LEY N°21.796

PARTIDA 32

GLOSA 04

PLANES, POLÍTICAS Y ACCIONES DESTINADAS A FORTALECER LA CIBERSEGURIDAD
Y
PROCEDIMIENTOS DE RESPALDO

Descripción de la Glosa
El Ministerio de Seguridad Pública informará, a más tardar el 31 de enero de 2026, a la Comisión Especial Mixta de Presupuestos y a las Comisiones de Desafíos del Futuro, Ciencia, Tecnología e Innovación, de Seguridad Pública y de Defensa Nacional del Senado y a las Comisiones de Futuro, Ciencias, Tecnología, Conocimiento e Innovación, de Seguridad Ciudadana y de Defensa Nacional de la Cámara de Diputados, acerca de todos los planes, políticas y acciones destinados a fortalecer la ciberseguridad. Asimismo, se deberá informar el o los protocolos internos de respaldo de información de los computadores. Trimestralmente, se deberá informar la ocurrencia de incidentes y ataques informáticos registrados, así como el cumplimiento del o los protocolos de respaldo. Semestralmente, 30 días después de terminado el semestre respectivo, deberá remitir informe que dé cuenta de las vulneraciones registradas durante el periodo y la manera en que se enfrentaron dichas contingencias.

Planes, Políticas y acciones destinadas a fortalecer la ciberseguridad

En relación a los planes, políticas y acciones destinados a fortalecer la ciberseguridad en la Subsecretaría de Prevención del Delito, como institución tenemos los siguientes objetivos para el 2026:

1) Publicar mediante Resolución Exenta la actualización de la política de seguridad de la información, alineada con lo exigido para los operadores de importancia vital según la Ley Marco de Ciberseguridad. Esta medida permite establecer un marco formal de control y gobierno, reduciendo riesgos de incumplimiento normativo que pueden derivar en sanciones, observaciones de entes fiscalizadores y costos asociados a la gestión de incidentes.
2) Desarrollar una norma general de protección de datos personales, en consideración a la próxima entrada en vigencia de la Ley de Protección de Datos Personales. Su implementación permitirá prevenir brechas de datos y eventuales responsabilidades legales, evitando costos económicos, reputacionales y operativos asociados a la exposición de información sensible.
3) Implementar un Centro de Operaciones de Seguridad de la Información y Ciberseguridad (SOC), con el objetivo de monitorear continuamente las redes y activos tecnológicos de la institución. Esto permitirá reducir significativamente los tiempos de detección y respuesta ante incidentes, disminuyendo el impacto operativo y los costos asociados a interrupciones de servicio o recuperación ante incidentes de seguridad.
4) Fortalecer el sistema de gestión de seguridad de la información, con el fin de mejorar la identificación, evaluación y tratamiento de riesgos. Esto permitirá una asignación más eficiente de los recursos institucionales, priorizando inversiones en función del nivel de exposición y criticidad de los activos.
5) Actualizar las normas y procedimientos asociados a la Política de Seguridad de la Información, asegurando su coherencia y aplicabilidad. Esto contribuye a estandarizar procesos, reducir errores operativos y evitar reprocesos, generando eficiencias en la gestión institucional.
6) Incorporar dos funcionarios adicionales a la sección de seguridad de la información y ciberseguridad, considerando que actualmente toda la función de la sección recae en el encargado. Esto permitirá distribuir adecuadamente las funciones y mejorar los tiempos de respuesta, evitando costos asociados a la falta de capacidad de respuesta ante incidentes o requerimientos normativos.

7) Realizar capacitaciones periódicas a los funcionarios en materias de protección de datos personales y ciberseguridad, buscando reducir la probabilidad de incidentes asociados a errores humanos, los cuales representan una de las principales causas de brechas de seguridad. Esto permite disminuir incidentes evitables, tales como phishing, pérdida de información o uso indebido de sistemas, contribuyendo además al cumplimiento normativo y a la reducción de riesgos operacionales.

En relación al **procedimiento de respaldo de equipos**, tanto los correos como los elementos de onedrive se respaldan automáticamente en nuestra plataforma de Microsoft y están disponibles por un periodo de 5 años desde la fecha de desactivación de la cuenta.

Finalmente, respecto **al plan de respaldo de los servidores**, este se encuentra adjunto a continuación.

Ministerio del Interior y Seguridad Pública

Subsecretaría de Prevención del Delito

Procedimiento de configuración de copias de respaldo de servidores

1. Objetivo

Establecer el conjunto de actividades a desarrollar para llevar a cabo la configuración de respaldo de los servidores de la Institución en el sistema centralizado Symantec Backup Exec y que soportan los sistemas de información de la Subsecretaría de Prevención del Delito.

2. Alcance

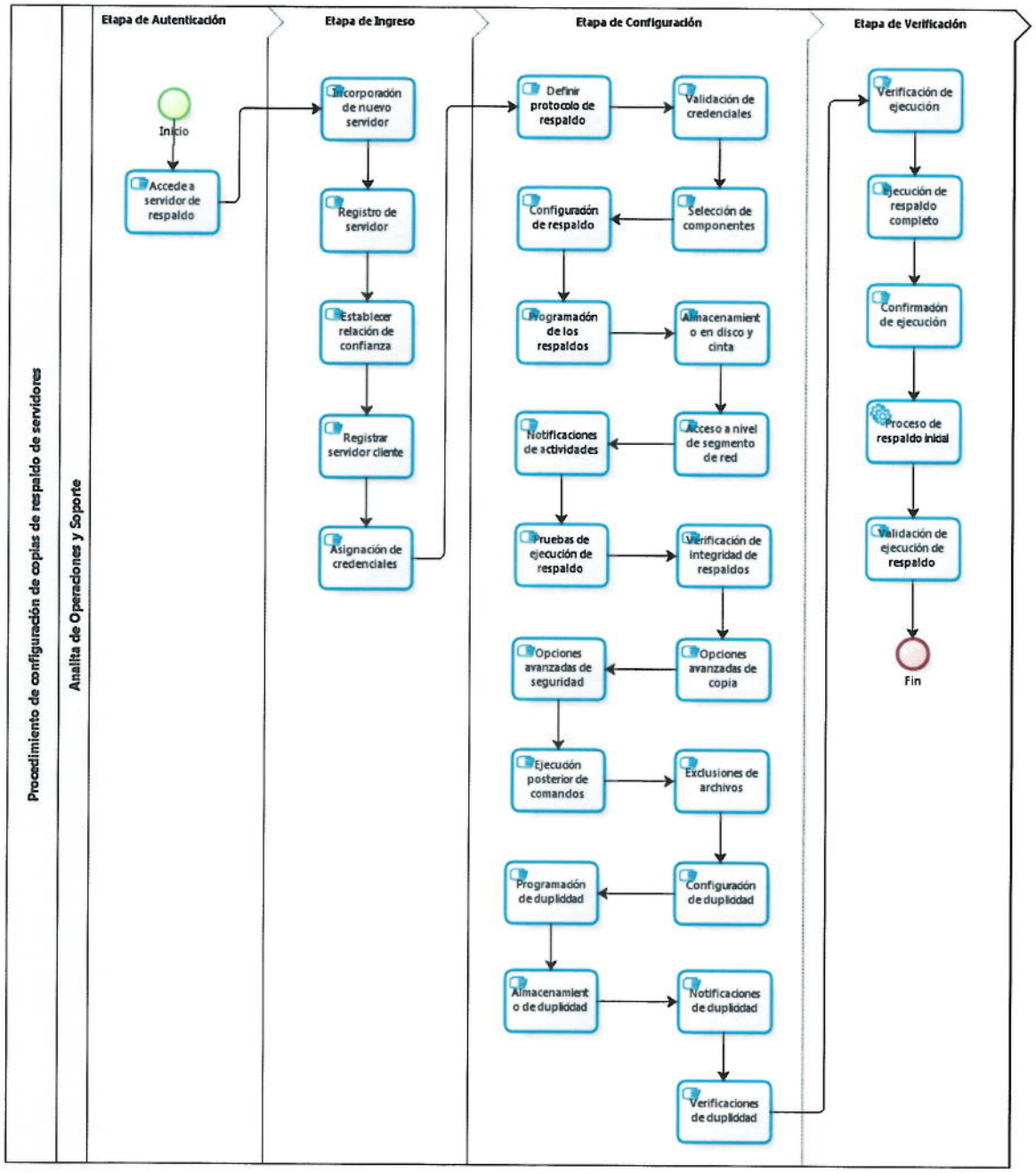
Este procedimiento aplica a los sistemas de información que mantengan sistema operativo Red Hat Linux en versiones 6.0 o superiores, Microsoft Windows 2008 Server o superiores, Microsoft Sharepoint 2010, Servidores de base de datos MSSQL Server y Oracle, como también servidores de archivos, cualquiera de estos que se encuentre en el ambiente de desarrollo, prueba o producción y que restrictivamente se encuentren en los segmentos de red 10.13.70.0/24, 10.13.71.0/24 y 10.13.72.0/24 del Data Center de la Subsecretaría de Prevención del Delito.

