UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
Facultad de Estudios Superiores
Aragón
Ingeniería en Computación

DRP (Plan de Recuperación de Desastres), EMPRESA ESPECIALIZADA EN MANEJO DE DATOS Y SEGURIDAD INFORMÁTICA

TRABAJO ESCRITO
EN LA MODALIDAD DE DESARROLLO
DE UN CASO PRÁCTICO

PARA OBTENER EL TÍTULO DE:
INGENIERO EN COMPUTACIÓN

PRESENTA:
JESÚS NORBERTO VITAL ARGUELLES

ASESOR: ING. HUGO PORTILLA VÁZQUEZ

NEZAHUALCÓYOTL, ESTADO DE MÉXICO, ABRIL DE 2020.

Agradecimientos

Gracias a mis padres, Rosalía Argüelles Rosales y Norberto Vital Martínez, así mismo a mi hermano José Ricardo Vital Argüelles por ser los principales promotores y patrocinadores para alcanzar mis sueños; y por cada día, en este proceso de vida, confiar y creer en mí y en mis expectativas.

Gracias por cada consejo dado y por siempre desear y anhelar lo mejor para mí.

Agradezco también a mi asesor de tesis, al Ing. Hugo Portilla Vázquez, quien durante la realización de mi proyecto ha sido mi mentor y guía en este complejo proceso, compartiendo su amplio conocimiento y, sobre todo, brindándome su amistad.

El resultado de este trabajo de titulación excede con mucho mis expectativas y en gran parte se lo debo a usted, al tiempo y dedicación que ha tenido a bien compartir conmigo.

Mi gratitud por siempre, ingeniero Portilla Vázquez.

Por último, agradezco a la Universidad Nacional Autónoma de México, a la Facultad de Estudios Superiores "Aragón" y a sus autoridades y docentes por haberme dado la oportunidad de formarme y desarrollarme profesionalmente.

Gracias a todas las personas que, de manera directa o indirecta, concurrieron en este proceso y, en particular, a ese grupo de amigos que conocí y aprecio.

"POR MI RAZA HABLARÁ EL ESPÍRITU."

Índice

Capítulo I. Definiciones

I.1. Tipos de Riesgos

Debido al uso intensivo que se da actualmente de la tecnología y la transmisión de datos, los ciberataques se colocan cada vez más en altos niveles de riesgos que influyen de manera masiva en el panorama global.

Las consecuencias que se derivan de un ciberataque no se limitan solo a cuestiones económicas, sino que incluso se ponen en riesgo vidas humanas, como en el caso de la importancia que tiene el buen funcionamiento de los dispositivos enfocados a la salud.

Entre los principales riesgos que afrontan las instituciones destacan, entre otros, tanto la pérdida como la divulgación de información específica que se encuentra almacenada en dispositivos especiales.

A este tipo de dispositivos se les denomina en el ámbito empresarial como “Servidores NAS” (siglas en inglés de Network Attached Storage [almacenamiento conectado en red]) y “Servidores RDP” (siglas en inglés de Remote Desktop Protocol [protocolo para el escritorio remoto]), los cuales se destinan al almacenamiento de una cantidad impresionante de información.

En materia de seguridad informática, la tarea de proteger información importante, específica, sensible, se sustenta en los tres principios fundamentales a los que se les conoce como el Triángulo de la Seguridad Informática. Dichos principios son:

- **Confidencialidad**
- **Integridad**
- **Disponibilidad**

En específico, el tercer principio debe garantizar que la información que se encuentre almacenada en los servidores debe estar siempre disponible para su consulta, lo cual se pondría en riesgo con un ataque informático de ciberdelincuentes y haría que toda la tarea de resguardo resultara nula.

De lo anterior se desprende que cualquier elemento que esté conectado a Internet es propenso a sufrir daños importantes; y se considera que, para atenuar o solventar el riesgo, con la implementación de un plan DRP se daría respuesta a las amenazas que una organización puede sufrir en cuanto a inundaciones, actos vandálicos, incendios o, en su caso más particular, un ciberataque.

Una muestra de los tipos de ataques que pueden poner en riesgo el principio de disponibilidad se integra por:

1. **Ataques insider.**
2. **Ataques por ransonware.**

Abordaré primeramente los **ataques insider**, que se caracterizan por ser aquellos que se lanzan desde el interior de una empresa u organización.

El perfil del atacante puede ser desde un espía infiltrado por un Estado o por la competencia, un empleado alineado a grupos dedicados al terrorismo, simplemente un empleado descontento, un antiguo trabajador con ansias de venganza o un terrorista que busca colapsar una infraestructura crítica.

En general, el autor de estos ataques resulta ser un trabajador o excolaborador con acceso privilegiado y gran conocimiento de la infraestructura de la empresa u organización.

De acuerdo con las cifras reportadas por el instituto Ponemon en su informe *2016 Cost of Data Breach Study: Global Analysis,* relativo al estudio de 2016 sobre el costo de la violación de datos:

- El 48.0% de las violaciones de datos fue causado por *hackers* o *insiders*;
- El 27.0%, por fallas o errores en los procesos de TI o de negocio; y
- El 25.0%, por negligencias de empleados o colaboradores.

Para evitar ese tipo de ataques, recomiendo que:

- Se adquiera una solución funcional de ciberseguridad que, además de brindar protección avanzada, permita monitorear, detectar y ofrecer posibles soluciones.
- Se revisen las políticas de personal y de sistemas de control (gestión de cuentas para cada empleado, políticas de contraseñas seguras, supervisión de las acciones del usuario).
- Se adquiera un SIEM (siglas en inglés de Security Information and Event Management [información de seguridad y gestión de eventos]), el cual ayudará a producir un registro completo de todas las acciones del usuario.

Mi principal recomendación es en el sentido de que se mantengan actualizados el sistema operativo, las aplicaciones etc a fin de evitar que exista alguna vulnerabilidad y que ello se convierta en una oportunidad para que el o los atacantes actúen.

Algunas empresas junto con sus soluciones de seguridad podrían ayudar a prevenir o evitar esos riesgos o ataques serían:

- **CyberArk:** con su control y gestión de usuarios y su administrador de sesiones privilegiadas.
- **Logrhythm:** un SIEM que ayuda a obtener un registro de todas las actividades en la red.
- **FireEye network security:** se trata de una solución efectiva de protección contra amenazas cibernéticas que es capaz de tomar acciones ante algún ataque informático.
- **Forcepoint insider threat:** ofrece visibilidad de posibles amenazas internas, demuestra la intención de las acciones de los usuarios e identifica amenazas internas a sistemas críticos.
- **El uso de una solución DLP (Data Loss Prevention):** un ejemplo puede ser el de la compañía Symantec, el cual monitorea y protege la información corporativa confidencial, correos o archivos en un escenario de fuga de información.
- **Bloquear el uso de memorias flash:** conocidas como “USB”, ya que así se evita que se pueda propagar malware (programa malicioso) que facilite el ingreso de un atacante.

Por lo que se refiere a los ataques por **ransomware,** se trata de un programa que toma el control del sistema o dispositivo que infecta y pide un rescate para devolverlo a su dueño.

Proveniente del inglés *ransom*, “rescate”, un **ransomware** es un tipo de malware (programa maligno) que impide o limita el acceso del usuario a su propio sistema informático.

Un **ransomware** cifra y bloquea los archivos de las víctimas a las que se solicita un rescate, por lo regular en *bitcoins*, moneda electrónica, a cambio de recuperar el acceso a la información.

A octubre de 2019, el valor aproximado de un bitcoin era de 185,963.06 pesos.

En un estudio reciente de Kaspersky Lab (compañía internacional dedicada a la seguridad informática con sede en Moscú, Rusia) se expone que cerca de 20.0% de los usuarios que pagan el rescate nunca recuperan sus archivos.

Para proteger la información o tratar de recuperarla en caso de haber sido víctima de un ataque, la compañía Kaspersky recomienda que:

- **Se realicen con regularidad copias de seguridad.**
- **Se utilice una solución de seguridad, como un antivirus o un antimalware.**

- **En caso de recurrir a una solución de Kaspersky, se compruebe que esté habilitada la opción "Vigía Activa". Está opción está diseñada especialmente para la detección de ransomware.**

Ejemplos de este tipo de ataques se dirigieron entre 2018 y 2019 a entidades gubernamentales de Lake City y Riviera Beach (en el estado norteamericano de Florida), las cuales fueron impactadas por un ataque y para hacerle frente tomaron la decisión de pagar a los atacantes.

En 2018, varios sistemas en la ciudad de Atlanta (en el estado norteamericano de Georgia) fueron víctimas de otro ataque de **ransomware**, mientras que en mayo de 2019 fue el turno de la ciudad de Baltimore (en el estado norteamericano de Maryland); en dicho ataque, que entre otros servicios afectó la emisión de facturas para el cobro de agua, se solicitó el pago de 76,000 dólares por el rescate.

Otros ejemplos son los que afectaron a las administraciones españolas en la localidad de Jerez, toda vez que sus sistemas permanecieron bloqueados durante varios días y esto ocasionó pérdidas monetarias y operacionales muy altas.

Con base en mi experiencia laboral, me permito expresar las siguientes recomendaciones para efectos de protección:

▪ Usar un antivirus o un antimalware (Kaspersky o Malwarebytes).
▪ Mantener actualizado el sistema operativo.
▪ Evitar la instalación de programas que tengan que ser crakeados o parchados para poder obtener todas sus funciones como si se tratara de un programa original.
▪ Cerrar en las empresas el puerto 443, que es puerto por el cual es inminente su propagación.
▪ Si se tiene un IDS, en el registro del evento aparecerá una dirección IP; se deberá validar dicha dirección en las páginas donde se compruebe que es una dirección IP legítima o, en su defecto, que esté catalogada en la blacklist, por ejemplo:
- https://hetrixtools.com/
- https://www.ipvoid.com/ip-blacklist-check/
▪ Cerrar la comunicación con esa dirección IP desde el firewall.
▪ En caso de sufrir un ataque por este tipo de malware, ingresar a la página www.nomoreransom.org, en la que encontrarán disponibles algunas herramientas para descifrar archivos.

La mejor manera de proteger su negocio del **ransomware** es disponer de una copia segura y eficiente. Asimismo, debe probar regularmente su copia de seguridad para cerciorarse de que funciona de manera óptima y de que, cuando sea necesario, logrará tener un acceso rápido a sus datos en la copia de seguridad. https://www.ontrack.com/uk/blog/pieces-of-interest/what-you-should-include-in-your-disaster-recovery-plan-2/

¿Qué son los riesgos?

A los riesgos se les define como:

> **“La probabilidad de que una amenaza se materialice, utilizando la vulnerabilidad existente de un activo o grupos de activos, generándoles pérdidas o daños.”**
>
> FUENTE: Organización Internacional de Normalización (ISO).

Los principales riesgos a que todo equipo informático está expuesto son:

1. Deficiente control de acceso a las aplicaciones y falta de políticas de acceso correctas.

2. Existencia de vulnerabilidades web, lo que abre la puerta de acceso a los equipos de cómputo con la finalidad de que se obtenga información importante de la empresa.

3. Carencia en los controles de acceso a la red: la nula administración de la red y la falta de implementación de soluciones de seguridad, incrementan el riesgo de que se vulnere la seguridad de la red empresarial.

4. Fugas de información: la fuga de datos es en la actualidad uno de los mayores riesgos a los que se exponen las compañías.

5. Fraude y robo de información: realizado desde un correo **phishing** encargado por medio de ingeniería social, se hace creer a la víctima que es un correo legítimo y, como resultado, logra que se proporcione información importante.

6. Falta de planificación de la continuidad del negocio y del proyecto de recuperación ante desastres: sucesos ocasionados por la naturaleza o por el uso de los activos de la empresa pueden originar que, en algún momento, se registre alguna pérdida de información importante para la empresa, lo que provoca que sea estrictamente necesario contar con un adecuado plan de la continuidad del negocio y un plan de recuperación ante desastres.

7. Toda empresa debe contar con software original legítimo, ya que el uso de software “crakeado” o “pirata” puede facilitar diferentes tipos de ataques, como lograr que se tenga acceso al equipo informático de la institución, conseguir privilegios de “administrador”, iniciar un movimiento lateral que derive en un control absoluto o infiltrarse en equipos de suma importancia donde se encuentre información muy sensible.

I.2. Tipos de Ataques

En el entendido de que los ciberataques representan las amenazas más grandes que deben enfrentar hoy en día las empresas u organizaciones, a continuación, hago una breve descripción de los **tipos de códigos maliciosos usados por atacantes informáticos:**

- **Troyanos:** encargados de abrir puertas traseras para permitir la entrada de otros programas maliciosos.

- **Spyware:** programa espía, cuyo principal objetivo es obtener la información que se esté manipulando en el equipo; normalmente suele trabajar en segundo plano, es decir, sus procesos de captura de información no son visibles ante el usuario, lo que a su vez le permite ocultarse hasta el momento en que sea necesario y transmitir la información recopilada a un destinatario; en este caso, el atacante**.**

- **Adware:** posiblemente el más común en páginas de Internet; si bien su principal función es mostrar publicidad, se le considera como un **spyware,** ya que recolecta y transmite información de los usuarios mediante un estudio del comportamiento.

- **Ransomware:** el **malware** más sofisticado, peligroso y popular hoy en día en la red, su función es secuestrar (encriptar) la información almacenada en el equipo de cómputo y solicitar un pago por liberarla; el rescate se debe pagar mediante bitcoins, moneda electrónica.

- **Phishing:** la técnica de **phishing** no se considera software, más bien se deriva en las diversas técnicas de suplantación de identidad para obtener datos de la víctima; esta técnica es muy usada mediante correo electrónico o llamadas telefónicas, haciéndose pasar por alguna entidad financiera y solicitando datos que después serán usados para cometer algún ilícito.

