989.** Por el cual se reglamenta la inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor.

- **Decreto 162 de 1995.** Por el cual se reglamenta en relación con las Sociedades de Gestión Colectiva de Derecho de Autor o de Derechos Conexos.

- **Decreto 460 de 1995.** Por el cual se reglamenta el Registro Nacional del Derecho de Autor y se regula el Depósito Legal.

- ISO/IEC 27001:2013 Norma técnica que describe los requerimientos del Sistema de Seguridad de la Información (*Information technology - Security techniques - Information security management systems - Requirements*) aprobado y publicado por la ISO International Organization for Standardization y por la IEC International Electrotechnical Commission.

- ISO/IEC 27002:2013 Documento que recopila el código de práctica y los controles para la gestión de la seguridad de la información (*Information technology - Security techniques - Code of practice for information security management*) aprobado y publicado por la ISO International Organization for Standardization y por la IEC International Electrotechnical Commission.

5. DEFINICIONES

Activo: cualquier elemento que tiene valor para la Entidad.

Almacenamiento externo: se refiere al servicio de custodia de medios físicos con la información respaldada por las herramientas de la entidad.

Autenticidad: es la propiedad de garantizar la identidad de un sujeto o recurso declarado. Se aplica a entidades tales como usuarios, procesos, sistemas e información.

Backup: copia total o parcial de información importante del disco duro, CDs, bases de datos u otro medio de almacenamiento, la cual puede recuperarse en caso de pérdida de la copia original.

Bases de datos: "almacén" que nos permite guardar grandes cantidades de información de forma organizada para que luego podamos encontrar y utilizar fácilmente. Conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.

Confidencialidad: propiedad de determinar que la información no esté disponible ni sea revelada a individuos, entidades, procesos o procedimientos no autorizados. GGGG

Cuentas vinculadas a Office 365: esta información corresponde a los buzones de correo electrónico, archivos almacenados en la herramienta Onedrive, Sharepoint y demás proporcionadas dentro del contrato con Microsoft y que se respaldan en la nube.

Datos: elemento aislado, recabado para un cierto fin, pero que no ha pasado por un proceso que lo interrelacione con otros de manera funcional para el fin previsto.

Disponibilidad: propiedad de la información de ser accesible y utilizable por solicitud de una Entidad o funcionarios autorizados.

Firewall: ordenador, software o dispositivo físico que se conecta en una red con salida a Internet con el fin de impedir el acceso no autorizado, incorporando elementos que garantizan la privacidad, autentificación, etc., conforme a las políticas de seguridad.

Hardware (Hw): partes físicas y tangibles de una computadora, sus componentes eléctricos, electrónicos, electromecánicos y mecánicos, sus cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado.

Hiperconvergencia: Solución compuesta por hardware y software que combina almacenamiento, cómputo y redes en un único sistema para reducir la complejidad de un centro de datos y aumentar su escalabilidad.

Información de usuarios: documentos y archivos el formato digital que es generada por los usuarios como parte de sus labores, así como la generada por terceros en custodia de los usuarios. Esta información es aquella que se almacena por parte del usuario en la unidad P:\ dentro del servidor de archivos.

Información de configuración de equipos de comunicaciones y redes: esta información contempla los archivos de configuración que es respaldada por el proveedor de comunicaciones y redes. Incluye políticas de firewall, políticas de equipos de red, rutas, configuraciones de interfaces u otros parámetros que el contratista requiera para garantizar su respectivo respaldo.

Integridad: propiedad de salvaguardar la exactitud y estado completo de los activos.

Intranet: red privada de computadoras que permite compartir recursos entre ellas y se encuentra enlazada. Puede o no tener acceso a Internet.

ISO (International Organization for Standardization): deriva del griego ISOS, que significa "igual"; Organización creada el 23 de Febrero de 1947, en Ginebra, Suiza, con el fin de “facilitar la coordinación internacional y unificación de normas industriales". Actualmente son miembros 165 países.

Políticas: actividad orientada en forma ideológica a la toma de decisiones de un grupo para alcanzar ciertos objetivos. Acción elegida como guía en el proceso de toma de decisiones al poner en práctica o ejecutar las estrategias, programas y proyectos específicos del nivel institucional.