3. Definiciones

SQL Server : Microsoft SQL Server es un sistema para la gestión de bases de datos producido por Microsoft basado en el modelo relacional. Sus lenguajes para consultas son T-SQL y ANSI SQL para el almacenamiento y tratamiento de la información.

Symantec Backup Exec : Sistema integral de respaldo que protege entornos físicos y virtuales, simplifica las copias de seguridad y la recuperación después de un desastre, y ofrece capacidades inigualables de recuperación. Basado en la tecnología V-Ray de Symantec, restaura servidores, aplicaciones críticas de Microsoft y entornos virtuales VMware o Microsoft Hyper-V para minimizar significativamente el tiempo fuera de servicio.

4. Flujo de Procedimiento



5. Procedimiento

5.1. Etapa de Autenticación

5.1.1. Inicio

El procedimiento se da por iniciado cuando un servidor requiere ser incorporado al sistema centralizado de respaldos.

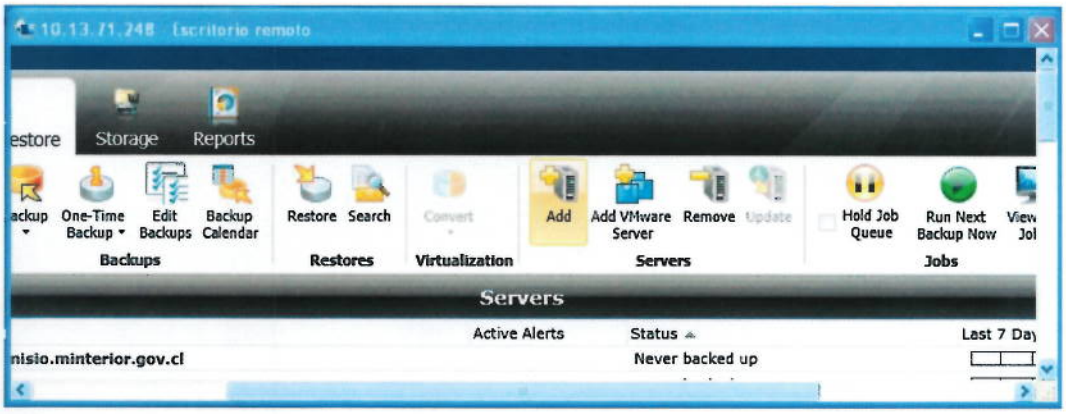
5.1.2. Acceder a servidor de respaldo

Se deberá considerar que el agente de respaldo ya se encuentra instalado en el servidor cliente (Véase Procedimiento de instalación de agentes de respaldo en servidores Red Hat Linux y/o Procedimiento de instalación de agentes de respaldo en servidores Windows Server), posteriormente deberá acceder al servidor de respaldo central "spd-respaldo" a través de escritorio remoto con la cuenta de administrador.

5.2. Etapa de Ingreso

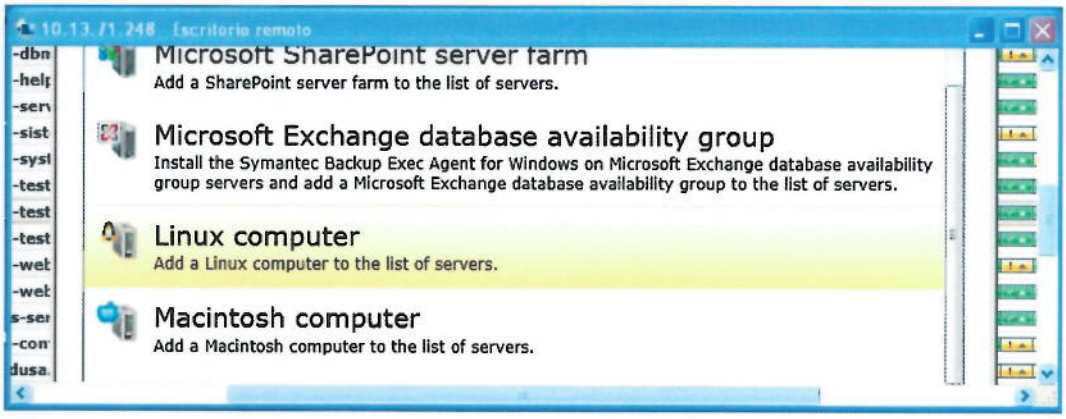
5.2.1. Incorporación de nuevo servidor

Inicialice el programa Backup Exec que se encuentra en el escritorio, seleccione en el menú superior la opción "Add" para ingresar el servidor cliente a respaldar.



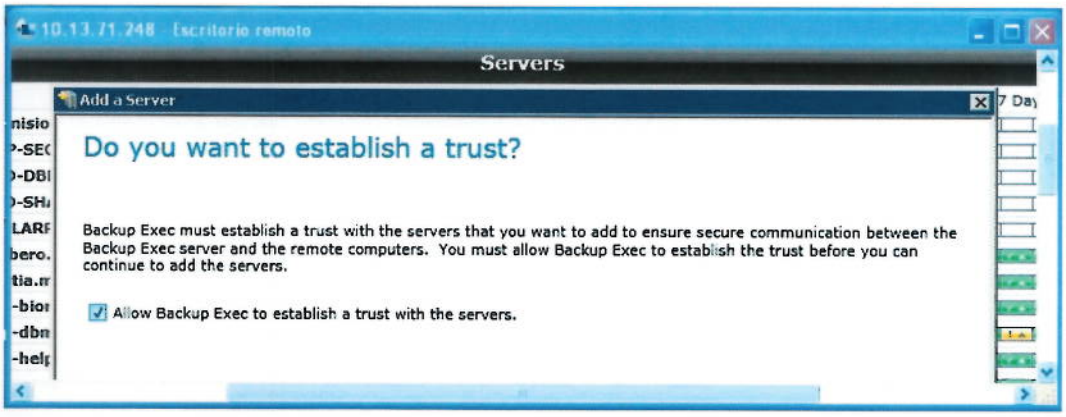
5.2.2. Registro de nuevo servidor

En la ventana emergente del aplicativo seleccione el servidor que corresponda a respaldar.