- **Denegación de servicio distribuido (DDoS):** es uno de los ataques más temidos, ya que, por un lado, resulta fácil de ejecutar y, por otro, es difícil rastrear al atacante. Los ataques de **DDos** consisten básicamente en realizar tantas peticiones a un servidor como sean posibles; esta acción en el servidor, al recibir demasiadas peticiones en intervalos cortos de tiempo, logran bloquearlo o inclusive llevarlo al colapso, lo que redunda en pérdidas para la empresa.

I.3. Software Iperius

Iperius Backup, desarrollado por *Enter srl,* es un software de copia de seguridad y una utilidad de sincronización compatible con todas las plataformas Windows.

Este software permite hacer copias de seguridad automáticas de archivos y carpetas en diferentes dispositivos, como:

- Discos duros externos USB.
- Unidades RDX.
- NAS.
- Unidades de cinta LTO/DAT.
- Equipos en red.
- Servidores remotos a través de FTP o Cloud Storage.
- Permite hacer la copia de seguridad de base de datos.
    - SQL Server
    - Oracle
    - PostgreSQL
    - MySQL,
- Imagen y recuperación de desastres.

Imagen Núm. 1. Logotipo del software Iperius.

I.4. Tipos de Respaldos

I.4.1. Respaldo Full

La copia de seguridad completa siempre reproduce todos los archivos, sobrescribiendo en los posiblemente ya existen.

El tiempo necesario para completar la copia de seguridad será siempre el mismo porque en cada copia todos los archivos se reproducirán nuevamente y se sobrescribirán.

I.4.2. Respaldo Incremental

Iperius realizará primero una copia completa de los archivos o una completa copia del disco que se tenga instalado en el equipo y, a continuación, en las copias posteriores reproducirá solo los archivos nuevos o modificados (en este caso, sobrescribiendo los archivos en el destino).

El resultado de este tipo de copia de seguridad es siempre una copia completa, que se actualiza de vez en cuando con los archivos nuevos o modificados.

Este modo es adecuado, ya que optimiza el rendimiento y reduce las escrituras en disco, así como en el ancho de banda requerido en el caso de copias de seguridad en red o remotas.

I.5. Servidores DRP

Se trata de un dispositivo diseñado para el almacenamiento mediante la red informática de la empresa.

Comparte sus unidades (discos duros) por red; estos sistemas de almacenamiento en red son perfectos para realizar copias de seguridad de información crítica o especial de la empresa que se traduce en la creación de una “nube privada” a la que solamente ciertos usuarios pueden tener acceso.

Cuentan con características especiales, como un sistema operativo; con una configuración de sus discos denominada “RAID” para garantizar mayor seguridad de la información; y están adaptados para funcionar todo el día.

Imagen Núm. 2. Servidor NAS con dos bahías de almacenamiento.

Imagen Núm. 3. Servidor NAS “Dell” con 16 bahías de almacenamiento.

I.5.1. Qué es un RAID

RAID son las siglas en inglés de **Redundant Array of Independent Disks.** Esta configuración combina varios discos duros para crear una sola unidad de almacenamiento, donde al escribir o guardar información en uno de ellos se almacena en todos los discos.

Estas configuraciones permiten tener una tolerancia alta contra las fallas que se llegaran a presentar, ya sea por variaciones de voltaje que podrían dañar a la unidad o por fallas mecánicas de los dispositivos.

Si se llegaran a presentar fallas en un disco, los demás continúan funcionando y permiten la consulta de datos como si nada hubiera ocurrido.

Para la correcta configuración de un RAID es necesario utilizar al menos dos discos duros.

I.5.2. Tipos de RAID

Los tipos de RAID más usados son los siguientes:

RAID 0 (requiere como mínimo dos unidades de disco duro).

Este tipo de RAID no ofrece tolerancia a fallos, pero una ventaja notoria es que brinda mayor velocidad.

En un RAID 0 los datos son almacenados entre los discos sin agregar ningún control de errores; en cada uno se escribe un bloque, es decir, la información será exactamente la misma en los dos discos.

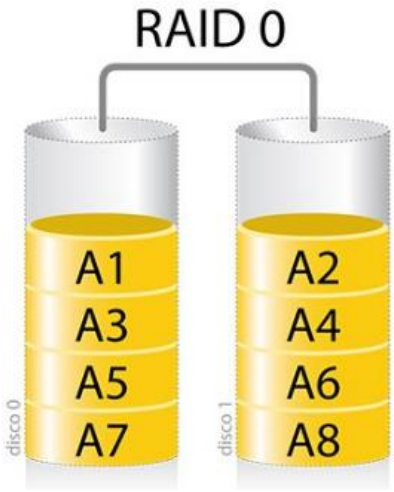

Imagen Núm. 4. Representación gráfica de un RAID 0.

RAID 1 (requiere como mínimo dos unidades de disco duro).

Conocido como **“mirroring”** o “espejado”, este raid funciona replicando todos los datos de un disco a otro.

Si se tiene una configuración de dos discos, ambos tendrán exactamente la misma información. este RAID es más tolerante a fallos y en servidores se usa solo para datos críticos, como es la instalación del sistema operativo.

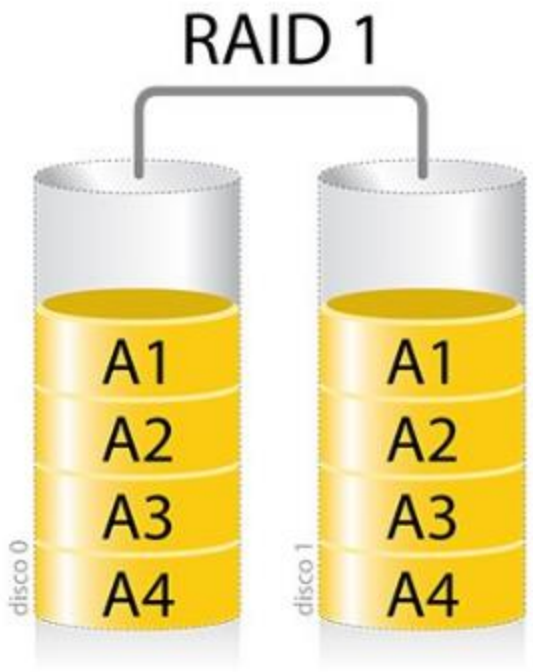

Imagen Núm. 5. Representación gráfica de un RAID 1.

RAID 3 (requiere como mínimo tres unidades de disco duro).

La información se almacena en dos discos y el último es utilizado para crear un cálculo sobre los demás; si uno de estos discos presenta una falla, el sistema es capaz de recuperarlo usando la información de los demás discos.

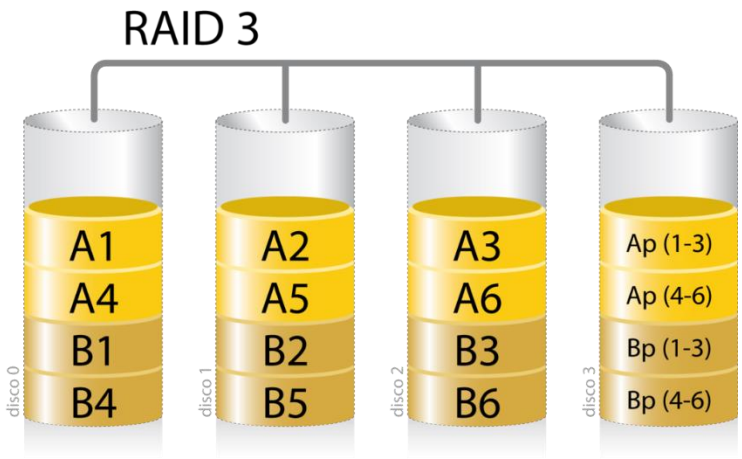

Imagen Núm. 6. Representación gráfica de un RAID 3.

RAID 5 (requiere como mínimo tres discos duros).

Se trata de uno de los arreglos de disco más adecuado para los servidores NAS que utilizan las empresas.

En este arreglo se logran repartir los datos en todos los discos; y si bien cada uno de ellos contiene una "copia de seguridad" de ciertos datos que pertenecen a otros discos (más que una copia, es información que puede ayudar a la recuperación de datos cuando se tenga que reconstruir un arreglo en caso de que se registre una falla), con este tipo de arreglo se pierde la capacidad de uno de los discos duros.

Por ejemplo, si se tienen cuatro discos duros de 2 TB, al efectuar un RAID 5 el resultado final de almacenamiento será de 6 TB de almacenamiento libre.

Suponiendo que se registra alguna falla en uno de esos cuatro discos duros configurados en un RAID 5, se podrá recuperar la información perdida de dicho disco, ya que la información está repartida en los otros tres discos; pero si en un escenario posible llegara a fallar alguno de los tres discos mencionados anteriormente, se perderá toda la información.

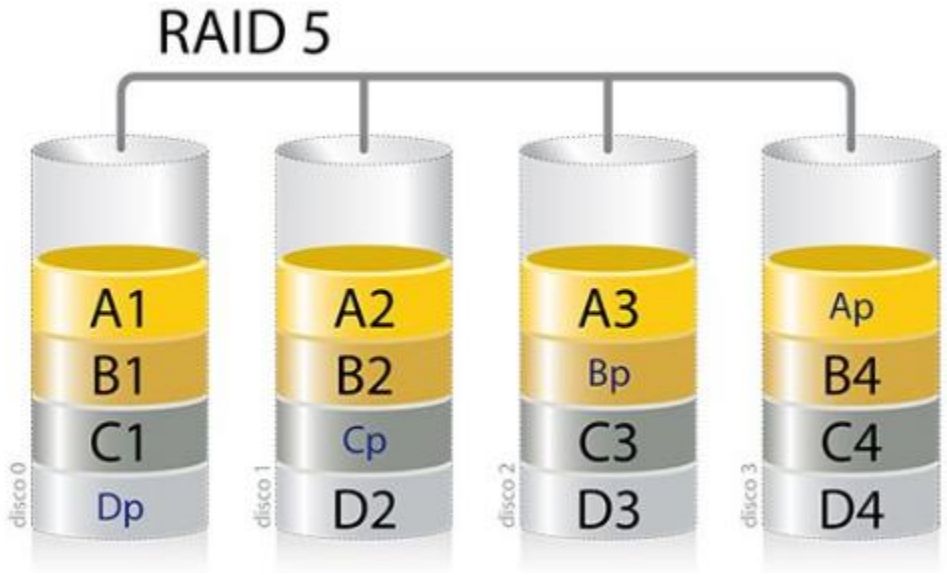

Imagen Núm. 7. Representación gráfica de un RAID 5.

I.5.3. Ventajas de los RAID

Dependiendo de las necesidades que se tengan, se recomienda seguir esta guía sobre qué tipo de RAID es el más adecuado (0, 1 o 5):

RAID 0: Es de utilidad si solo se desea tener velocidad y un almacenamiento grande, pero si se llegara a presentar un error no es posible recuperar datos; es adecuado para el diseño de enormes gráficos y la edición de video en HD.

RAID 1: Esta configuración es adecuada para entornos donde la continuidad del trabajo sea muy importante; por ejemplo, en lugares donde el servidor esté trabajando las 24 horas.

Se debe tener presente que la capacidad de almacenamiento se divide a la mitad; una mitad es para guardar datos y la otra se usará para tener una copia exacta del primer disco.

RAID 5: Es ideal para donde sea necesario aumentar la velocidad y a la vez contar con resistencia a fallos.

Otorga rendimiento rápido y protección al guardar los datos; y se destina un ¼ de la capacidad de cada disco para la tolerancia a fallos.

I.6. Máquinas Virtuales

Se trata de un equipo que de manera virtual se ejecuta mediante un virtualizador (software como VMware o Virtual Box) utilizando los recursos como memoria Ram, capacidad de almacenamiento del disco duro y el procesador del equipo anfitrión (equipo físico).

Esto se complementa con una simulación de redes virtuales configurables según las propias necesidades.

Ello se deriva en dos tipos de máquinas virtuales y la principal diferencia entre ellas es su funcionalidad:

- **Máquinas virtuales de sistema.**
- **Máquinas virtuales de proceso.**

I.6.1. Máquinas Virtuales de Sistema

Este tipo de máquinas virtuales emulan a un equipo en su totalidad haciéndolo pasar por **"Otra PC",** de tal modo que permiten la ejecución de un sistema operativo diferente del instalado en el equipo anfitrión.

Posee su propio disco duro, memoria Ram y demás componentes de hardware, los cuales son utilizados desde el equipo anfitrión.

