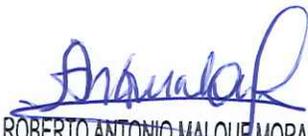


<b>Manual de Normas y Procedimientos</b>  <b>POLÍTICA DE MANEJO DE RESPALDOS Y RESTAURACIÓN</b>  <b>ME-DS-TI-MNP-PMRR-09</b>  <b>Versión 02</b>
---

Aprobado por	Cargo	Fecha	Firma y sello
Ing. Roberto Antonio Malouf Morales	Ministro de Economía	25/05/2021	 <b>ROBERTO ANTONIO MALOUF MORALES</b> MINISTRO DE ECONOMÍA 

Revisado por	Cargo	Fecha	Firma y sello
Marco Antonio Hernandez	Director de Tecnologías de la Información	16/02/2021	 <b>Marco Antonio Hernandez</b> Director Dirección de Tecnologías de la Información Ministerio de Economía

Actualizado por	Cargo	Fecha	Firma y sello
Gladis Corina Lorenzana	Técnico de Tecnologías de la Información	18/02/2021	 <b>Gladis C. Lorenzana</b> Dirección de Tecnologías de la Información Ministerio de Economía

Documentado por	Cargo	Fecha	Firma y sello
Lic. Mynor Zúñiga	Director de Desarrollo Institucional	24/03/2021	 <b>Lic. Mynor Zúñiga</b> Director de Desarrollo Institucional Ministerio de Economía

<b>Vigente a partir de:</b> <b>26/05/2021</b>
---

### ÍNDICE

<b>1.</b>	<b>OBJETIVO:</b> .....	<b>3</b>
<b>2.</b>	<b>ALCANCE:</b> .....	<b>3</b>
<b>3.</b>	<b>DEFINICIONES:</b> .....	<b>3</b>
<b>4.</b>	<b>BASE LEGAL, DOCUMENTOS O DATOS RELACIONADOS:</b> .....	<b>4</b>
<b>5.</b>	<b>NORMAS:</b> .....	<b>4</b>
<b>6.</b>	<b>RESPONSABILIDADES:</b> .....	<b>6</b>
<b>7.</b>	<b>PROCEDIMIENTO:</b> .....	<b>7</b>
<b>8.</b>	<b>FLUJOGRAMA:</b> .....	<b>9</b>
<b>9.</b>	<b>ANEXOS:</b> .....	<b>11</b>





	Manual de Normas y Procedimientos	ME-DS-TI-MNP-PMRR-09 Versión 02
	POLÍTICA DE MANEJO DE RESPALDOS Y RESTAURACIÓN	Página 3 de 13

### 1. OBJETIVO:

El presente manual de normas y procedimientos define las directrices para la realización de copias de seguridad o respaldos de los datos almacenados en los servidores del Ministerio de Economía identificados como críticos, con la finalidad de prevenir la pérdida total o parcial de la información contenida en los mismos y poder llevar la restauración de dicha información en el caso de presentarse cualquier contingencia.

### 2. ALCANCE:

El presente manual de normas y procedimientos debe ser cumplido para llevar a cabo exclusivamente los respaldos de los datos almacenados en los servidores críticos del Ministerio de Economía (servidores de base de datos, servidores de archivos y servidores de aplicación) ubicados en centros de datos principales y centros de datos distribuidos (Registros y/o Unidades Ejecutoras). Esta política no aplica para los archivos guardados en estaciones de trabajo de uso diario de los usuarios de la institución.

### 3. DEFINICIONES:

#### 3.1. Encargado de la administración de plataforma informática:

Persona conocedora del funcionamiento y el contenido de los servidores a los que se les realizará el respaldo.

#### 3.2. Encargado de la administración de respaldos:

Persona designada para ejecutar las funciones requeridas y llevar a cabo los procesos de respaldo en términos de configuración del software, monitoreo y actividades operativas relacionadas.