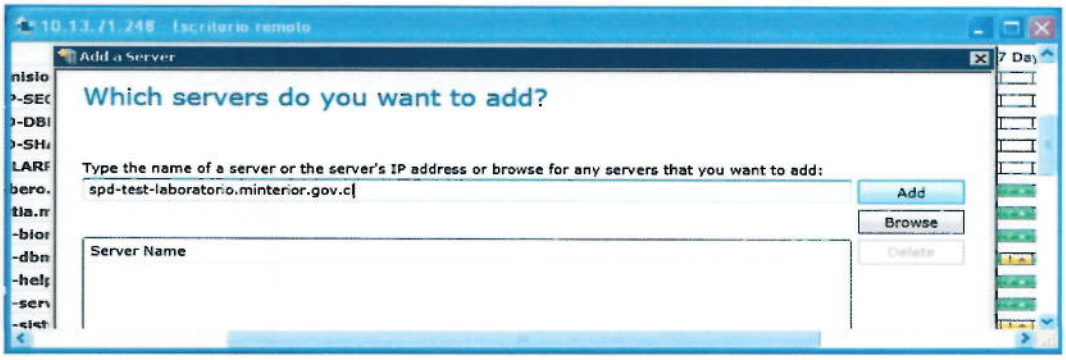
5.2.3. Establecer relación de confianza

Seleccione el checkbox para establecer una relación de confianza entre el servidor cliente y el servidor central, presione NEXT para continuar.



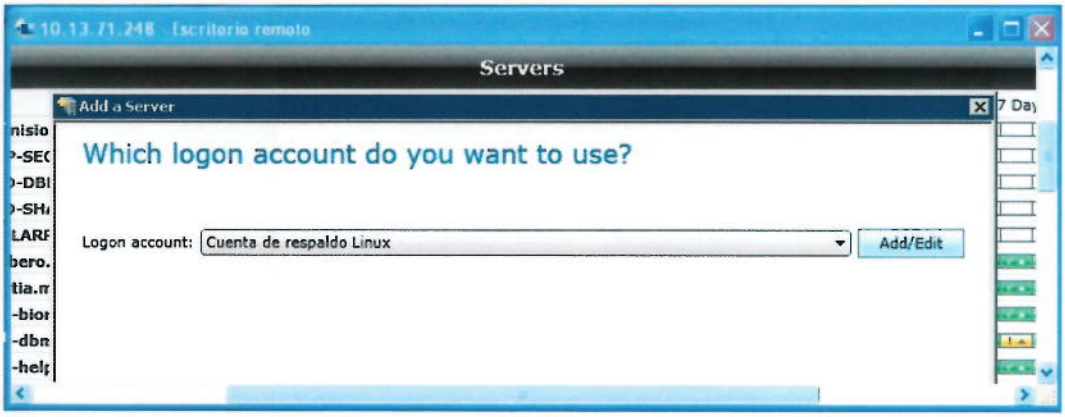
5.2.4. Registrar servidor cliente

Digite el nombre del servidor cliente que deberá ser respaldado, incluido el nombre de dominio en que se encuentra, presione NEXT para continuar.



5.2.5. Asignación de credenciales

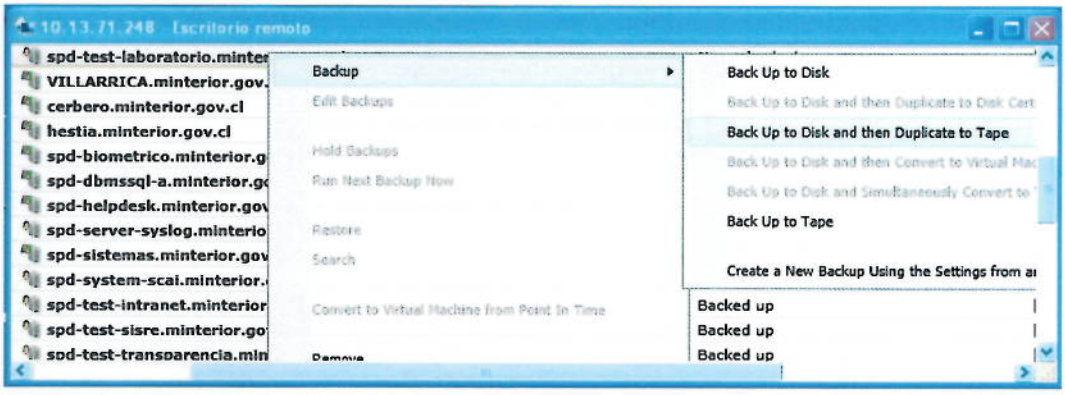
Seleccione la cuenta de usuario con que el sistema central deberá conectarse al servidor cliente para llevar a cabo el respaldo, presione FINISH para continuar.



5.3. Etapa de Configuración

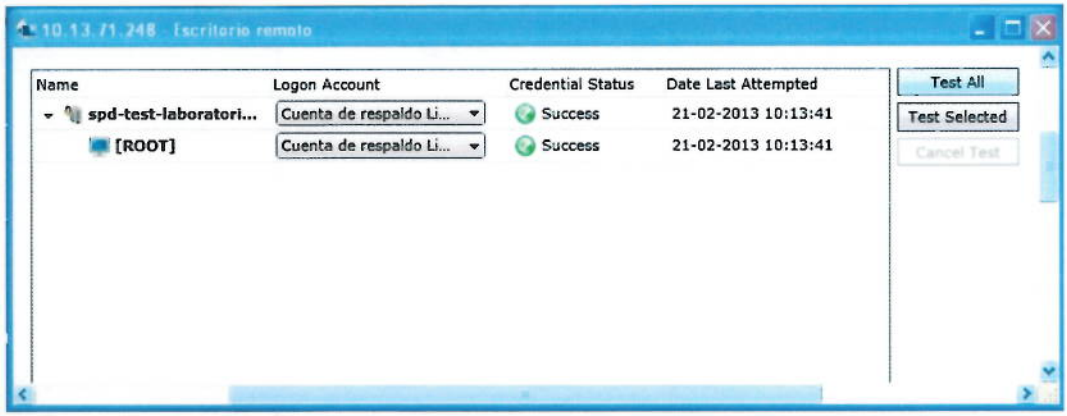
5.3.1. Definir protocolo de respaldo

Seleccione el servidor ingresado y haga click con el botón derecho del mouse, aparecerá un menú desplegable donde deberá seleccionar siempre la opción de respaldo en disco y respaldo en cinta.