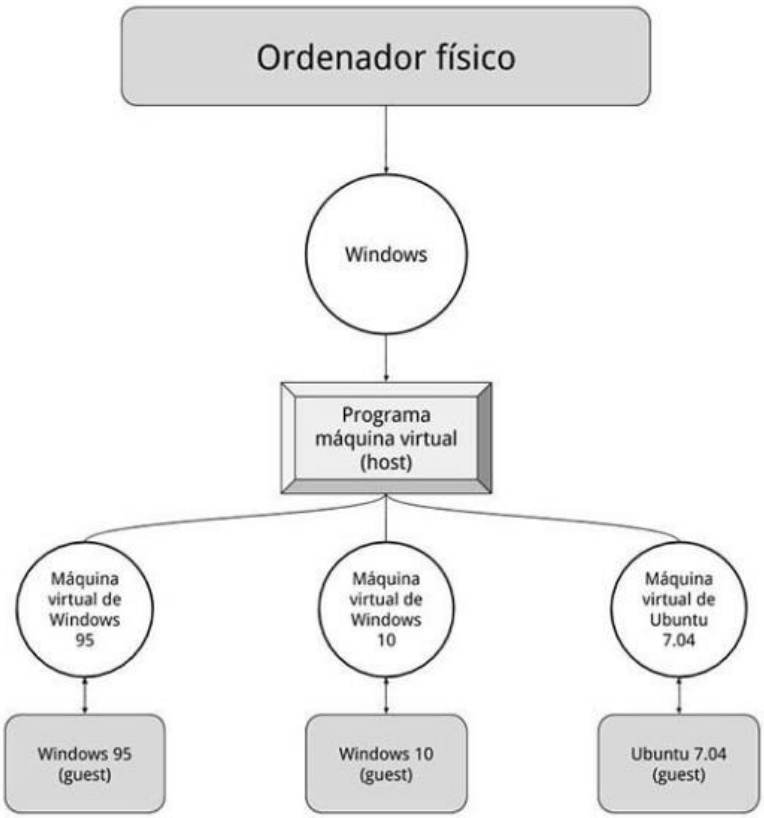

Imagen Núm. 8. Representación de un sistema virtualizado.

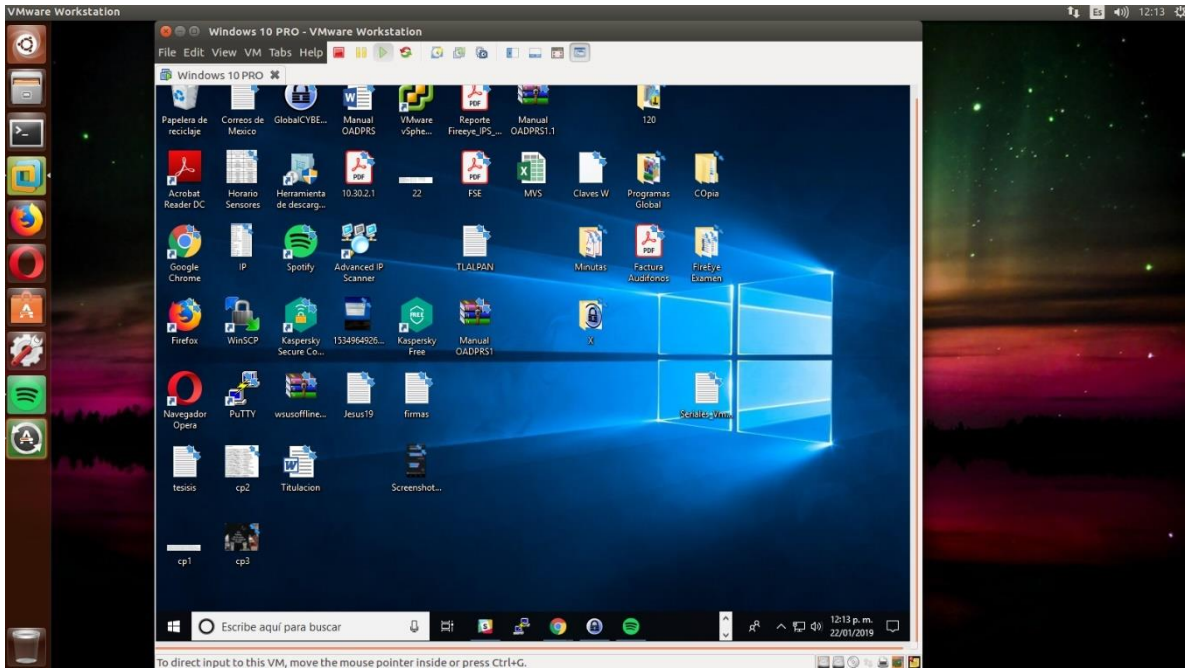

Imagen Núm. 9. Sistema operativo anfitrión (Ubuntu 16.04 LTS) ejecutando una máquina virtual VMware (Windows 10).

I.6.2. Máquinas Virtuales de Proceso

También conocida como **máquina virtual de aplicación**, cuyo funcionamiento es un proceso normal dentro del sistema operativo, está diseñada para soportar un solo proceso.

Hoy en día se usa con frecuencia, por ejemplo, cuando se ejecuta una aplicación basada en el lenguaje de programación Java o en .NET Framework.

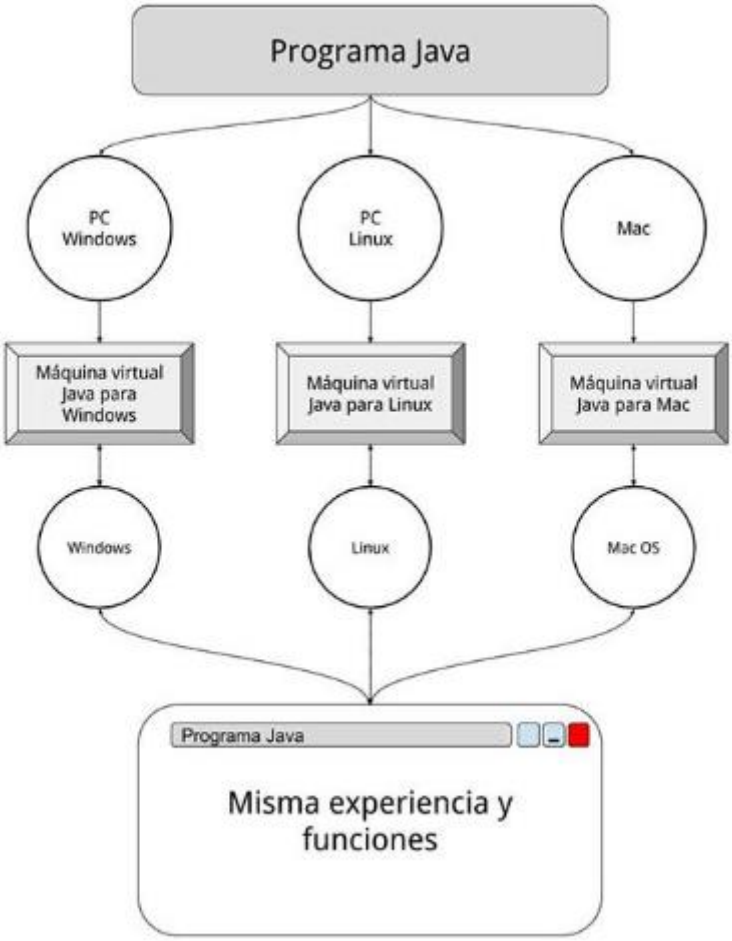

Imagen Núm. 10. Representación gráfica de una máquina virtual de proceso.

I.6.3. Software para virtualizar

VMware: aunque se trate de una versión de paga (VMware Workstation), de igual forma cuenta con una versión gratuita (VMware Player), la cual permite virtualizar cualquier sistema operativo y compartir los recursos del equipo anfitrión.

Imagen Núm. 11. Logotipo del software para virtualizar.

Virtual Box: se trata de una versión gratuita que permite crear máquinas virtuales, es propiedad de Oracle y facilita la ejecución de varias máquinas a la vez.

Imagen Núm. 12. Logotipo del software para virtualización.

I.6.4. Tipos de Redes Disponibles

En el software para virtualizar se encuentran diferentes tipos de conexión que pueden ser asignadas a los equipos según sus necesidades.

- Bridge.
- Host-Only
- NAT.

Bridge: el equipo virtual se considera como un equipo físico conectado a la misma red y recibe una dirección IP única, ya sea del servidor DHCP o de nuestro módem.

Host-Only: se trata de una comunicación solo con los equipos que estén configurados en este modo y se encuentra aislada de la salida a Internet.

NAT: la conectividad de la máquina virtual es mediante una IP totalmente diferente de la IP del equipo físico; y si se intenta comunicar desde el equipo virtual hacia el equipo físico o a Internet lo hace a través de un firewall propio dentro de la aplicación de virtualización.

I.6.5. Ventajas de virtualizar

Las principales ventajas para tomar la decisión de virtualizar son las siguientes:

1. Se puede instalar cualquier sistema operativo para probar o realizar experimentos, ya sea desde programación hasta laboratorios de hacking ético e inclusive antes de actualizar un sistema operativo.

2. Si se tiene instalado el sistema operativo Linux y se necesita usar alguna aplicación que solo funciona en Windows, esto se puede hacer a través de una máquina virtual.

3. Se pueden ejecutar aplicaciones viejas, muchas aplicaciones que no recibieron alguna actualización de su equipo de desarrollo para que funcionen de manera correcta en sistemas operativos viejos, como es el caso de Windows XP (sistema operativo que dejó de ser soportado por Microsoft en el año 2008).

4. Probar una aplicación en distintos sistemas; si uno es desarrollador, la principal meta es que las aplicaciones funcionen de manera correcta y probarlas en los diferentes sistemas para considerar posibles cambios.

Capítulo II. Copias de Seguridad

II.1. Proyecto DRP

Durante los últimos semestres de mi carrera entré a trabajar en la empresa de ciberseguridad llamada **Global Cybersec,** ubicada al sur de la Ciudad de México; es una empresa mexicana de consultoría especializada en servicios de seguridad informática, con experiencia en gestión de seguridad de TI, administración de SOC/CERT (Security Operation Center) y sistema de monitoreo de incidentes.

Para atender los servicios que proporciona, sus divisiones son:

*** Blue Team:**

Equipo encargado de la gestión y respuesta a incidentes.

Análisis de seguridad de la infraestructura de TI.

Monitoreo de incidentes de seguridad.

Cibervigilancia

*** Red Team:**

Hacking ético.

Análisis de vulnerabilidades

Análisis forense.

Laboratorio de malware.

Me incorporé al Blue Team como consultor de ciberseguridad y fui asignado a un proyecto que en ese momento la empresa estaba desarrollando con un cliente.

Mi principal tarea fue tener comunicación constante con el cliente para saber sus necesidades y entender la dinámica de trabajo de todo su equipo.

II.2. Respaldo Full de un Sistema Operativo

El respaldo full de un sistema operativo, también conocido como **Windows Image Backup,** consiste en una copia de seguridad del sistema completa (sistema operativo, programas instalados, etc.) para poder utilizarla en cualquier momento en caso de una eventual pérdida de datos.

En el proyecto en que participé se plantearon varios escenarios; en el primero, hacer la copia de seguridad (Windows Image) de algunos servidores importantes para el cliente, tarea que se nos facilitó con la herramienta Iperius.

El objetivo fue ejecutar la copia de seguridad del servidor “origen” y enviarla a través de la red del cliente hacia un equipo NAS ubicado en otro edificio, con medidas de seguridad extremas por parte del cliente.

La finalidad es, en un caso de pérdida de información o de falla del sistema, restaurar el servidor en el menor tiempo posible y continuar las actividades en un lapso determinado de tiempo.

Imagen Núm. 13 . Windows 7 por realizarle un backup Windows Image.

En esta captura de pantalla se muestra un Windows 7, al cual se le hará un backup full de la imagen de sistema tal como se ejecutó en los equipos del cliente.

II.2.1. Configuración de la Tarea “FULL Windows Image”

Una vez instalado el software en el equipo que se habrá respaldar, se debe configurar la tarea FULL Windows Image conforme a los pasos que se detallan a continuación.

1. Dar clic en la opción **“Crear nueva tarea de copia de seguridad”,** como se muestra en la imagen siguiente:

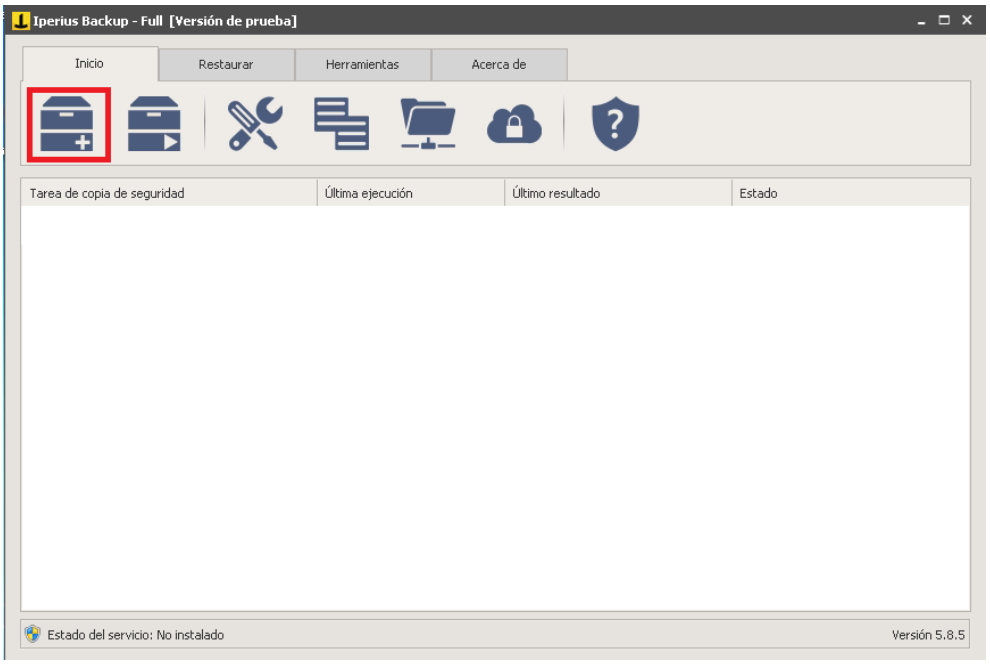

Imagen Núm. 14. Crear nueva tarea de copia de seguridad.