#### 3.3. Copias de seguridad o respaldo:

Copia de la información almacenada en los servidores críticos y no críticos del Ministerio de Economía, los cuales son grabados en medios de almacenamiento.

#### 3.4. Respaldo Completo:

Es una copia de seguridad de toda la información contenida en un servidor, directorio, carpeta o base de datos, que permite recuperar en su totalidad la información necesaria para continuar operando.

#### 3.5. Respaldo Diferencial:

Es una copia de seguridad que contiene los datos que cambiaron desde que se realizó la última copia o respaldo completo.

#### 3.6. Respaldo Incremental:

(o Diferencial Incremental) es la copia más avanzada al respecto, ya que copia los archivos creados o modificados desde el último respaldo realizado, ya sea de una copia completa o incremental, reduciendo de este modo los archivos a copiar y el tiempo empleado en el proceso de respaldo.

#### 3.7. Prueba de restauración:

Actividad que se realiza para comprobar la correcta ejecución del respaldo.

#### 3.8. Restauración de la información:

Actividad que permite restablecer la información hasta el último respaldo realizado.





**3.9. Información crítica:**

Información que es indispensable para la continuidad de la operación.

**3.10. Sitio alternativo:**

Ubicación física que contiene la infraestructura necesaria para ser utilizada en los casos de emergencia.

**3.11. Hipervisor:**

Software de administración de equipos virtuales, actualmente en producción vmWare 6.5.

**4. BASE LEGAL, DOCUMENTOS O DATOS RELACIONADOS:**

Base legal, documentos o datos relacionados	
Número o código del documento o dato	Descripción del documento o dato
Acuerdo Gubernativo No. 211-2019	Reglamento Orgánico Interno del Ministerio de Economía
Acuerdo Ministerial 762-2019	Estructura Orgánica Interna Complementaria a la estructura establecida en el Reglamento Orgánico Interno del Ministerio de Economía

**5. NORMAS:**

**5.1.** Las personas designadas para la administración de la plataforma informática o para la administración de los respaldos, son las responsables de realizar las configuraciones necesarias para la ejecución de los respaldos.

**5.2.** La persona encargada para la administración de respaldos es designada por el Jefe de Departamento de Operaciones.

**5.3.** Los respaldos serán ejecutados con frecuencia mensual, semanal o diaria, según la categoría del servidor (crítico o no crítico) y que la pérdida de la información sea perjudicial para la institución.

**5.4.** La frecuencia de los respaldos está sujeta a la disponibilidad de la solución de respaldos, horario con menos demanda en servidores y sistemas en producción. Esta será definida en conjunto con las personas encargadas de administrar la plataforma informática y de la administración de respaldos.

**5.4.1. Respaldos en servidores críticos:**

**5.4.1.1.** Respaldos en base de datos central: Los respaldos de la base de datos central, se realizarán aplicando el tipo diferencial incremental, el tipo de respaldo dependerá del tamaño de la información a respaldar y de los recursos disponibles en la solución de respaldos.

**5.4.1.2.** Estos respaldos se realizan a información crítica para la continuidad de la operación en el Ministerio de Economía, dichos respaldos son solicitados por las personas encargadas de la administración de la plataforma informática correspondiente.



 <b>GOBIERNO de GUATEMALA</b> <small>DR. ALEJANDRO GUZMÁN</small>	 <b>MINISTERIO DE ECONOMÍA</b> <b>GUATEMALA</b> <small>1985-2023</small>	<b>Manual de Normas y Procedimientos</b>	<b>ME-DS-TI-MNP-PMRR-09</b> <b>Versión 02</b>
		<b>POLÍTICA DE MANEJO DE RESPALDOS Y RESTAURACIÓN</b>	<b>Página 5 de 13</b>

**5.4.2. Respaldos en servidores no críticos:**

**5.4.2.1.** Los respaldos de la información en los ambientes de desarrollo y preproducción deberán ser solicitados al Encargado de la Administración de Respaldos por las personas encargadas de la administración de cada plataforma y se tomará en cuenta toda la información cuya pérdida pueda perjudicar a los sistemas que la Dirección de Tecnologías de la Información esté desarrollando y que son parte de futuras entregas de sistemas.