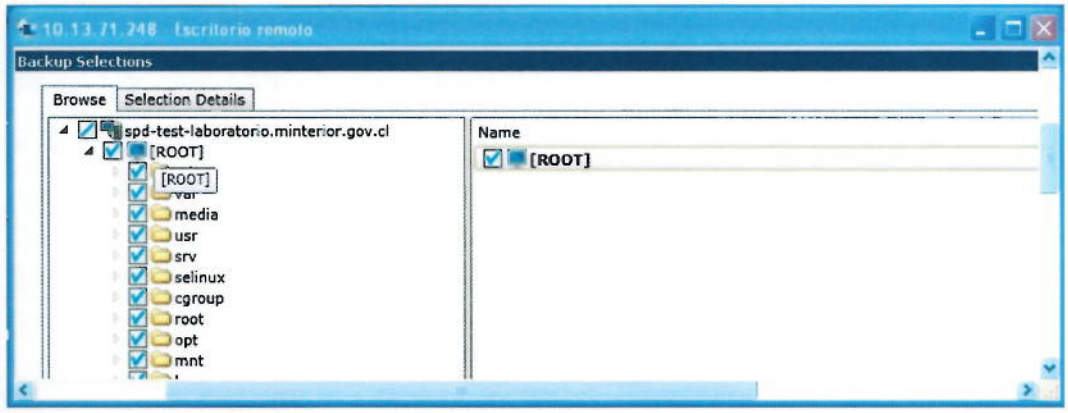
5.3.2. Validación de credenciales

Aparecerá una venta emergente de propiedades, seleccione la opción "Test Credentials" para verificar que la cuenta de acceso al servidor cliente es correcta.



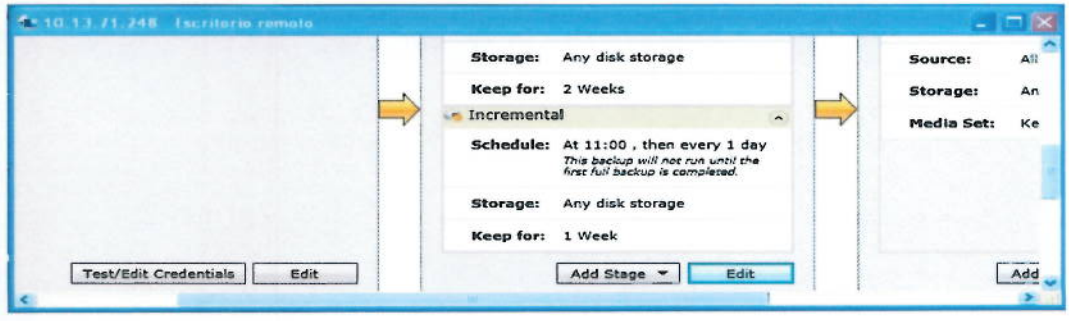
5.3.3. Selección de componentes

Seleccione los componentes o carpetas que deberán respaldarse, considere que las opciones cambiarán de acuerdo al sistema operativo en cuestión y en otras ocasiones aparecerán instancias de bases de datos como Oracle o MSSQL.



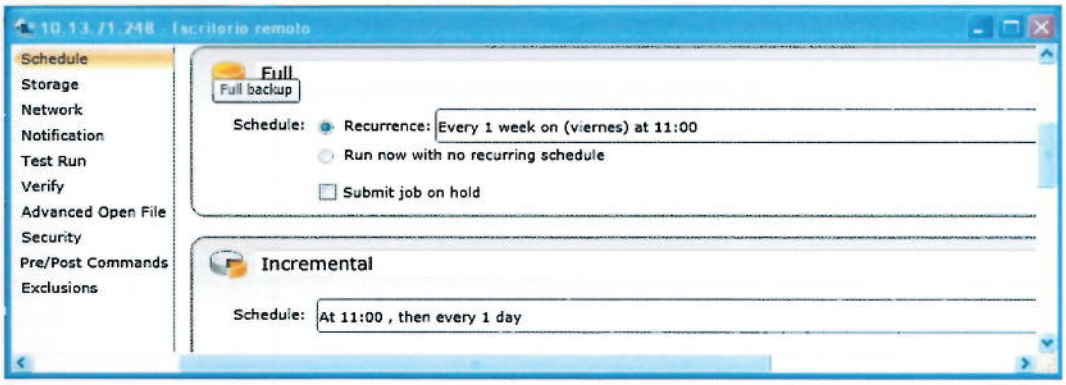
5.3.4. Configuración de respaldo

Una vez seleccionado los componentes a respaldar, deberá seleccionar la opción de respaldo para configurar el protocolo definido.



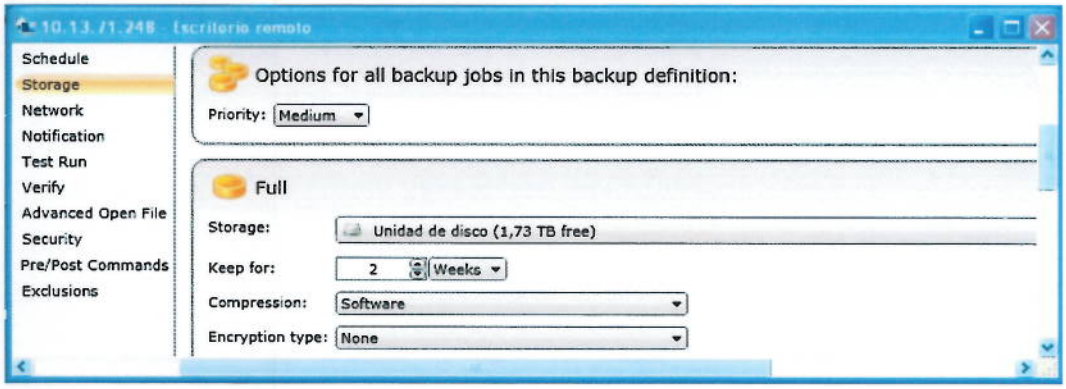
5.3.5.Programación de los respaldos

Seleccione la programación de respaldo según corresponda al calendario y a las ventanas de tiempo disponibles para llevarlo a cabo, considere además realizar siempre un respaldo completo a la semana y los otros días respaldos incrementales.



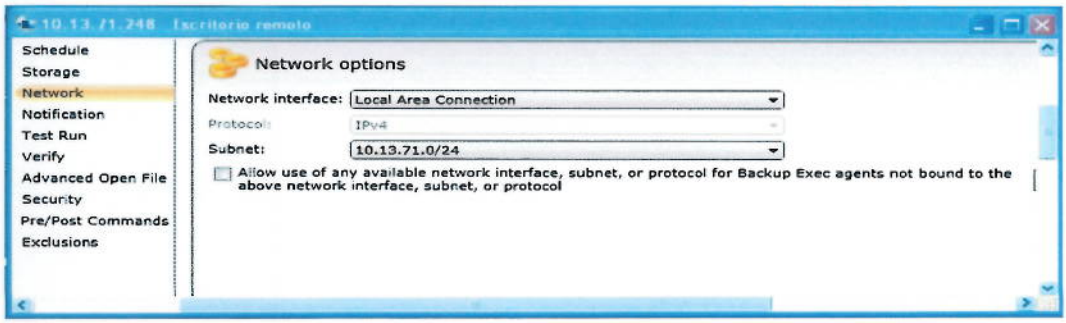
5.3.6.Almacenamiento en disco y cinta

Seleccione siempre prioridad "Medium" y aloje los respaldos en disco, defina una retención de una semana en esta unidad y habilite las propiedades de compresión del archivo de datos, aplique esta configuración para ambos respaldos.