Respaldo de datos o de información: se refiere a la tarea de copia y almacenamiento de los datos de los usuarios, cuentas de office 365, bases de datos entre otra información que se resguarda con el fin de contar con una contingencia en caso de que la información original sea eliminada, modificada o destruida, ya sea de forma accidental o intencional.

Restauración de información: se refiere a la actividad de recuperación de la información desde los archivos de respaldo de datos o de información. Esta tarea se realiza como prueba periódica con el fin de validar que las copias de respaldo de datos o de información se haya realizado correctamente, así como cuando se requiera recuperar un dato borrado, eliminado o destruido, de forma accidental o intencional.

Riesgo: potencial de que una amenaza determinada aproveche las vulnerabilidades de una activo o grupo de activos y produzca daño a la Entidad. Se mide en términos de la combinación de la probabilidad de un evento y sus consecuencias.

Seguridad informática: consiste en preservar la confidencialidad, integridad y disponibilidad de la información; además puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad.

Sistema de gestión de la seguridad de la información SGSI: parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

Sistemas de información: software y programas que utiliza la entidad para el cumplimiento de sus objetivos.

Terceros: personal que pertenece a empresas que proveen servicios a TRASMILENIO S.A.

TICs (Tecnologías de la Información y las Comunicaciones): es la dirección dentro de la entidad que se encarga de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones. Dentro de sus funciones está incrementar y facilitar el acceso de los usuarios de la Entidad a las Tecnologías de la Información, las Comunicaciones y a sus beneficios.

Tipo de respaldo: Se refiere a los tipos de copias que se realizan en un proceso de respaldo

Usuarios: funcionarios, empleados contratados, consultores y contratistas que tienen algún vínculo con TRANSMILENIO S.A.

Vulnerabilidad: debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas.

Web: significa “red”, “telaraña” o “malla”. El concepto se utiliza en el ámbito tecnológico para nombrar a una red informática y, en general a Internet.

6. CONDICIONES GENERALES

- Los responsables de la Dirección de TIC encargados de entregar los equipos de cómputo deberán configurar en cada equipo cuando el usuario ingresa a la entidad, de la siguiente manera: Nombre de usuario (\\server-file\DEPENDENCIA)(P:)

  Por ejemplo: PEPITO PEREZ (\\server-file\DIRECCION DE TIC´S) (P:)

- Es responsabilidad de todos los usuarios guardar la información institucional en la unidad (P): configurada por la Dirección de TIC.

- Todos los casos de solicitudes de respaldo y/restauración de información deben ser notificados a través de la mesa de ayuda.

- No se podrá almacenar en los equipos de cómputo asignados por la Entidad información de índole personal o que no corresponda a la legalmente autorizada, cumpliendo con la normatividad relacionada con derechos de autor.

- Los funcionarios involucrados en este procedimiento de la Dirección de TIC y sus proveedores deberán garantizar que se lleve a cabo el respaldo de las bases de datos de los sistemas de información de la entidad, información usuarios, configuración dispositivos de comunicación y redes, servicios office365 y solución de hiperconvergencia.

- Las cintas de respaldo serán identificadas conforme lo permite la librería de backup y en otros mecanismos de respaldo se deberán identificar con el contenido y fecha de realización, al igual con el número de veces que ha sido usado el mecanismo.

- Los funcionarios involucrados en este procedimiento de la Dirección de TIC y sus proveedores deberán realizar pruebas de restauración de los archivos de respaldo de forma periódica o por demanda, realizando un muestreo de la misma debido a la capacidad de la infraestructura requerida para el mismo.