**5.4.3. Respaldos en Registros y/o Unidades Ejecutoras:**

**5.4.3.1.** La unidad de Informática de cada Registro y/o Unidad Ejecutora deberá velar por la realización de copias de seguridad de los servidores que cuenten con información crítica, tales como bases de datos y servidores de archivos, con el fin de prevenir la pérdida parcial o total de la información. Así, como también, deberán contar con un plan de restauración de la información en el caso que sea necesario.

**5.4.3.2.** Para la restauración de la información se utilizará en primera instancia el respaldo obtenido de las unidades de Informática de cada Registro y/o Unidad Ejecutora. Como último recurso se tomará el respaldo generado en la Dirección de Tecnologías de la Información.

**5.4.4. Respaldo a servidores de archivos:**

**5.4.4.1.** Los respaldos de los servidores de archivos se realizarán específicamente a los recursos compartido, de igual forma a los servidores de aplicaciones o bases de datos que así se defina, una vez se defina el requerimiento por el Director(a) de la Unidad, Dirección o Registro.

**5.4.4.2.** Con base a la política de seguridad informática para usuarios vigente, los respaldos de información de los servidores de archivos, así como los servidores de aplicaciones o bases de datos, no deberán contener juegos, video, fotos, archivos, presentaciones y música que no estén relacionados con sus actividades laborales.

**5.4.5. Período de retención de respaldos:**

**5.4.5.1.** El período de retención puede ser de un año, treinta días o quince días y aplicará para: servidores de base de datos central, servidores críticos y servidores de base de datos de registros; de acuerdo con lo que el/la Director(a) de la Dirección de Tecnologías de la Información defina con las Autoridades responsables de la información.

**5.4.6. Restauración de información:**

**5.4.6.1.** Se realizará por lo menos una prueba de restauración de información al año, a uno de los servidores respaldados, la selección se hará dependiendo de los recursos disponibles para llevar a cabo este proceso.

**5.4.6.2.** El encargado de la administración de respaldos diseñará un plan de restauración, programando la ejecución de las pruebas de restauración de los respaldos seleccionados con el apoyo del encargado de la administración de plataforma informática correspondiente.



	<b>Manual de Normas y Procedimientos</b>	<b>ME-DS-TI-MNP-PMRR-09</b> <b>Versión 02</b>
	<b>POLÍTICA DE MANEJO DE RESPALDOS Y RESTAURACIÓN</b>	<b>Página 6 de 13</b>

**5.4.7. Continuidad de la operación:**

**5.4.7.1.** Para responder ante una emergencia de manera adecuada y lograr un mínimo impacto en los servicios que presta la institución, se debe contar con una solución adicional de respaldos para la información clasificada como crítica en diferente ubicación, con el fin de mantener una alta disponibilidad y protección ante desastres en caso de cortes de servicios planificados o no planificados en el sitio de producción.

**5.4.8. Medios de almacenamiento:**

**5.4.8.1.** Se deberá contar con dispositivos de almacenamiento para almacenar las copias de seguridad que podrán ser utilizadas para restaurar la información en caso de desastre. Dichos dispositivos deben estar almacenados en un sitio alternativo.

**5.4.8.2.** Todo dispositivo de almacenamiento que sea desechado por encontrarse en mal estado no deberá contener información.

**5.5.** Los Funcionarios y empleados que intervienen en el numeral “7. PROCEDIMIENTO” del presente Manual de normas y procedimientos, son corresponsables del contenido y cumplimiento del mismo, según corresponda;

**5.6.** Situaciones no previstas en el presente manual de normas y procedimientos, serán resueltas por el Director de Tecnologías de la Información;

**5.7.** El presente manual deja sin efecto el manual de procedimientos “BACKUP DE INFORMACIÓN ALMACENADA EN SERVIDORES DE LA DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN”, ME-VIAFI-DTI-MP-BA-10, versión 01.