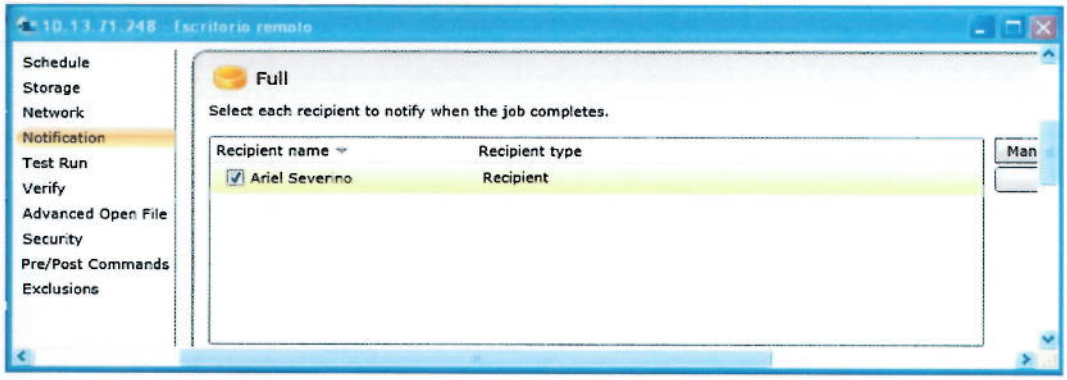
5.3.7.Acceso a nivel de segmento de red

Por seguridad se ha definido el acceso de servidores que se encuentren en el segmento crítico de red 10.13.71.0 del data center.



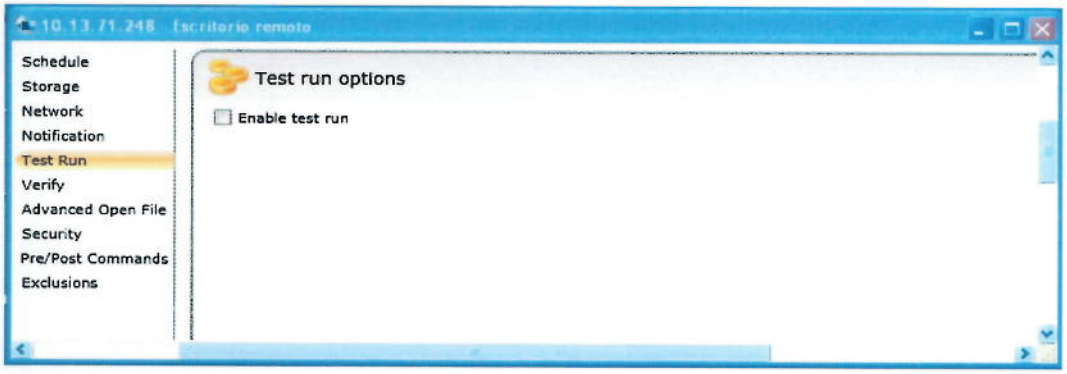
5.3.8. Notificaciones de actividades

Defina y seleccione los usuarios que deberán ser notificados sobre las actividades de respaldo, este informará siempre el resultado de la ejecución del trabajo.



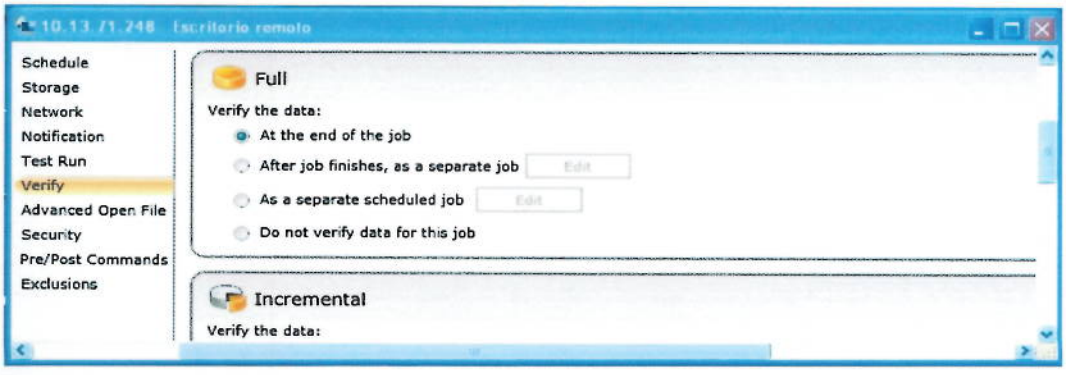
5.3.9. Pruebas de ejecución de respaldo

No seleccione la opción de "Enable test run", esto mejorará los tiempos de proceso de respaldo ya que la estimación de capacidad de almacenamiento ya se encuentra dimensionada.



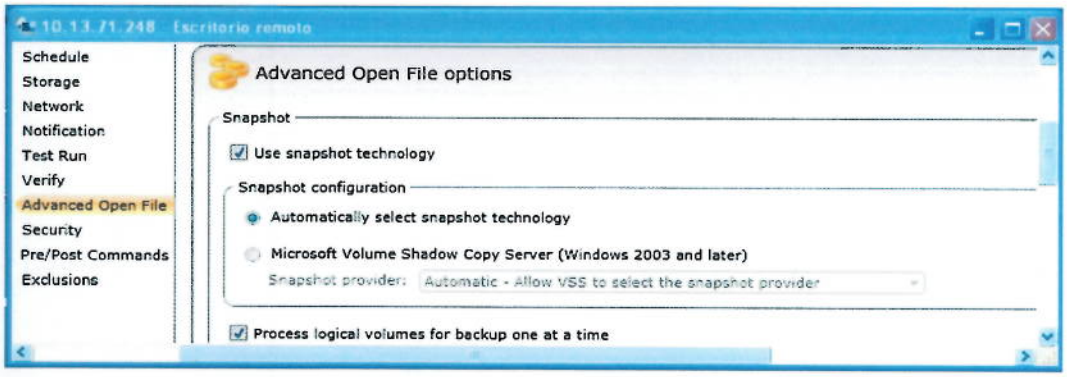
5.3.10. Verificación de integridad de respaldos

Seleccione siempre la verificación de los respaldos realizados, esto permitirá garantizar de mejor forma la integridad y la recuperación en caso de ser necesitado, aplique esta opción para ambos respaldos.



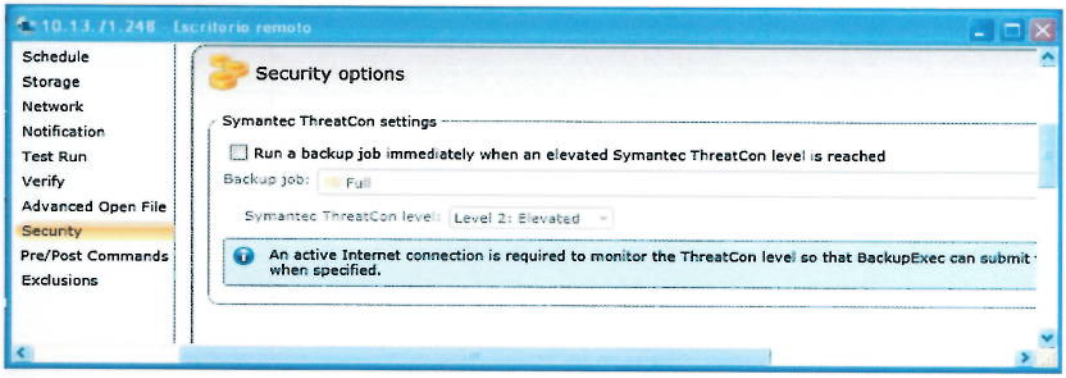
5.3.11. Opciones avanzadas de copia

Seleccione la opción de "Use snapshot technology" para todo respaldo y déjelo como automático, esto permitirá liberar los programas que están en memoria para desbloquearlos y lograr su respaldo.