2. Clic en la opción Windows Image Backup, tal como se muestra en la siguiente imagen:

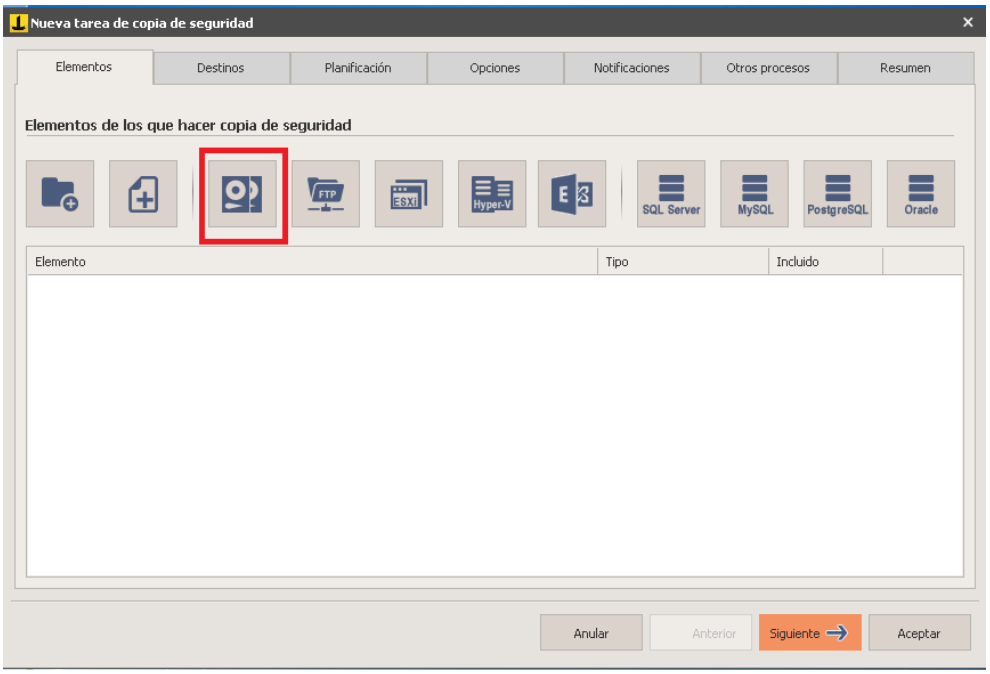

Imagen Núm. 15. Windows Image Backup.

3. Al dar clic en la opción anterior, nos mostrará la siguiente imagen, en la cual debemos seleccionar el disco que se habrá de respaldar; en algunos casos el equipo puede tener dos discos, los cuales deberán ser seleccionados.

    a. Seleccionar el disco que se deberá respaldar, en este caso se trata de la unidad C:\.
    b. Seleccionar el destino de la ruta de red, para lo cual se deberá colocar la dirección IP y la carpeta donde se almacenarán los respaldos; como nota importante, la carpeta donde se almacenará la información debe estar compartida para facilitar al software su rápida localización.
    c. Clic en la opción “Utilizar la siguiente cuenta de usuario para acceder a la red”; esta opción es de suma importancia, ya que si no se configuran las credenciales correspondientes no se podrá efectuar el backup.

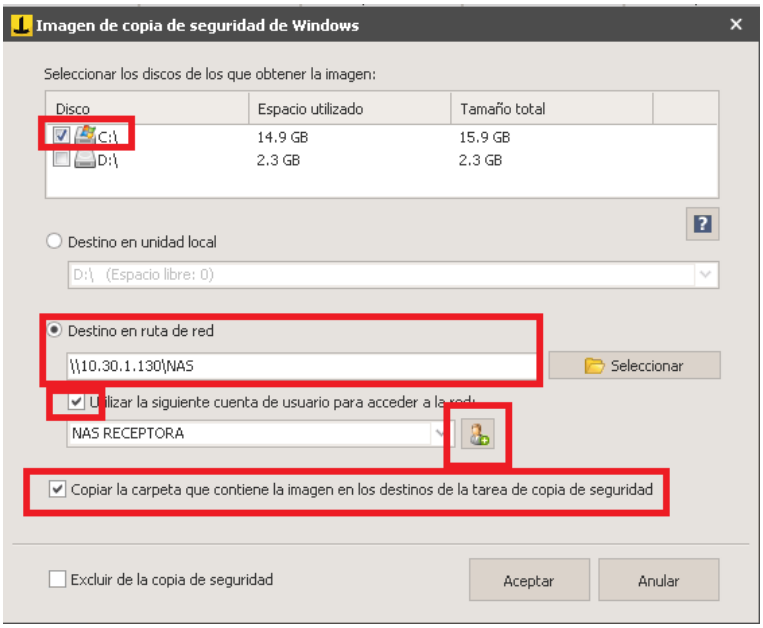

Imagen Núm. 16. Configuración de la copia de seguridad.

d. Clic en la opción “Agregar cuenta”.
e. Clic en la opción “Nuevo”.

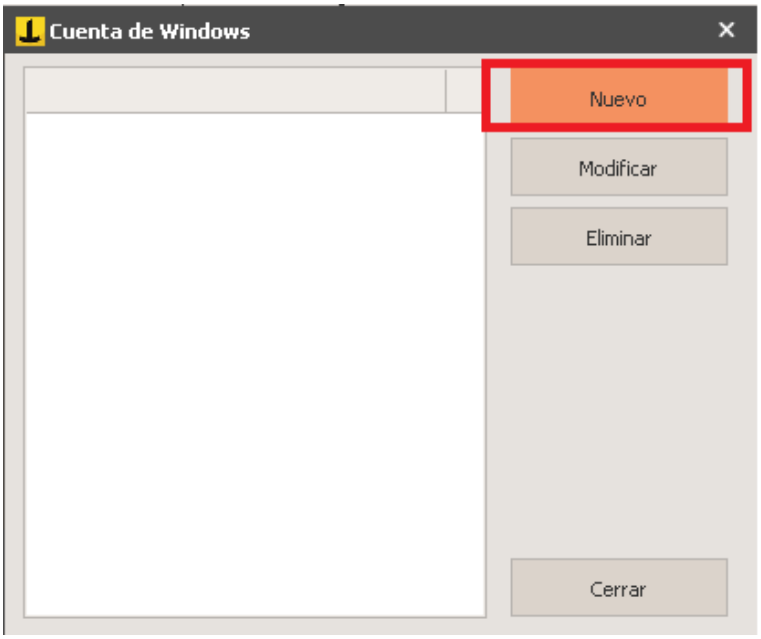

Imagen Núm. 17. Crear cuenta de Windows.

f. Al entrar a la ventana “Añadir nueva cuenta de Windows” se deberá ingresar el nombre de cómo se desea llamar a las credenciales en caso de contar con varias tareas; este método es práctico para poder tener control sobre los equipos.
g. Ingresar el nombre de usuario con el cual podemos acceder a nuestra **NAS;** y verificar en el equipo cómo se tiene el nombre de usuario.
h. En la opción “Establecer contraseña” se deberá ingresar la contraseña con la cual se puede acceder a la NAS.

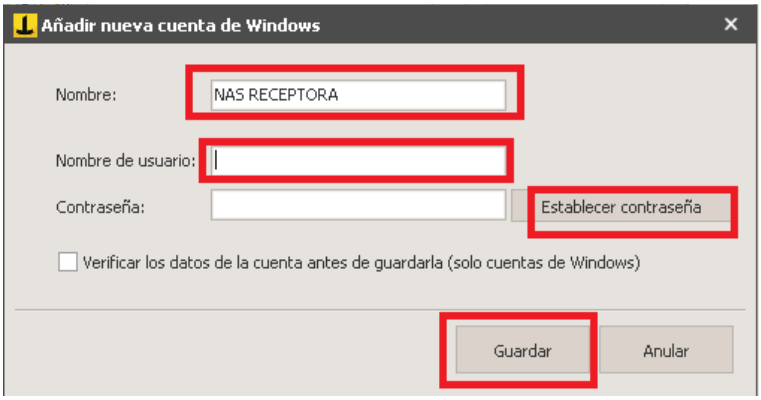

Imagen Núm. 18. Nombre de la tarea, nombre de usuario y contraseña.

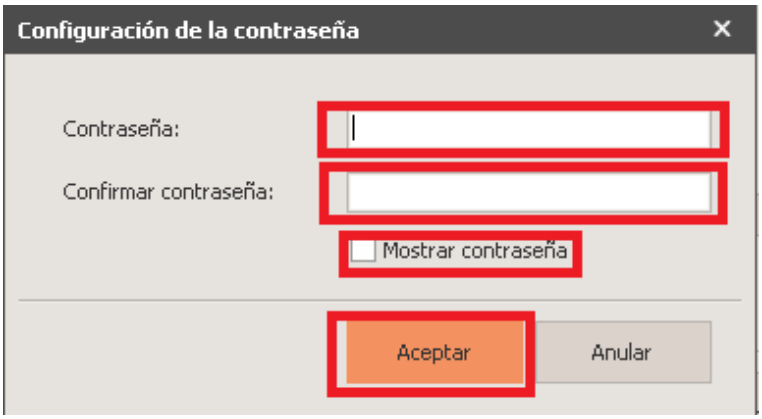

Imagen Núm. 19. Configuración de la contraseña.

4. Seleccionar la opción “Copiar la carpeta que contiene la imagen en los destinos de la tarea de copia de seguridad”.
5. Dar clic en “Aceptar”.

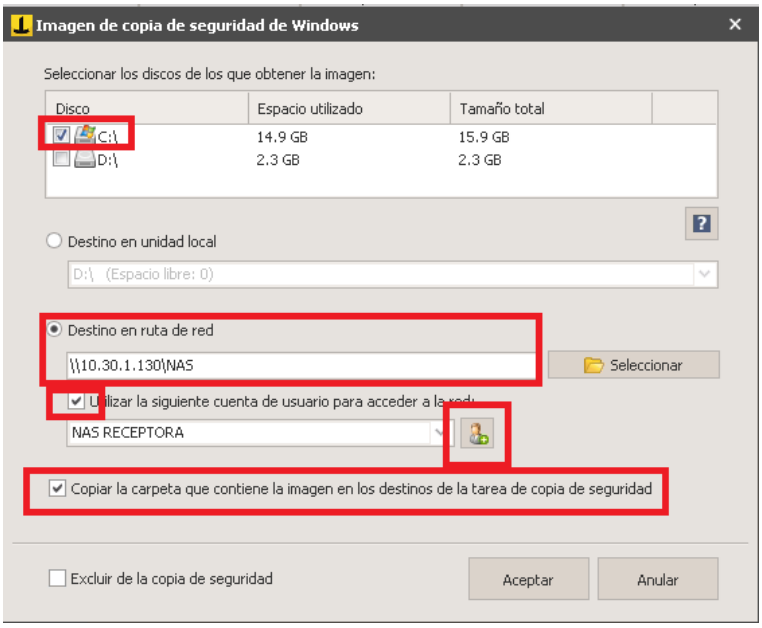

Imagen Núm. 20. Configuración de la copia de seguridad.

6. Las opciones “Destinos” y “Planificación” se usan cuando se tiene un destino alterno donde se puede guardar una copia de seguridad extra; en tanto que la opción de planificación sirve para automatizar las tareas, como por ejemplo, los días de la semana o incluso las horas en que se ejecutarán las copias, esto ayuda en gran medida, ya que en el caso de nuestro cliente las tareas se efectúan cada martes y jueves de manera local a partir de la 01:00 hrs. y los días sábados vía red hacia otras instalaciones ubicadas en Av. Tlalpan y a sus oficinas en la Alcaldía Iztapalapa.

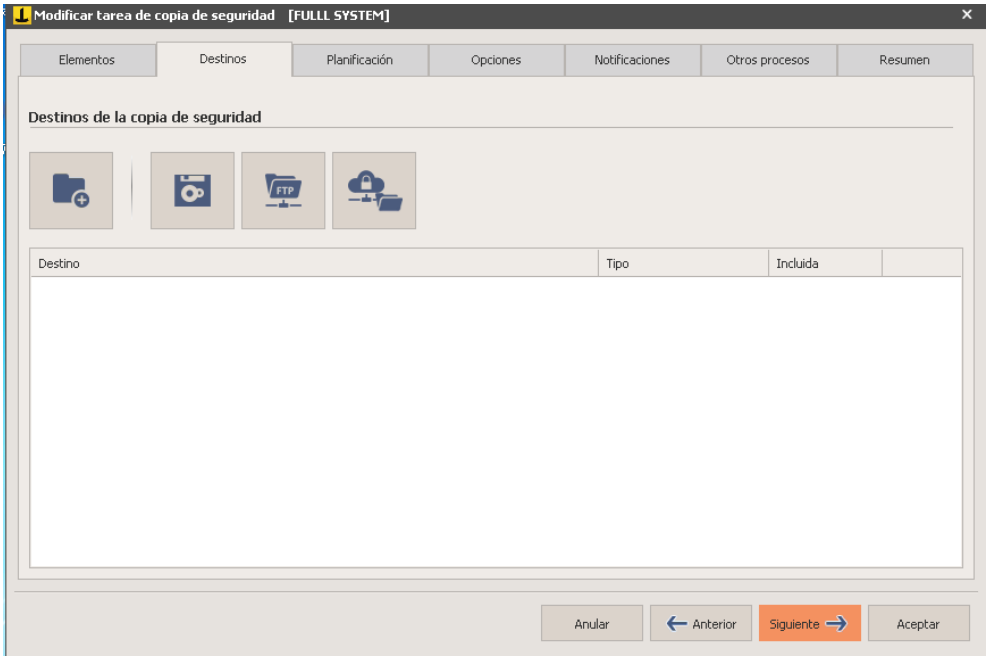

Imagen Núm. 21. Opción “Destino” si se desea crear un destino adicional.