**6. RESPONSABILIDADES:**

**6.1. Despacho Superior es responsable de:**

**6.1.1.** Aprobar, firmar y sellar el presente manual de normas y procedimientos.

**6.2. Director de Tecnologías de la Información es responsable de:**

**6.2.1.** Revisar, firmar y sellar el presente manual de normas y procedimientos, garantizando que su contenido responde al proceso que norma y documenta el mismo;

**6.2.2.** Actualizar o delegar y supervisar la actualización oportuna del presente manual de normas y procedimientos, en coordinación con la Dirección de Desarrollo Institucional;

**6.2.3.** Cumplir y supervisar en lo que corresponde, el cumplimiento del presente manual de normas y procedimientos;

**6.2.4.** Otras responsabilidades que correspondan, establecidas en el numeral 7. “PROCEDIMIENTO” del presente manual.

**6.3. Técnico encargado de la Dirección de Tecnologías es responsable de:**

**6.3.1.** Actualizar oportunamente el presente manual de normas y procedimientos por instrucciones del Director de Tecnologías de la Información y en coordinación con la Dirección de Desarrollo Institucional;





- 6.3.2. Firmar y sellar el presente manual de normas y procedimientos, garantizando que su contenido responde al proceso que norma y documente el mismo;
- 6.3.3. Cumplir en lo que corresponda con el presente manual de normas y procedimientos;
- 6.3.4. Otras responsabilidades que correspondan, establecidas en el numeral 7: "PROCEDIMIENTO" del presente manual.

**7. PROCEDIMIENTO:**

**7.1. Gestión de los Respaldos**

Responsable	Actividades	Tiempo
Usuario	<ul style="list-style-type: none"> <li>• Define la información que será resguardada, esta información deberá tratarse como confidencial;</li> <li>• Llena formulario de requerimiento de respaldo, indicando el detalle de carpetas a resguardar;</li> <li>• Gestiona firma de aprobación de la Autoridad Superior del formulario;</li> <li>• Una vez firmado, genera el ticket con el formulario adjunto en el sistema de gestión de Tickets -OTRS-</li> </ul>	20 minutos
Service desk Tecnologías de la Información	<ul style="list-style-type: none"> <li>• Recibe el ticket generado por el usuario;</li> <li>• Verifica que el ticket lleve adjunto el formulario de solicitud debidamente firmado;</li> <li>• Traslada el ticket a encargado de Operaciones</li> </ul>	15 minutos
Encarado de Operaciones Tecnologías de la Información	<ul style="list-style-type: none"> <li>• Recibe el ticket trasladado por Service Desk;</li> <li>• Procede a evaluar los recursos disponibles en el hardware designado;</li> <li>• Si no existen recursos, regresar el ticket para que se notifique al usuario.</li> <li>• Si existen recursos, se procede a crear la tarea automatizada de respaldo y asignar el dispositivo destino, utilizando el software Veeam;</li> <li>• Una vez creada la tarea automatizada, en Veeam, evalúa la funcionalidad de ésta, posteriormente se notifica al Director (a) de la Dirección de Tecnologías de la Información sobre el proceso implementado y los recursos a consumir;</li> <li>• Traslada el ticket de vuelta a Service Desk.</li> </ul>	1 hora
Service desk Tecnologías de la Información	<ul style="list-style-type: none"> <li>• Recibe el ticket trasladado por Operaciones;</li> <li>• Informa al usuario solicitante respecto a la implementación del respaldo;</li> </ul>	15 minutos