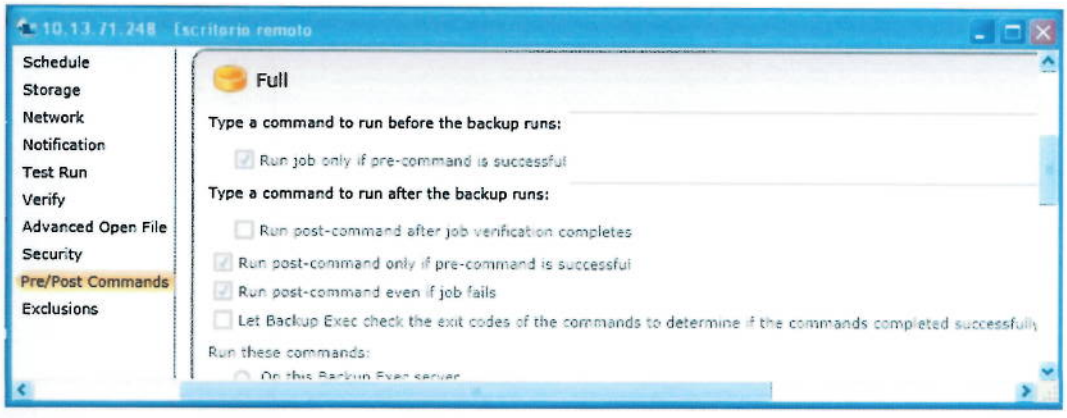
5.3.12. Opciones avanzadas de seguridad

Inhabilite las opciones de "Security options" ya que estás se activarán con los servidores de Symantec frente a posibles niveles de inseguridad que ellos determinen.



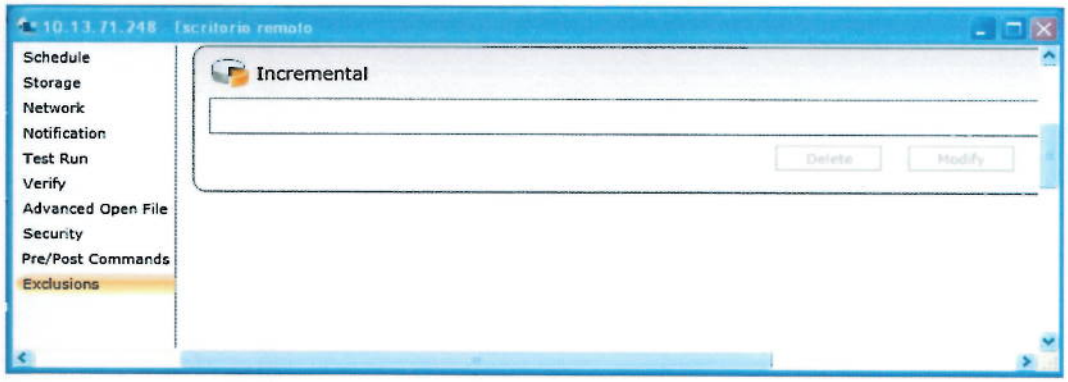
5.3.13. Ejecución posterior de comandos

Sólo en caso de ser requerido, defina los comandos deberán ejecutarse antes o después de cada proceso de respaldo.



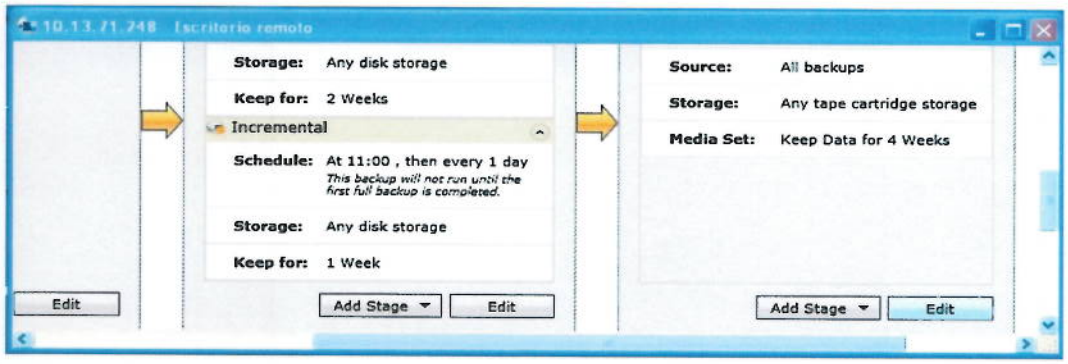
5.3.14. Exclusiones de archivos

Sólo en caso de aplicar, incorpore los filtros necesarios para excluir archivos o carpetas del proceso de respaldo.



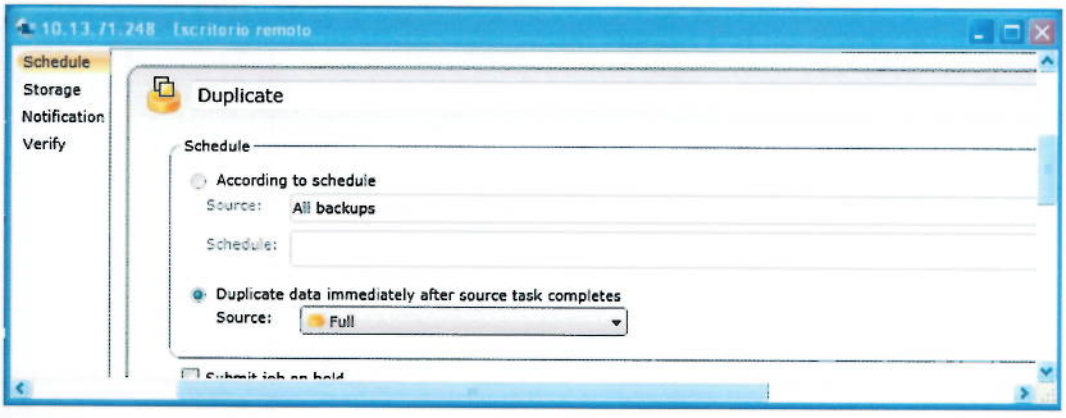
5.3.15. Configuración de duplicidad

Vuelva al menú de la ventana emergente y seleccione el submenú "Duplicidad", esto permitirá configurar los parámetros del respaldo duplicado que se irá a cinta.