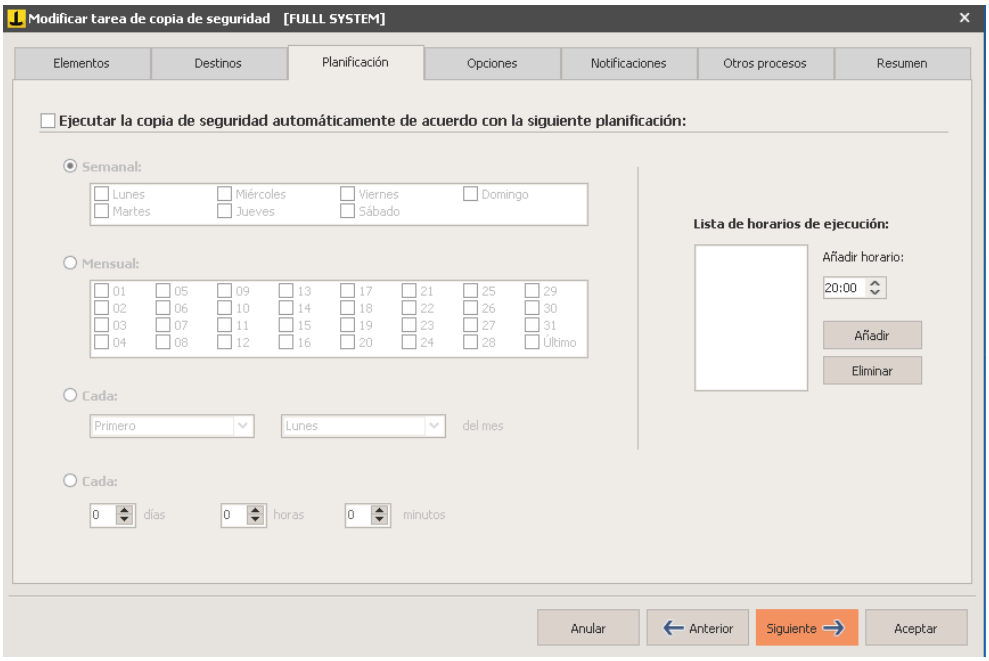

Imagen Núm. 22. La opción "Planificación" automatiza la ejecución de las tareas.

7. En la pestaña "Opciones" se deberá configurar como está en la siguiente imagen.

Imagen Núm. 23. Pestaña "Opciones".

8. Las opciones “Notificaciones” y “Otros Procesos” no se configuran, así que se recomienda pasar a la siguiente pestaña.
9. En esta pestaña se muestra cómo está configurada la tarea para buenas prácticas; al respecto, recomiendo que se le asigne un nombre específico para que sea fácil recordar qué es lo que hace esa tarea en caso de tener varias tareas configuradas.

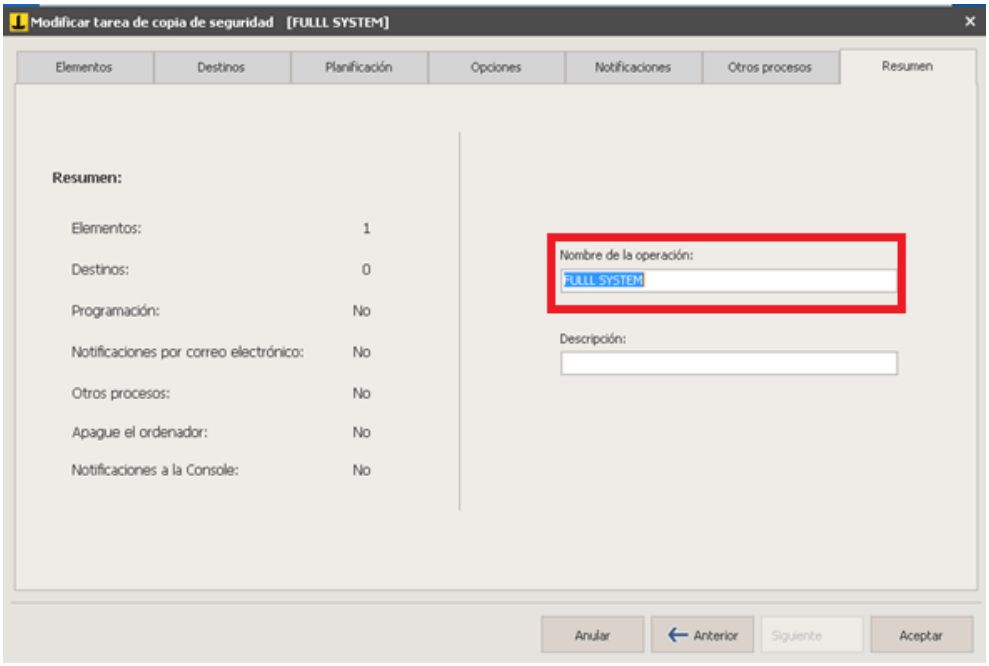

Imagen Núm. 24. Resumen.

10. Al dar clic en la opción “Aceptar” se finaliza la configuración de las tareas y a continuación éstas se deben ejecutar.

II.2.2. Ejecución de la Tarea “FULL Windows Image”

Al terminar la configuración de las tareas FULL Windows Image en Iperius, la siguiente actividad es ejecutar dichas tareas.

Lo que se tiene que hacer es dar clic derecho sobre el icono de la tarea configurado anteriormente y después en “Ejecutar la copia de seguridad”, tal como se muestra en la siguiente figura.

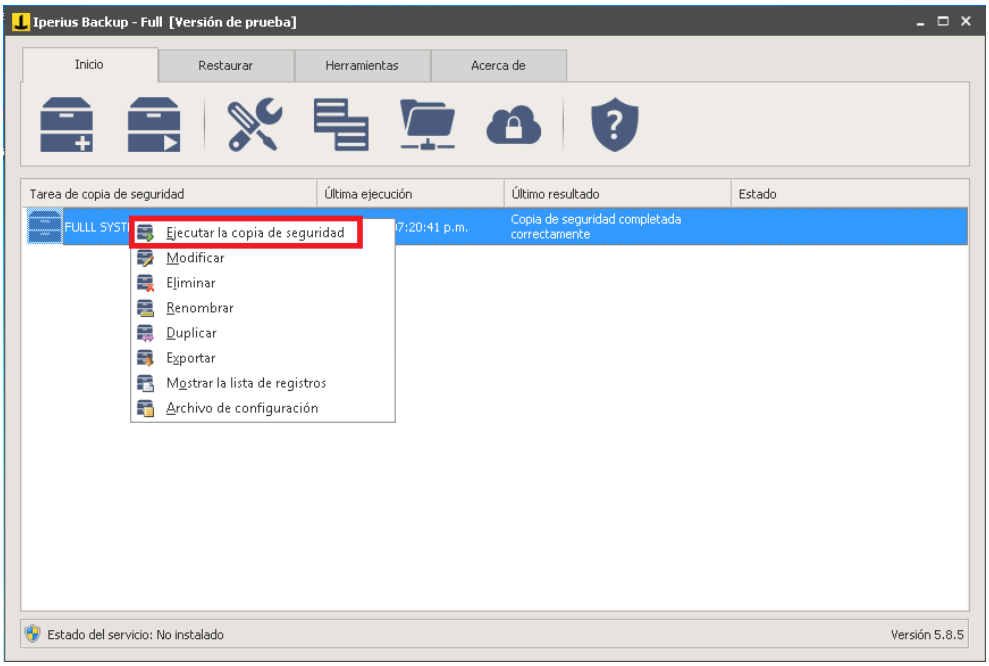

Imagen Núm. 25. Ejecución de tarea programada en Iperius.

En seguida aparecerá otra ventana, donde mostrará los procesos en los cuales se efectuará la copia de seguridad, tal como se aprecia en la siguiente imagen.

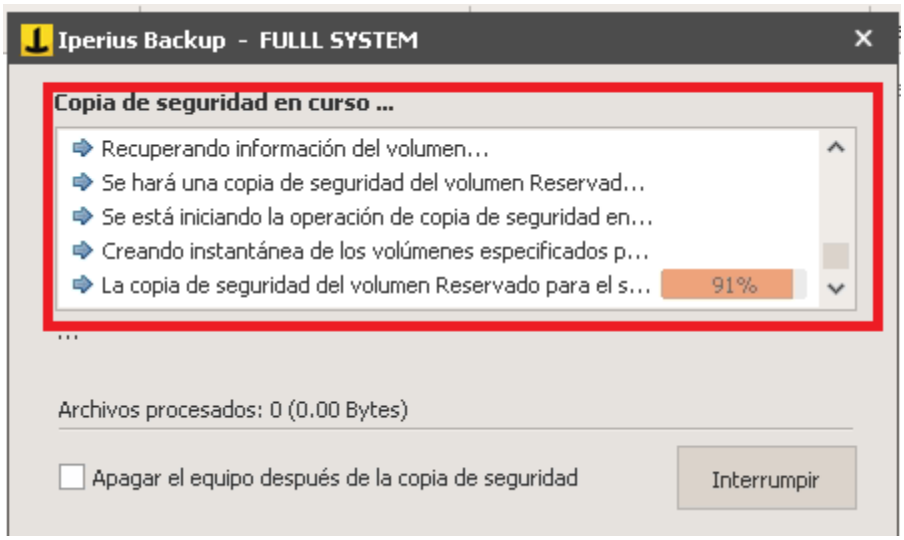

Imagen Núm. 26. Copia de seguridad "Full".

Al finalizar la copia de seguridad mandará el mensaje "Copia de seguridad completada correctamente"; de igual manera, el número de archivos procesados y el peso de la información almacenada, como se muestra en la siguiente imagen.

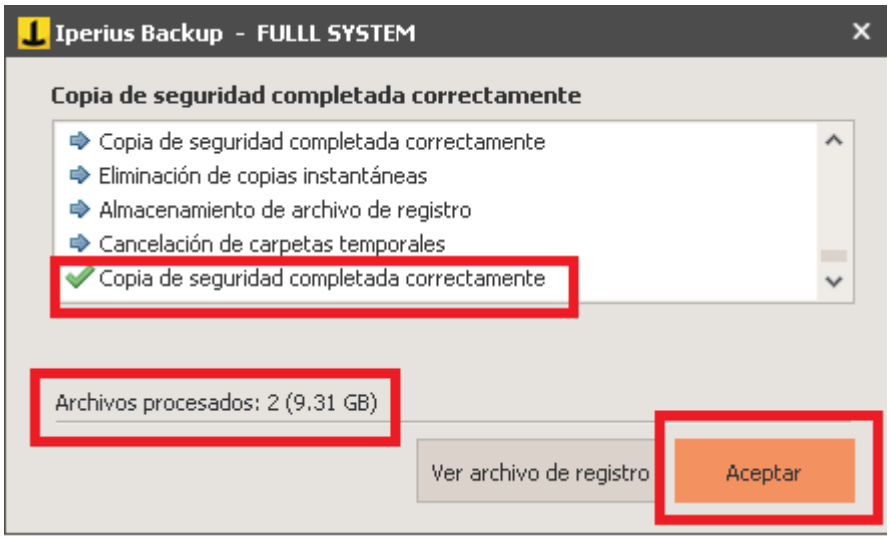

Imagen Núm. 27. Fin de la copia de seguridad "Full".

Para verificar que la copia de seguridad fue realizada de manera correcta, recomiendo que se acceda a la NAS de destino y se ubique la carpeta que contiene las copias de seguridad; en este caso, para el presente documento se creó la carpeta en la ubicación **"C:\NAS",** como se muestra en la siguiente imagen.

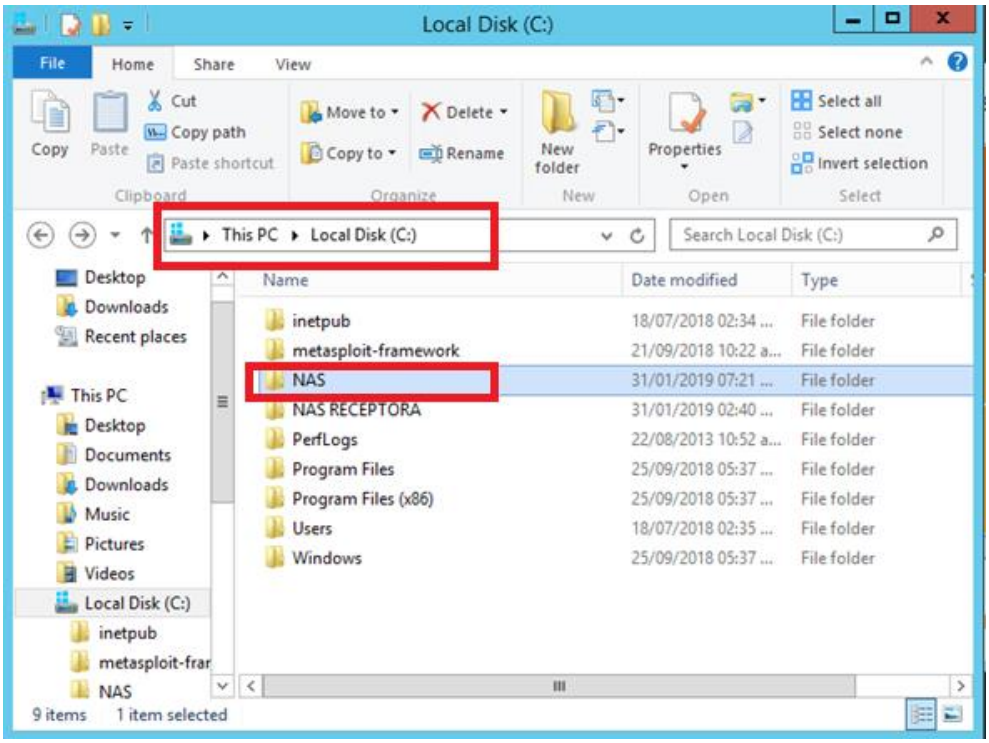

Imagen Núm. 28. Comprobando el backup realizado.