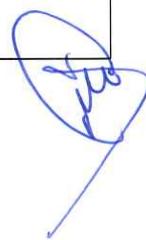
*[Handwritten signature]*

*[Handwritten mark]*

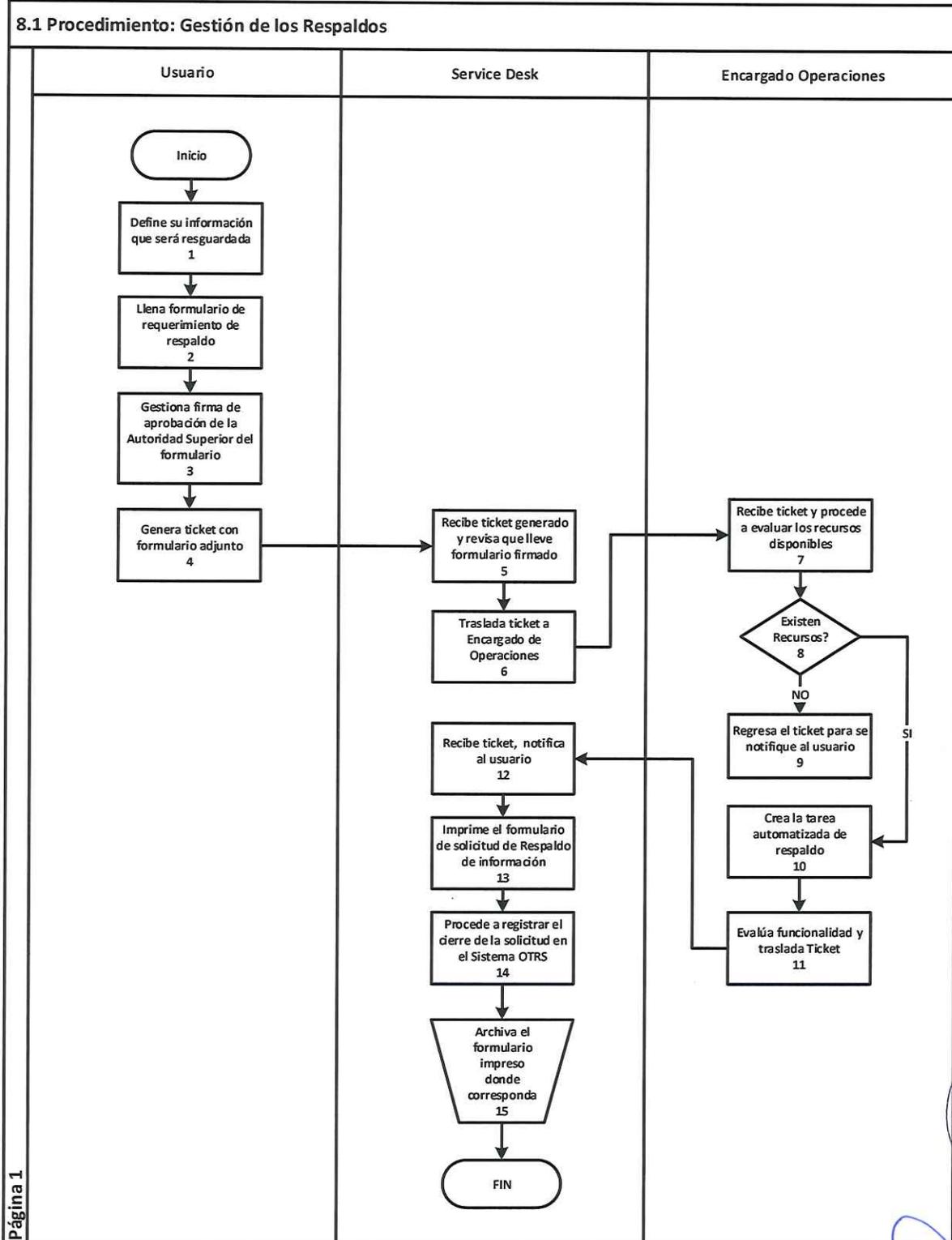
Responsable	Actividades	Tiempo
	<ul style="list-style-type: none"> <li>• Imprime el formulario de solicitud de Respaldo de información;</li> <li>• Procede a documenta el cierre de la solicitud en el Sistema OTRS.</li> <li>• Archiva el formulario impreso donde corresponda;</li> </ul> <p>En el caso que se hayan realizado modificaciones durante el proceso, éstas deberán ser registradas como un anexo al formulario original, también deberán ser impresas y archivadas como parte del expediente.</p>	