- La información y los tipos de respaldo que se deben aplicar para la información de la entidad son:

ID	Tipo de información	Información a respaldar	Tipo de respaldo	Periodicidad	Responsable
1	Información de usuarios	Información de usuarios que se encuentra almacenada en la unidad (P).	Incremental	Diario	Profesional Especializado Grado 06 – Coordinador de Procesos Corporativos de TI y Mesa de Ayuda
2	Bases de datos de los sistemas de información	Instancias de base de datos. Archivos de Base de datos.	Full	Diario	Profesional Universitario Grado 3 de Bases de Datos y Aplicaciones Corporativas y el Proveedor
3	Solución de Hiperconvergencia	Máquinas virtuales que se encuentran en la solución.	Full	Diario, Semanal, Mensual	Profesional Especializado Grado 06 - Coordinador de Procesos Corporativos de TI y el Proveedor
4	Equipos de comunicaciones, seguridad y red.	Archivos de configuración de los equipos de red.	Full	Mensual	Profesional Especializado Grado 06 - Seguridad informática y el Proveedor
5	Office365	Correos electrónicos que se encuentran en el buzón a la fecha y archivos que se encuentren en OneDrive y Sharepoint.	Full	Diaria	Profesional Especializado Grado 06 - Coordinador de Procesos Corporativos de TI

Nota: No se incluye en el respaldo de información en lo relacionado con sistema operativo para equipos diferentes a los de la solución de Hiperconvergencia.

- Los requisitos a tener en cuenta para la toma del respaldo de información son:
    - Disponer de un espacio de almacenamiento de los archivos de respaldo en TRANSMILENIO S.A.
    - Disponer de un entorno de pruebas de restauración de los archivos de respaldo.
- La retención de las copias de respaldo se realiza de acuerdo con la periodicidad de su ejecución. Para el caso de office 365 (correo electrónico), se tiene 1 año de retención de información de respaldo.

7. DESCRIPCIÓN DE ACTIVIDADES

7.1 Copias de respaldo

7.1.1 Respaldo de la información de Usuarios

A continuación, se describen los pasos que se deben seguir para realizar el respaldo de la información de los usuarios, almacenada en la unidad (P:).

ETAPA	ACTIVIDAD	RESPONSABLE
10	**Inicio**	
20	Almacenar los archivos en la unidad P:\	Usuarios de TMSA
30	Configurar la(s) herramienta(s) de respaldo para que realice la copia de la Unidad P: en cinta. Esta configuración se realiza de tal forma que la copia de respaldo se inicie automáticamente.	Técnico Administrativo Grado 02 - Soporte a Infraestructura de TIC´s y Mesa de Ayuda
40	Insertar en el equipo de respaldo las cintas etiquetadas con su respectivo código de barras y previamente configuradas, esto se realiza antes de que inicie la copia de respaldo. En estas cintas se almacenarán los datos respaldados de cada uno de los usuarios.	Técnico Administrativo Grado 02 - Soporte a Infraestructura de TIC´s y Mesa de Ayuda
50	Monitorear la herramienta de respaldo con el fin de identificar si la capacidad de las cintas se completó	Técnico Administrativo Grado 02 - Soporte a Infraestrutura de TIC´s y Mesa de Ayuda
¿15? 	¿La capacidad de la cinta se completó? **No: se continua en esta actividad hasta detectar una cinta completa.** **Si: se realiza el reemplazo de esta cinta por una vacía, siguiendo las instrucciones del Software de respaldo y se continua con la actividad 60**	Técnico Administrativo Grado 02 - Soporte a Infraestructura de TIC´s y Mesa de Ayuda

ETAPA	ACTIVIDAD	RESPONSABLE
60	Archivar en gabinete Cada vez que se retira una cinta completa, esta se archiva en el gabinete de la Entidad ubicado en el centro de cómputo.	Técnico Administrativo Grado 02 - Soporte a Infraestructura de TIC´s y Mesa de Ayuda
¿25? 	¿La cinta esta etiquetada como almacenamiento externo? **No: ir a etapa 70** **Si: mantener en el gabinete de cintas dentro del centro de cómputo e ir a etapa 80**	Técnico Administrativo Grado 02 - Soporte a Infraestructura de TIC´s y Mesa de Ayuda
70	Remitir al proveedor las cintas etiquetadas como externas para su custodia e ir a etapa 100	Profesional Especializado Grado 06 – Coordinador de Procesos Corporativos de TI
80	Verificar diariamente la correcta toma de las copias, si se presenta algún problema, analizarlo y solucionarlo.	Técnico Administrativo Grado 02 - Soporte a Infraestructura de TIC´s y Mesa de Ayuda
¿35? 	¿Las copias de seguridad están completas y correctas? **No: informar al Profesional Especializado Grado 06 – Coordinador de Procesos Corporativos de TI e ir a etapa 90** **Si: ir a etapa 100**	Técnico Administrativo 02 - Soporte a Infraestructura de TIC´s y Mesa de Ayuda
90	**Analizar y tomar decisiones**	Profesional Especializado Grado 06 – Coordinador de Procesos Corporativos de TI
100	**Fin**	