Dé clic en la carpeta **NAS** (esto con la finalidad de explorar el contenido de las carpetas) y a continuación doble clic en la carpeta **"WindowsImageBackup",** como se muestra a continuación.

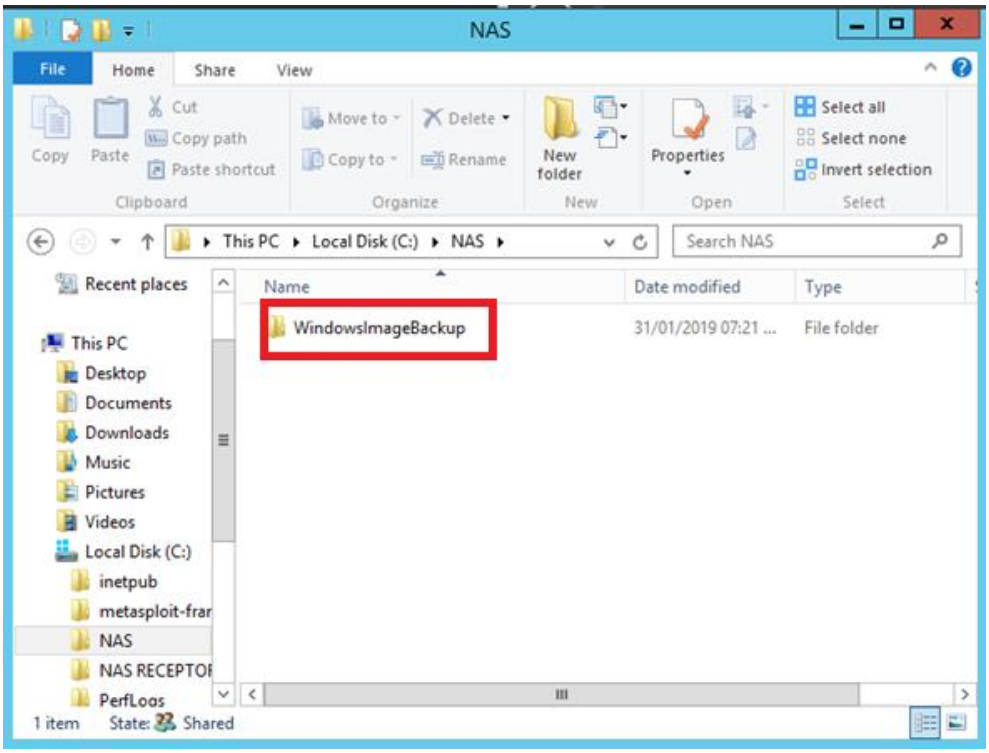

Imagen Núm. 29. Comprobando el backup realizado.

En este punto se muestra el nombre del equipo al que se le hizo una copia de seguridad. Dé clic para abrir la carpeta.

Imagen Núm. 30. Comprobando el backup realizado.

Al realizar esta tarea llegaremos a la ventana que muestra una carpeta con la copia de seguridad indicada con su fecha de creación y la demás información que Iperius colocó en ella; y para poder explorar los discos se deberá dar clic en la carpeta “Backup 2019…”.

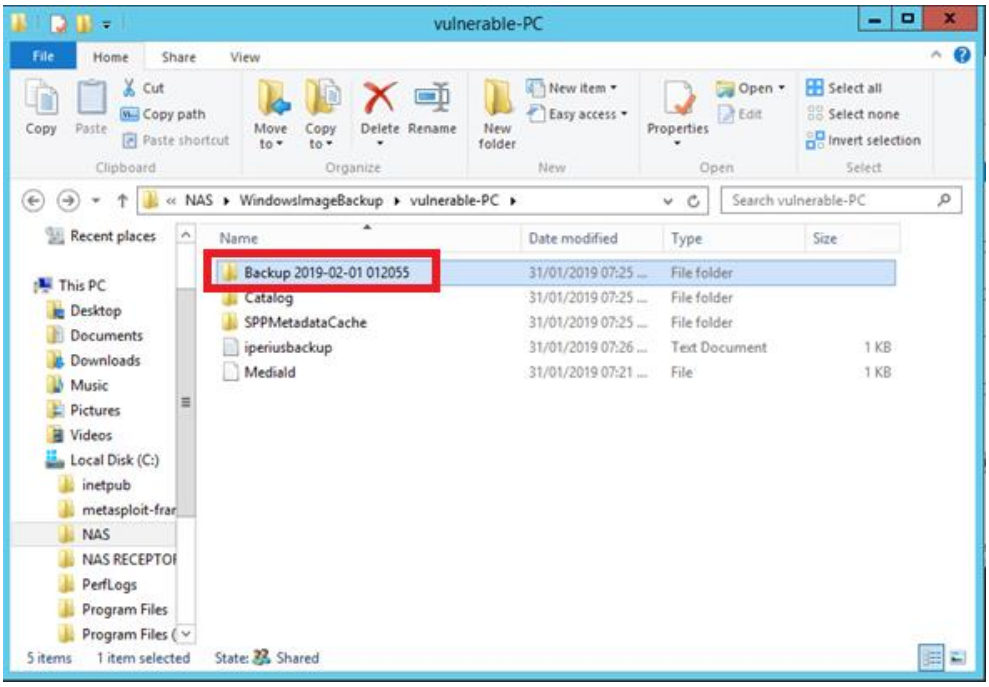

Imagen Núm. 31. Comprobando el backup realizado.

Aparecerá una ventana como la que se muestra en la **imagen núm. 32**, en donde los dos primeros iconos corresponden a una imagen virtual del disco duro; para explorarlo, se deben dar dos clics en el ícono del disco que muestre mayor cantidad de atributos.

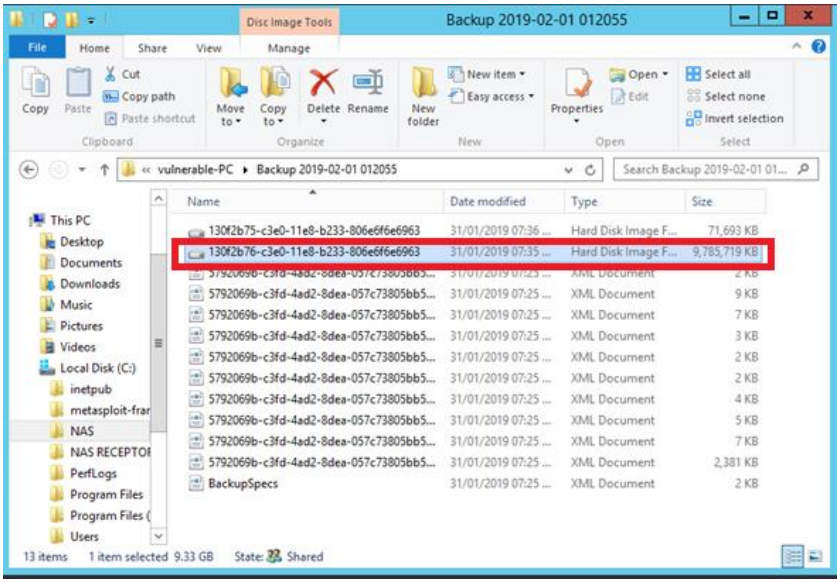

Imagen Núm. 32. Explorando el disco duro.

Para este ejemplo visualizaremos los archivos que se encontraban en el escritorio; para ello se puede consultar la **imagen núm. 13** y se deberá acceder a las siguientes carpetas:

a. Users
b. vulnerable (nombre del equipo)
c. Desktop o Escritorio (dependiendo cómo sea mostrado al momento de explorar discos)
d. Al final estaremos situados en el escritorio del disco virtual, donde podremos comprobar que están los archivos como en la imagen núm. 13.

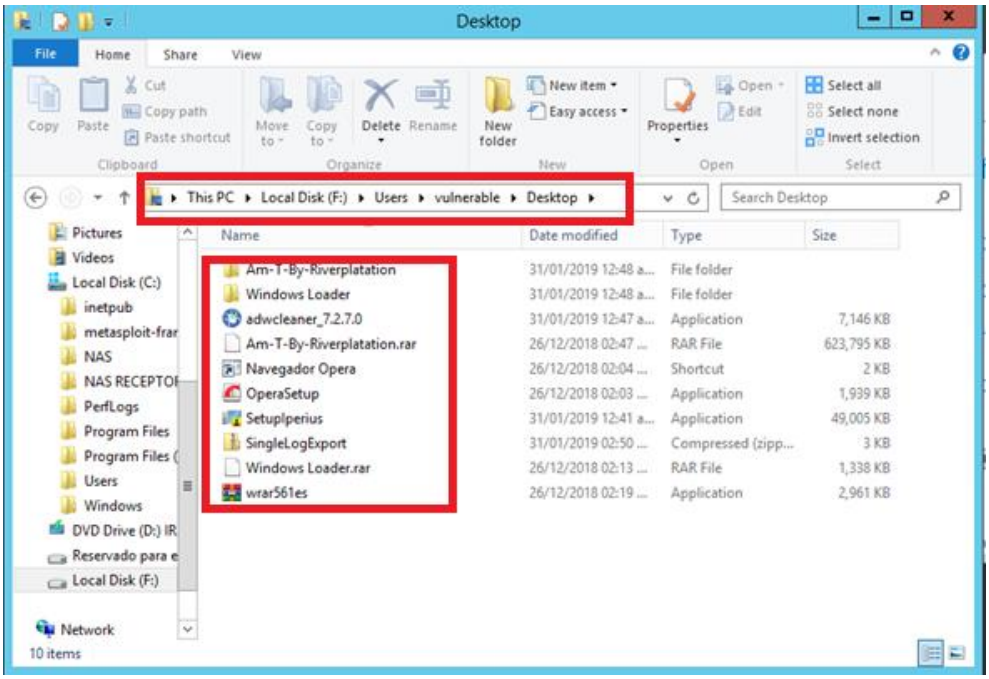

Imagen Núm. 33. Archivos respaldados.

II.3. Respaldo de un File Server

Un *file server* es un equipo que permite guardar archivos provenientes de otros equipos conectados en la red.

En el proyecto que se tiene con el cliente la tarea principal consiste en realizar copias de seguridad de los ***file servers***; dichos equipos contienen información importante, por ejemplo, registros especiales, como asistencias del personal a las instalaciones, proveedores, etcétera.

El primer inconveniente que se me presentó fue tener equipos **NAS** que soportaran dicha cantidad de almacenamiento, esto al tratarse de grandes volúmenes de información, la cual se respaldaría.

Después de valorar qué equipo sería necesario para realizar los respaldos; y una vez que los inicié, determiné el tiempo que podría demorarse copiar el 100% de la información.

El tiempo que tardaron los dos servidores que debían respaldarse fue como sigue:

- **File Server Núm. 1: 17 días, con una capacidad de 12 TB.**
- **File Server Núm. 2: 7 días, con una capacidad de 5 TB.**

En esta tarea configuré una opción adicional para que el cliente logrará tener los respaldos actualizados, ya que en su "File Server Origen" se detectó que es constante el cambio en los archivos.

A este tipo de respaldos se les denomina respaldos incrementales.

Como hice mención en la **pág. núm. 11** , "un respaldo incremental necesita de un respaldo completo como base y cada que se ejecuta una tarea de respaldo solo agregará la información nueva con que se cuenta".

Ahora se realizará la demostración del respaldo de un ***file server***.

Para el ejemplo utilizaremos el ***file server*** nombrado como **"Prueba File Server",** situado en el escritorio de nuestro servidor, como se muestra en la siguiente imagen.

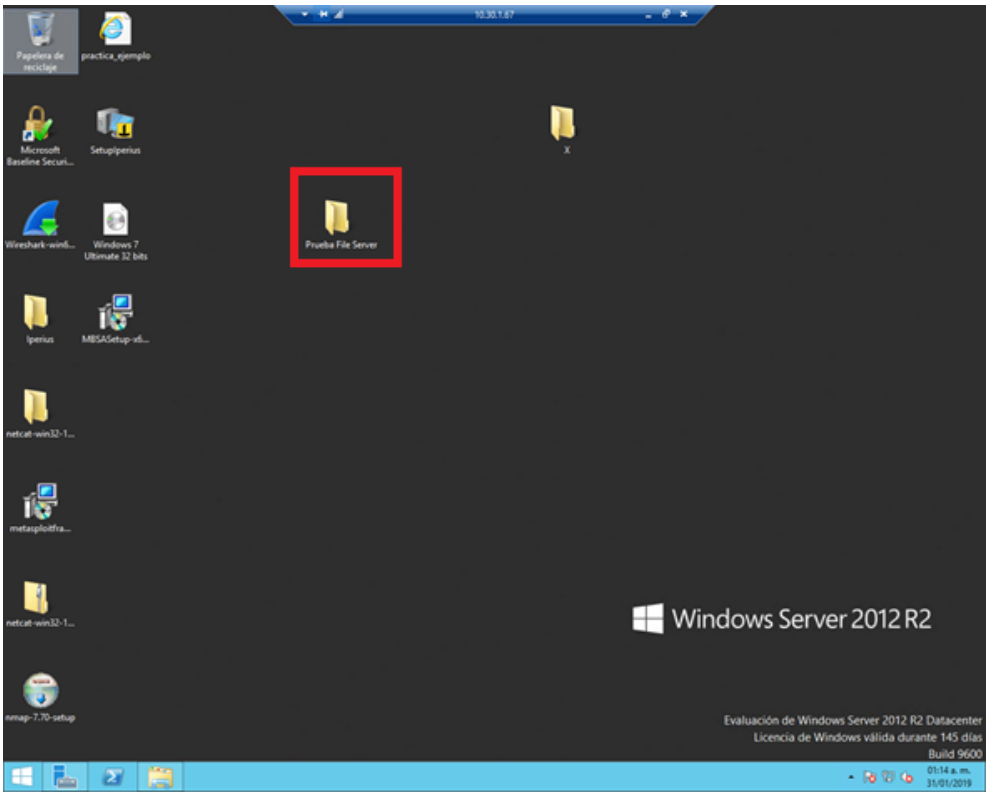

Imagen Núm. 34. Respaldo de un *file server*.