### 7.2. Gestión de la Restauración

Responsable	Actividades	Tiempo
Encargado de Operaciones Tecnologías de la Información	<ul style="list-style-type: none"> <li>• Ingres a la plataforma de administración Veeam;</li> <li>• Selecciona el servidor a restaurar;</li> <li>• Selecciona los recursos a utilizar en el hipervisor vmWare 6.5;</li> <li>• Ejecuta el proceso de restauración.</li> <li>• El software Veeam Backup &amp; Replication software ejecuta el proceso, el tiempo puede ser corto como treinta (30) minutos o extenso como tres (3) horas;</li> <li>• Limpia meta data en el recurso restaurado, en caso sea necesario;</li> <li>• Notifica de la finalización del proceso a Dirección.</li> </ul>	2 horas




8. FLUJOGRAMA:

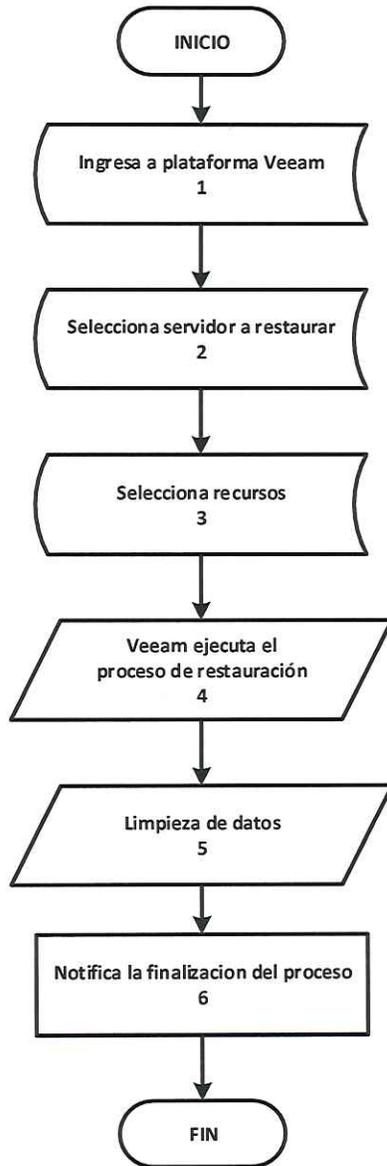


*[Handwritten signature]*

*[Handwritten mark]*

8.2 Procedimiento: Gestión de la Restauración

Encargado Operaciones



Handwritten signature and initials in blue ink.

9. ANEXOS:



Fig. 01 – Ingreso de credenciales en la consola de administración de Veeam.