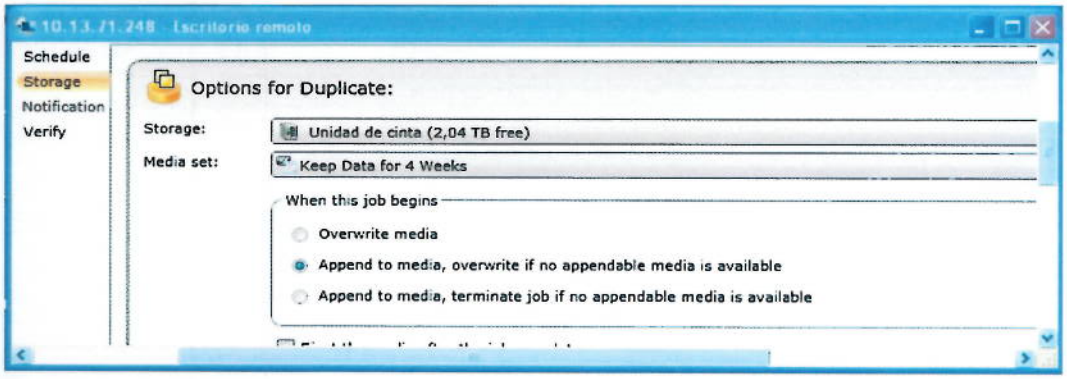
5.3.16. Programación de duplicidad

Para realizar la duplicación del respaldo de disco, se deberá considerar siempre que este sea realizado una vez terminado el respaldo completo de disco.



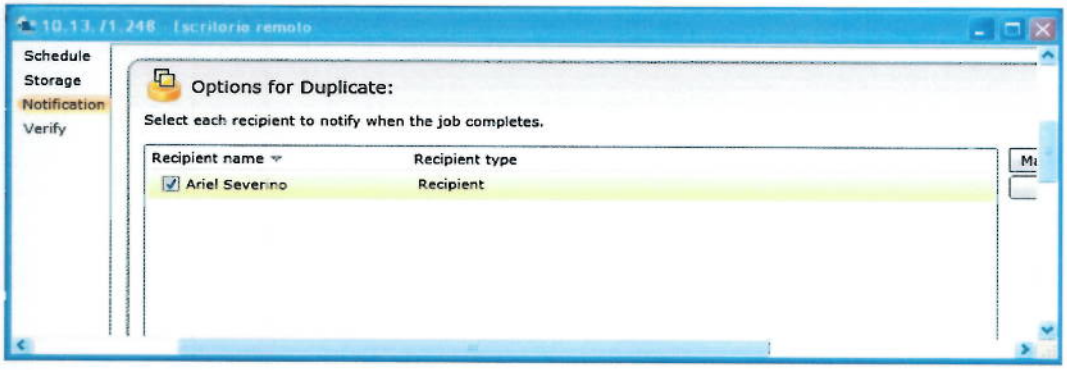
5.3.17. Almacenamiento de duplicidad

Seleccione la unidad de cinta como destino del respaldo, adicionalmente configure la retención por un período de cuatro semanas y activado la agregación de respaldos en caso de no quedar espacio.



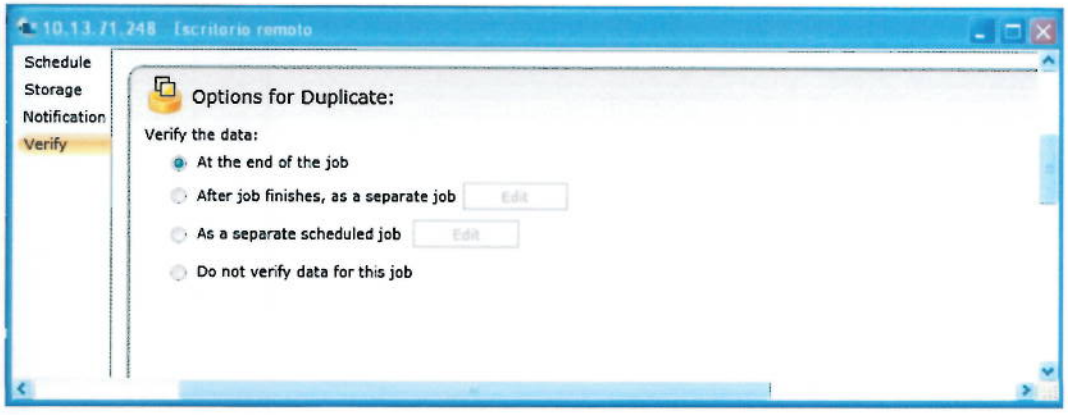
5.3.18. Notificaciones de duplicidad

Seleccione los destinatarios que serán confirmados una vez terminado el proceso de duplicación de respaldo.



5.3.19. Verificaciones de duplicidad

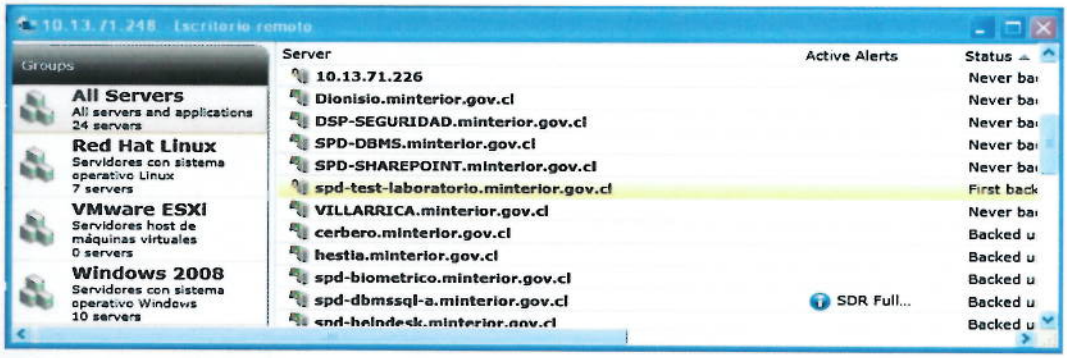
Seleccione siempre la verificación de respaldo de cinta, esto permitirá garantizar la integridad del archivo y alertar en caso de tener problemas.



5.4. Etapa de Verificación

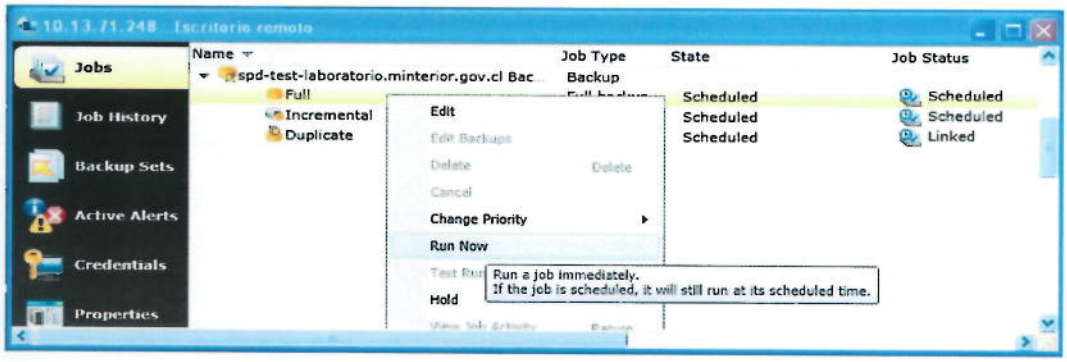
5.4.1. Verificación de ejecución

Seleccione el servidor que ha sido ingresado y configurado para ser respaldado y haga doble click sobre este para acceder a su administración.