Dentro de la carpeta **"Prueba File Server"** se encuentra un **"subdirectorio de carpetas"** ejemplificando alguno de los dos ***file servers*** (servidores de archivos) que el cliente tiene almacenados en sus servidores.

En pocas palabras, se tienen carpetas almacenadas dentro de otras carpetas.

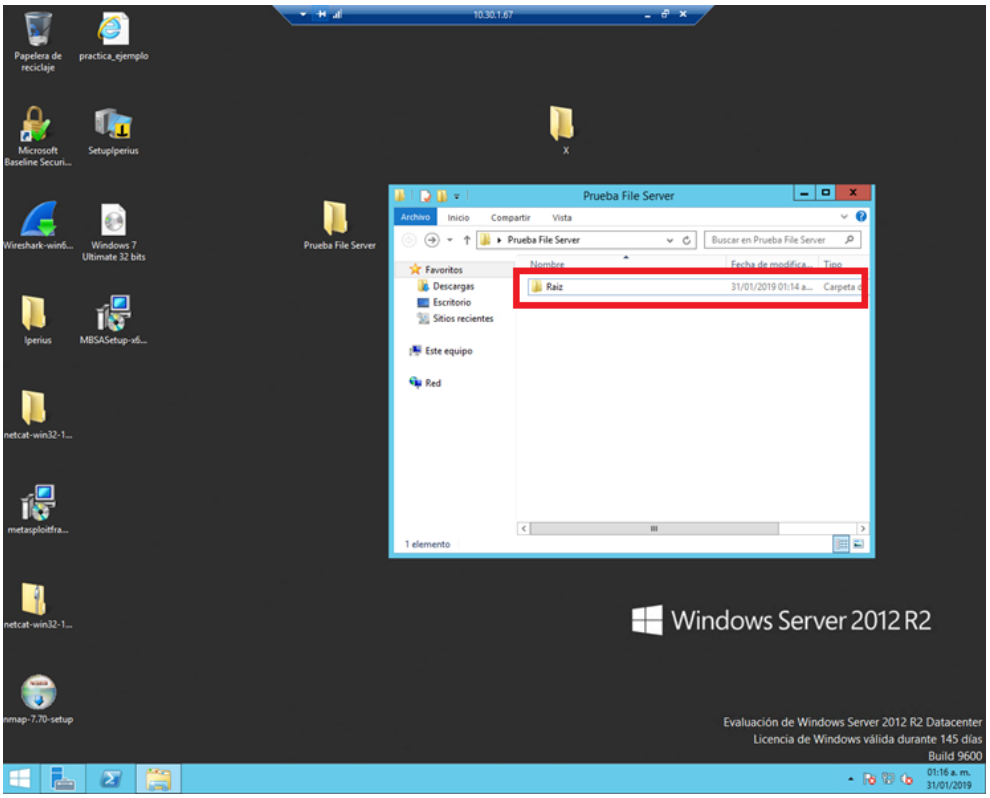

Imagen Núm. 35. Carpeta raíz donde se encuentran las demás carpetas con información similar a la estructura de un *file server* con la que cuenta el cliente.

II.4. Configuración de un *File Server* con Copias Incrementales

La configuración de las tareas para respaldar un ***file server*** son las siguientes una vez abierto el software Iperius:

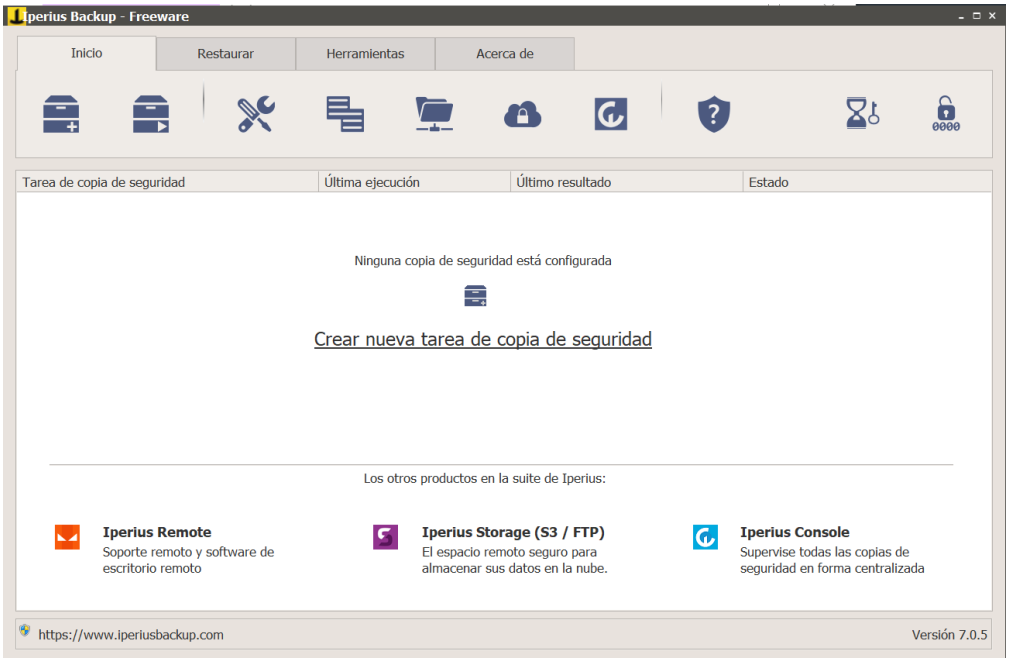

Imagen Núm. 36. Pantalla Inicial deIperius Backup.

1. Dé clic en la opción **“Nueva tarea de copia de seguridad”**, como se muestra en la siguiente imagen.

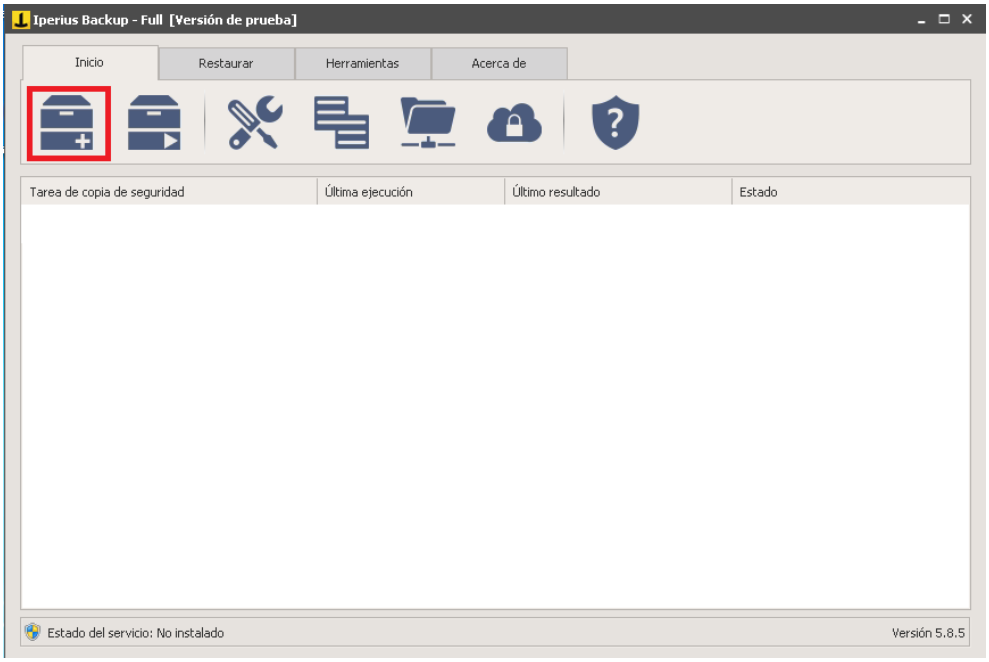

Imagen Núm. 37. Configuración inicial del *file server.*

2. En la pestaña **Elementos** dar click en la opcion **Añadir Carpeta**.

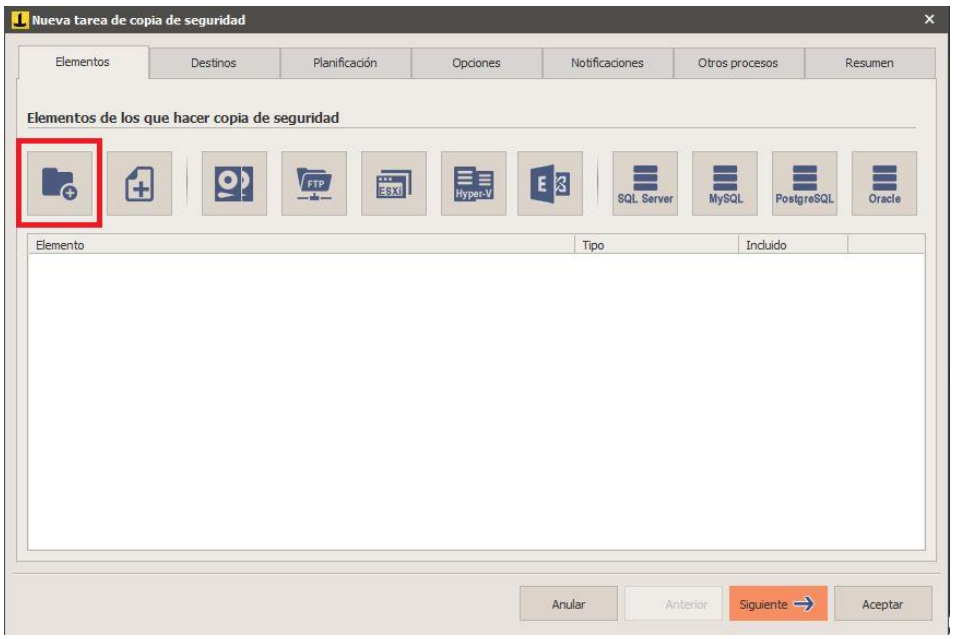

Imagen Núm. 38. Configuración inicial del *file server.*

3. Una vez elegida, se abrirá la siguiente imagen, por lo que debe configurar la ubicación del ***file server*** dando clic en la opción **"Seleccionar".**

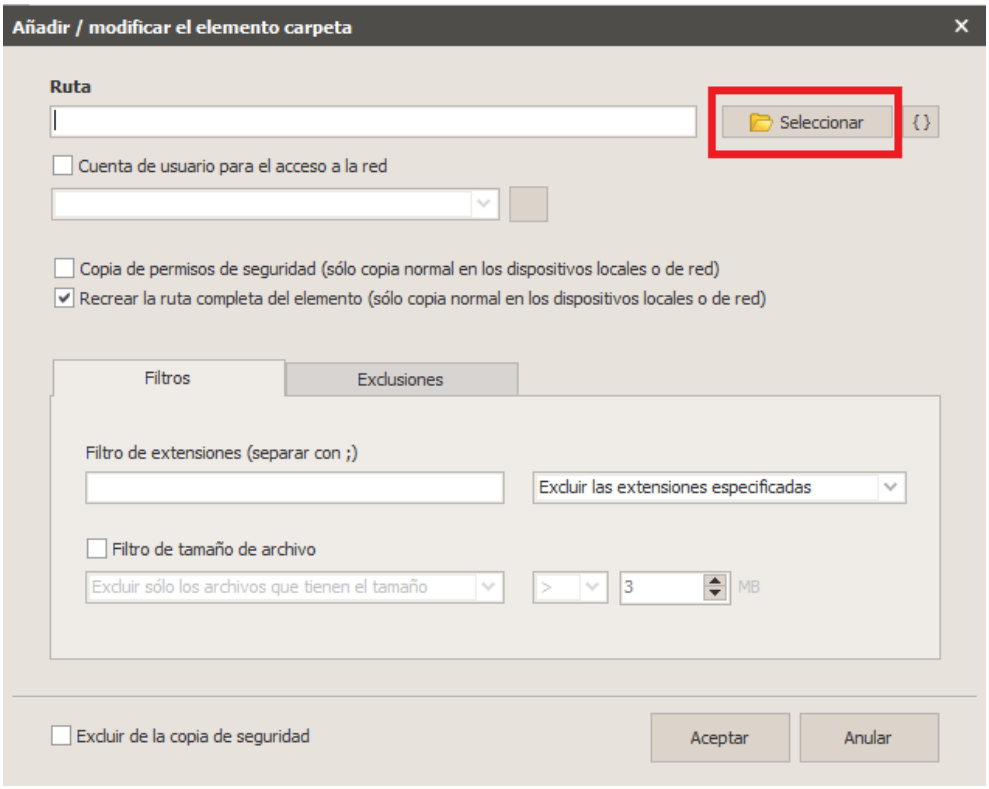

Imagen Núm. 39. Configuración inicial del *file server.*

4. En este caso, el ***file server*** se encuentra en el escritorio; conviene recordar que el nombre de la carpeta es **"Prueba File Server"**; y una vez seleccionada la carpeta, el siguiente paso es dar clic en **"Aceptar".**

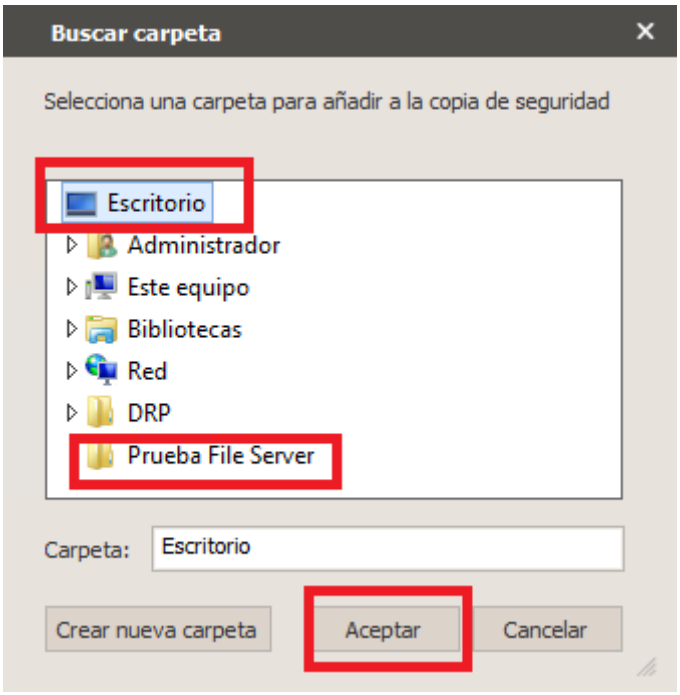

Imagen Núm. 40. Configuración inicial del *file server.*

5. Al dar clic, la ventana regresará a la imagen que aparece abajo; el siguiente paso consistirá en seleccionar tal cual las dos opciones que se muestran en dicha imagen; y nuevamente hay que dar clic en **“Aceptar”**.