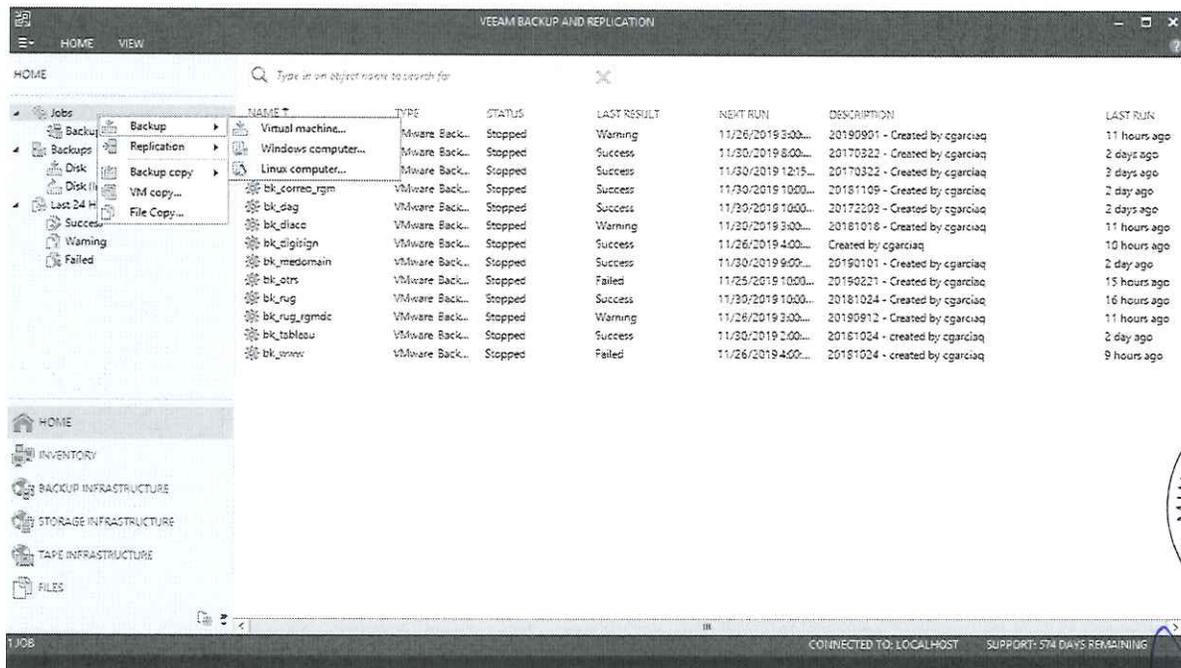


Fig. 02 – Definición de la tarea automatizada.



*Handwritten signature*

*Handwritten checkmark*

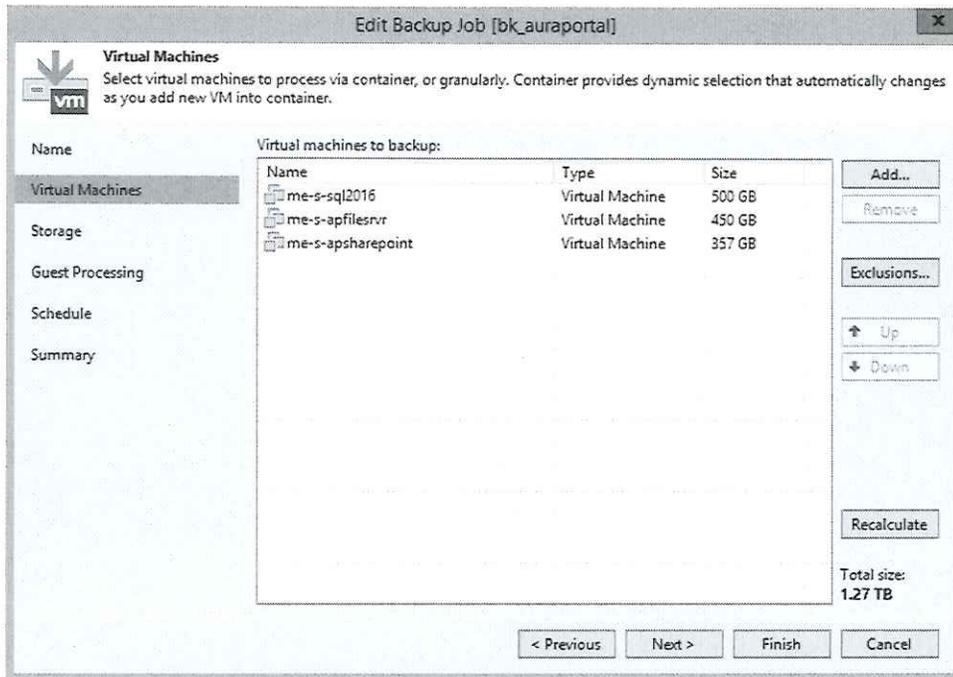


Fig. 03 – Definición de Servidores o carpetas de archivos.