7.1.2 <u>Respaldo de bases de datos, solución de hiperconvergencia y equipos de comunicaciones y de red</u>

Para el respaldo de la información de las bases de datos de los sistemas de información, la solución de hiperconvergencia, equipos de red y comunicaciones que son administrados por proveedores de servicio a través de contratos de soporte y mantenimiento se aplicarán las siguientes acciones.

- El Profesional Especializado Grado 06 – Coordinador de Procesos Corporativos de TI debe especificar en los contratos las condiciones de respaldo de información acorde con el servicio prestado por cada proveedor.

- **BASES DE DATOS**. El Profesional Universitario Grado 03 - Gestor de Base de Datos y Aplicaciones debe:
  - Validar con el proveedor que se cuente con la configuración para la ejecución del respaldo de la información. Respaldo de las instancias de bases de datos de los sistemas de información.
  - Validar con el proveedor que se realicen las copias de respaldo acorde con lo requerido dentro del contrato
  - Solicitar al proveedor las copias de respaldo por demanda en caso de que de que se requiera.
  - Restaurar los archivos de respaldo en caso de que sea requerido por la entidad.

- **HIPERCONVERGENCIA**. El Profesional Especializado Grado 06 – Coordinador de Procesos Corporativos de TI debe:
  - Validar con el proveedor que se cuente con la configuración para la ejecución del respaldo de la información. Configuraciones de los equipos.
  - Validar con el proveedor que se realicen las copias de respaldo acorde con lo requerido dentro del contrato.
  - Solicitar al proveedor las copias de respaldo por demanda en caso de que de que se requiera.
  - Restaurar los archivos de respaldo en caso de que sea requerido por la entidad.

- **EQUIPOS DE COMUNICACIONES Y REDES**. El Profesional Especializado Grado 06 – Seguridad Informática debe
  - Validar con el proveedor que se cuente con la configuración para la ejecución del respaldo de la información. Respaldo de máquinas virtuales que se encuentran en la solución.
  - Validar con el proveedor que se realicen las copias de respaldo acorde con lo requerido dentro del contrato
  - Solicitar al proveedor las copias de respaldo por demanda en caso de que de que se requiera.

7.2 Copias de restauración

A continuación, se describe la forma en que se realiza la restauración de información que demandan los usuarios, así como las pruebas de restauración de información para comprobar la calidad del respaldo.

7.2.1 Restauración de la información de Usuarios

ETAPA	ACTIVIDAD	RESPONSABLE
10	**Inicio**	
20	Revisar el tipo de restauración: 1. Si es una actividad de restauración solicitada por un usuario, entonces se inicia con la actividad 30. 2. Si es una prueba de restauración se inicia con la actividad 40.	Mesa de Ayuda
30	Solicitar restauración de información. El usuario solicita la restauración de un archivo/carpeta/unidad de la copia de respaldo. Esta solicitud se realiza a través de correo electrónico a la mesa de ayuda, al correo soportetecnico@transmilenio.gov.co. Continua en actividad 50.	Usuarios de TMSA
40	Solicitar prueba de restauración. El Técnico Administrativo 02 de TIC, realiza solicitud a la mesa de ayuda al correo soportetecnico@transmilenio.gov.co con definición de la prueba de restauración. Donde se indica: • Archivo que será restaurado • Fecha de la prueba • Resultado esperado.	Técnico Administrativo 02 - Soporte a Infraestructura de TIC´s
50	Verificar que la información a restaurar en la herramienta de respaldo esté disponible. (*)	Técnico Administrativo 02 - Soporte a Infraestructura de TIC´s y/o Mesa de Ayuda o Proveedor