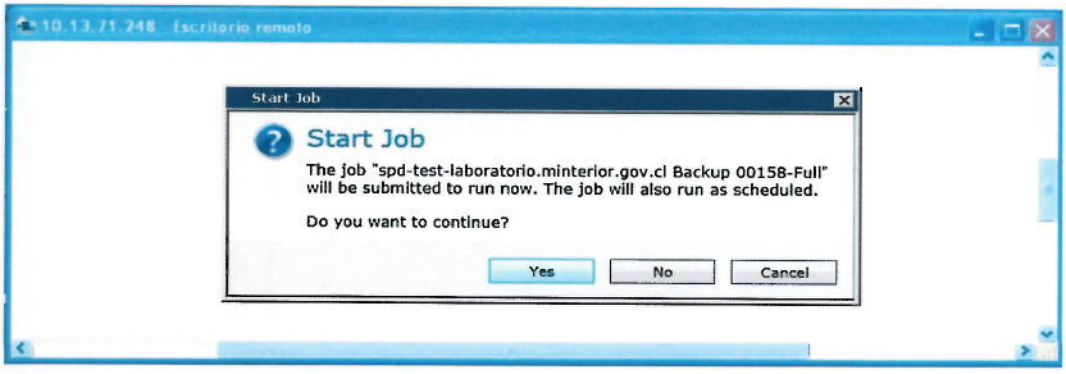
5.4.2. Ejecución de respaldo completo

Seleccione el submenú "Jobs" y desplegué las configuraciones de respaldo existentes, posteriormente deberá presionar el botón derecho del mouse sobre la configuración "Full" y ejecutar la opción "Run Now" que dará inicio al primer respaldo completo del servidor.



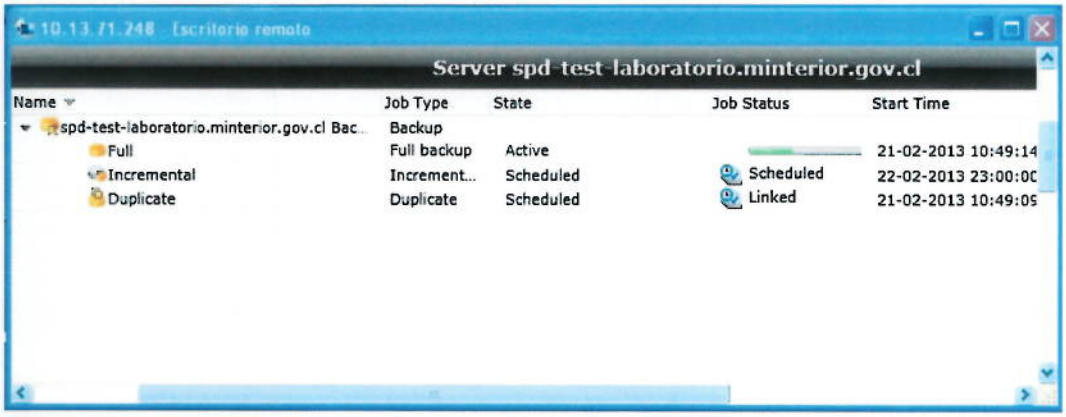
5.4.3. Confirmación de ejecución

El sistema le pedirá confirmar la ejecución del trabajo de respaldo, presione "Yes" para continuar con el procedimiento.



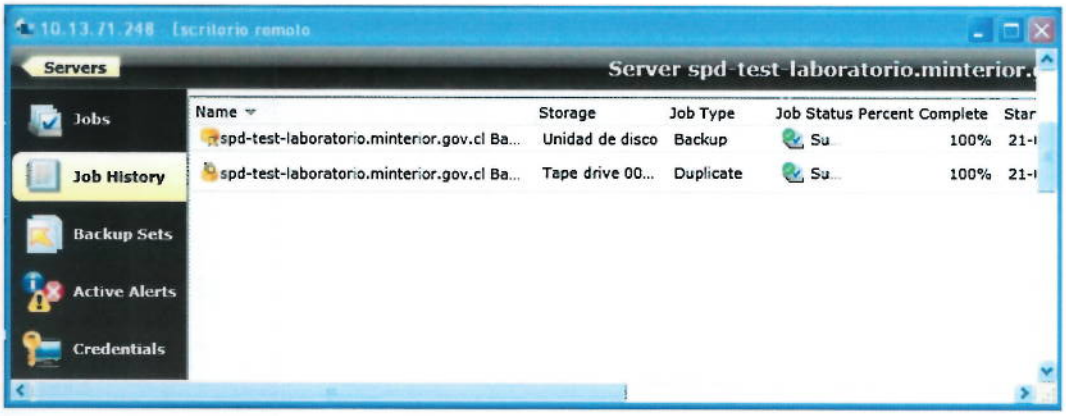
5.4.4.Proceso de respaldo inicial

En esta instancia, el servidor cliente se encuentra en proceso de respaldo, para lo cual se muestra una barra que indica el grado de avance de la operación, considere además que podrá visualizar mayor información haciendo doble click sobre esta tarea.



5.4.5.Validación de ejecución de respaldo

Para visualizar los resultados del trabajo de respaldo puede seleccionar el submenú "Job History" que le entregará información detallada sobre el proceso de respaldo.



5.4.6.Fin

El procedimiento se da por terminado.

6. Referencias

- Resolución Exenta N° 1.400/2012 - Aprueba la Política General de Seguridad de la Información de la Subsecretaría de Prevención del Delito.
- Resolución Exenta N° 1.892/2013 – Modifica Resolución Exenta N° 1.400, de la Subsecretaría de Prevención del Delito, que aprueba la Política General de Seguridad de la Información de la Subsecretaría de Prevención del Delito.
- Resolución Exenta N° 5.986/2015 – Modifica Resolución Exenta N° 1.892, de la Subsecretaría de Prevención del Delito, que aprueba la Política General de Seguridad de la Información de la Subsecretaría de Prevención del Delito.
- NCh-ISO 27001.Of2013 Tecnología de la Información – Técnicas de seguridad – Sistema de gestión de seguridad de la información (12.3.1.- Respaldo de información).
- NCh-ISO 27002.Of2013 Tecnología de la Información - Código de prácticas para la gestión de la seguridad de la información (12.3.1.- Respaldo de información).

7. Control Documental

Control de revisión

Nombre	Cargo	Actividad
Ariel Severino Fuentes	Coordinador Unidad de Proyectos, Tecnología e Innovación	Creación del documento
Mauricio Quitral Leiva	Coordinador Unidad de Operaciones y Soporte	Revisión del documento

Control de aprobación

Nombre	Cargo	Fecha	Firma
Alejandro Yuretic de la Cuadra	Jefe Departamento de Informática	05.07.2017	

Control de cambios

Versión	Cambio	Fecha	Aprobador
1.0	Aprobación y difusión del documento.	05.03.2013	Carlos Nuñez Duque
2.0	Se revisa vigencia de control y se adapta a nueva normativa NCh-ISO 27.001.Of2013. Se agregan al alcance la separación de las redes de desarrollo, prueba y producción respectivamente.	05.07.2017	Alejandro Yuretic de la Cuadra

Publicación y difusión

Listado de Distribución
• Intranet de la Subsecretaría de Prevención del Delito

8. Anexos