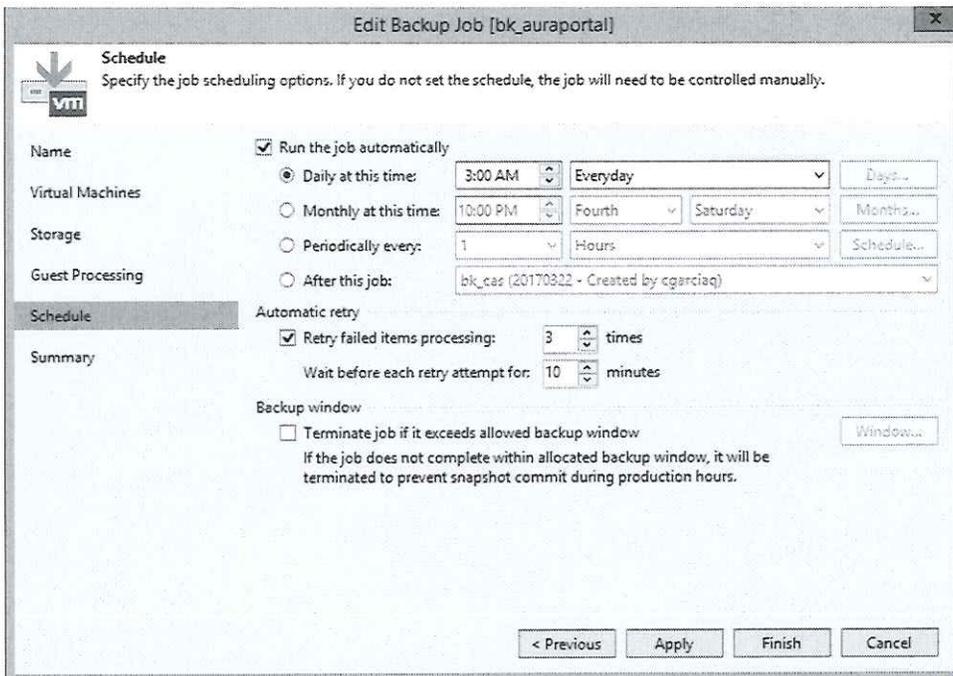


Fig. 04 – Definición de la frecuencia para la tarea automatizada.



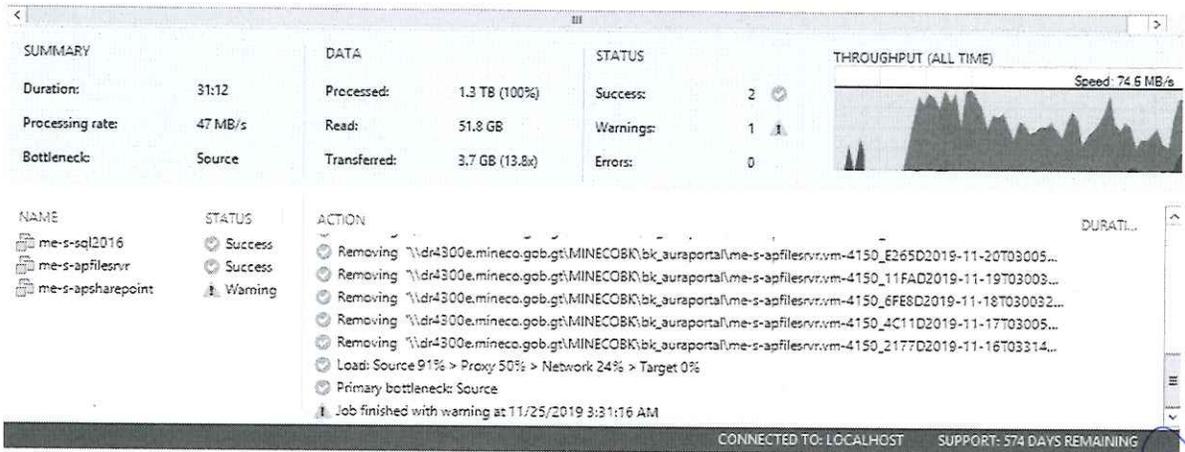


Fig. 05 – Validación de la funcionalidad de la tarea automatizada.