ETAPA	ACTIVIDAD	RESPONSABLE
¿15? 	¿Se encontró la información a restaurar? **Si: ir a etapa 60** **No: ir a etapa 80**	Mesa de Ayuda o Proveedor
60	Restaurar la información (*) Se restaura el archivo usando la herramienta de respaldo bajo las siguientes condiciones: 1. Si el archivo es reciente, se restaura sobre la ubicación original. 2. Si el archivo supera los 5 años de antigüedad o es un archivo de prueba de restauración, entonces se restaura en una unidad específica dentro del servidor de archivos.	Técnico Administrativo 02 - Soporte a Infraestructura de TIC´s y/o Mesa de Ayuda o Proveedor
¿25? 	¿La restauración presentó alguna falla? **Si: ir a etapa 70** **No ir a etapa 90**	Mesa de ayuda o Proveedor
70	Informar al Profesional Especializado Grado 06 – Coordinador de Procesos Corporativos de TI	Mesa de ayuda o Proveedor
80	Analizar el caso, buscar soluciones alternativas para la restauración de la información e ir a etapa 90	Profesional Especializado Grado 06 – Coordinador de Procesos Corporativos de TI
90	Notificar al usuario Se notifica al usuario la restauración del archivo y su ubicación. De lo contrario se notifica las posibles alternativas de solución.	Técnico Administrativo 02 - Soporte a Infraestructura de TIC´s y Mesa de Ayuda –
100	Realizar registro de la restauración La documentación de cualquier tipo de restauración sea por demanda o por prueba, debe registrarse en la herramienta de soporte técnico/mesa de ayuda o la que haga sus veces, con el fin de que se pueda identificar y consultar posteriormente.	Técnico Administrativo 02 - Soporte a Infraestructura de TIC´s y Mesa de Ayuda

ETAPA	ACTIVIDAD	RESPONSABLE
110	Fin	

(*) Nota: si es información administrada directamente por la Dirección de TIC la realiza Técnico Administrativo 02 - Soporte a Infraestructura de TIC´s , en caso contrario el proveedor externo.

7.2.2 Procedimiento de restauración de copias de respaldo de proveedores

Para el caso de restauración de la información que gestionan los proveedores de equipos de comunicaciones o redes de datos, bases de datos y sistema de hiperconvergencia se deben seguir las siguientes actividades:

- Solicitar al proveedor a través de correo electrónico la entrega del archivo de respaldo, incluyendo el sistema, periodo y demás información relevante que permita identificar el archivo a restaurar.

- Proveer al proveedor el espacio de almacenamiento respectivo con el fin de que se pueda restaurar el archivo de respaldo de datos o información.

- Solicitar al proveedor la restauración del archivo de respaldo de datos o información para que se realicen las pruebas respectivas.

Para el caso de las copias de respaldo de Office 365, estas se deben solicitar a la Dirección de TIC a través de la mesa de ayuda y se restaurarán desde la plataforma de office 365, la cual almacena la información en la nube.

7.2.2.1 Pruebas de restauración de copias de respaldo

Con el fin de verificar que las copias de respaldo funcionan adecuadamente y que la información esté completa cuando se requiera una restauración de emergencia, se realizarán pruebas de restauración de forma periódica basado en las siguientes premisas:

- Las pruebas de restauración se realizarán por lo menos 2 veces al año.

- Las pruebas de restauración se realizarán por lo menos de la información de los usuarios que respalda TRANSMILENIO S.A. Sin embargo, también se podrá solicitar por demanda a los proveedores de servicio o terceros que realicen la prueba de restauración de otro tipo de plataformas. Lo anterior dado que el respaldo de dicha información está contractualmente a cargo del proveedor.

- Las pruebas de restauración serán realizadas por la Dirección de TIC y deberán quedar registradas en un documento de acta, la cual deberá contener la información de la información donde se probó la restauración, así como las evidencias.