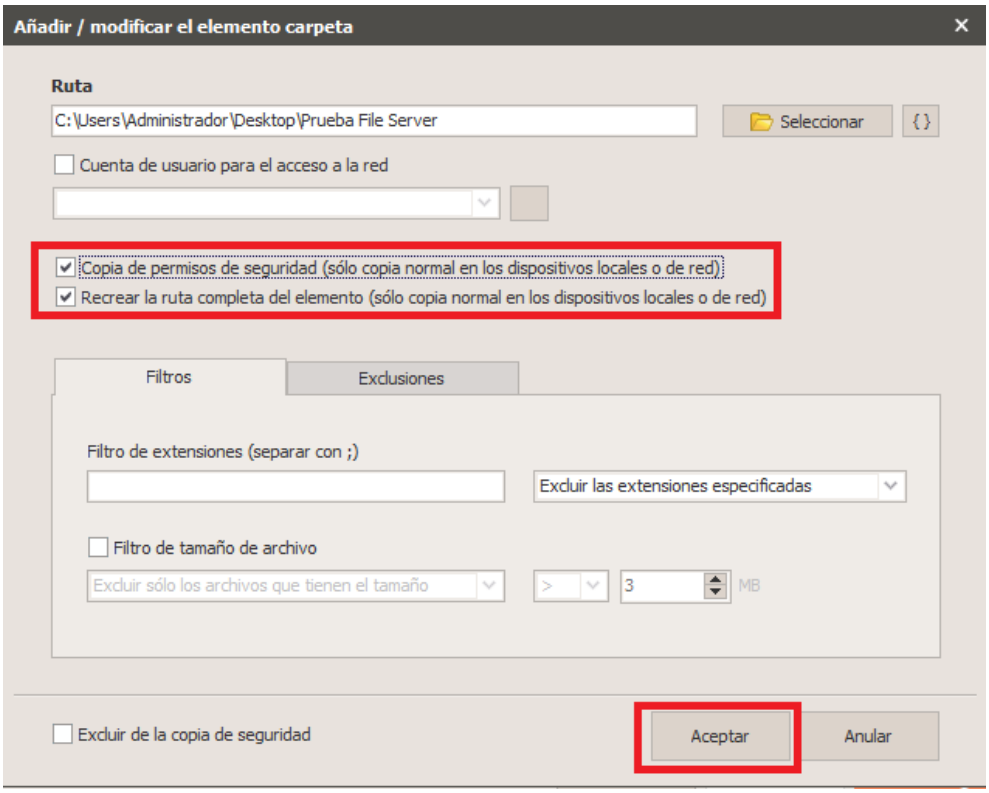

Imagen Núm. 41. Configuración inicial del *file server.*

6. Una vez configurado el ***file server,*** aparecerá esta ventana y a continuación hay que dar clic en la opción **“Siguiente”.**

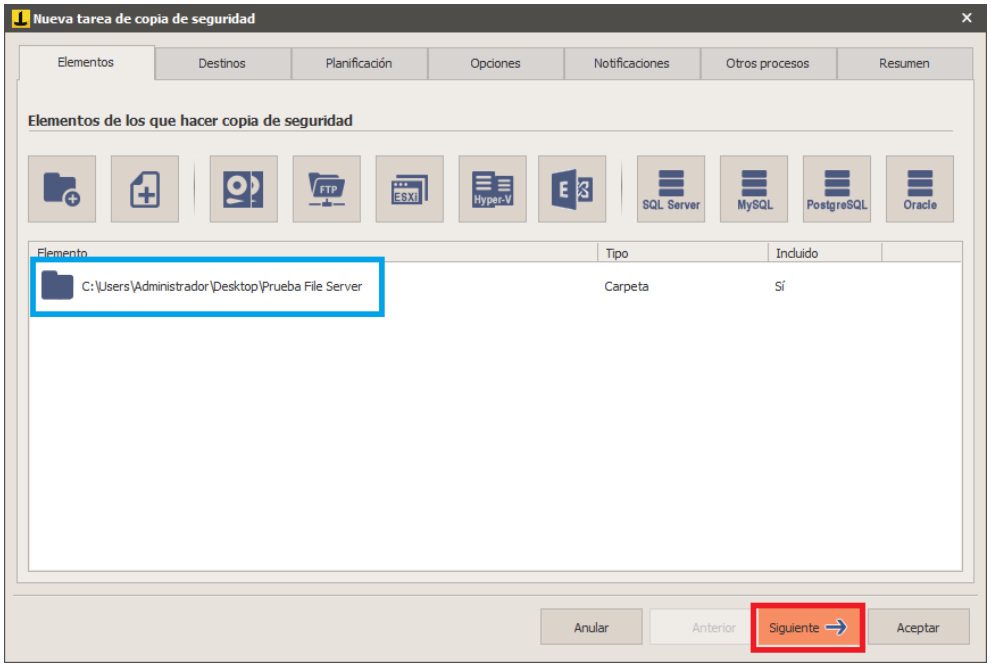

Imagen Núm. 42. Configuración inicial del *file server.*

7. En la pestaña denominada **“Destinos”** se deberá configurar la ruta, junto con las credenciales, donde se encuentre la **NAS** o la carpeta que usaremos para almacenar nuestro respaldo.

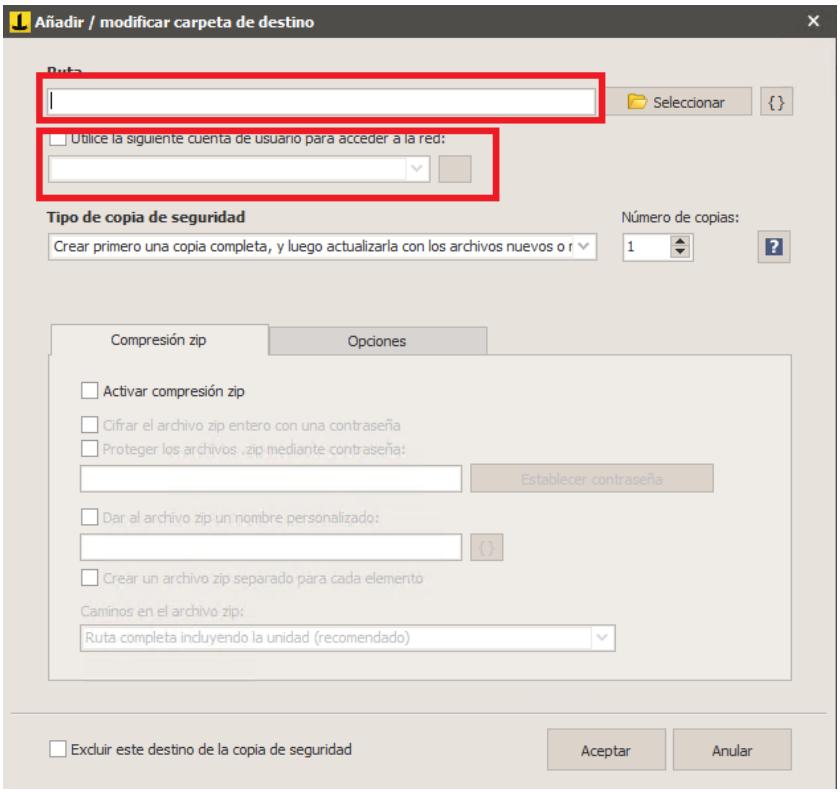

Imagen Núm. 43. Configuración inicial del *file server.*

8. Para crear una cuenta con la cual se ingresará al ***file server*** y con objeto de realizar la copia de seguridad sin ninguna restricción, se debe dar clic en la opción **“Nuevo”.**

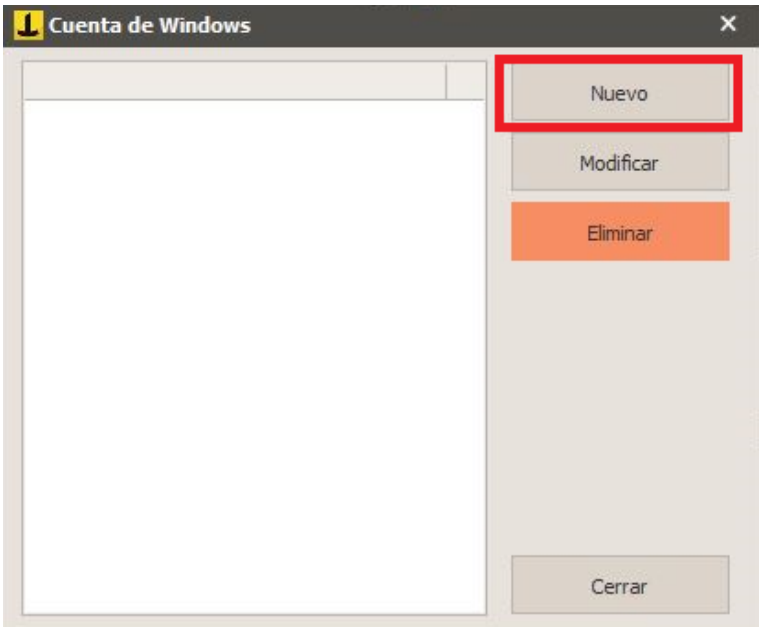

Imagen Núm. 44. Configuración inicial del *file server.*

9. Al dar clic, aparecerá la ventana que se muestra a continuación y en ella se anotarán los siguientes datos:

    - **Nombre,** en el cual podremos identificar las credenciales en caso de tener varias conexiones configuradas.

    - **Nombre de usuario** con el que se accede al servidor; en este ejemplo el nombre de usuario será **"Administrador".**

    - **Establecer contraseña,** se trata en este apartado de la contraseña que nos permite iniciar sesión en nuestro servidor.

    Al terminar de llenar los campos anteriores con la información solicitada se deberá dar clic en la opción **"Guardar".**

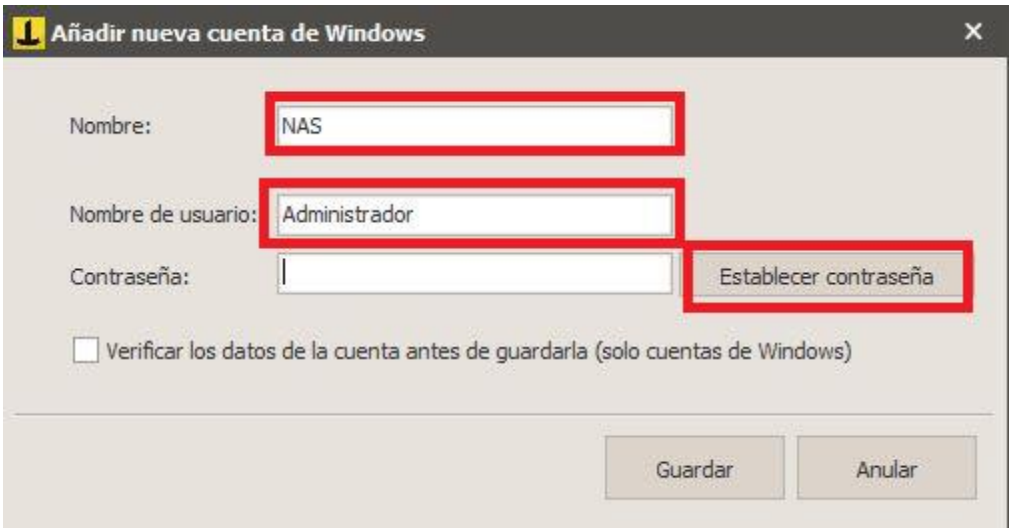

Imagen Núm. 45. Configuración inicial del *file server.*

10. Una vez que ingresó toda la información requerida, aparecerá el icono de las credenciales listas para seleccionar y para comenzar a realizar respaldos.

    Posteriormente, dé clic en las opciones **"Cerrar"** y **"Siguiente",** en ese orden.

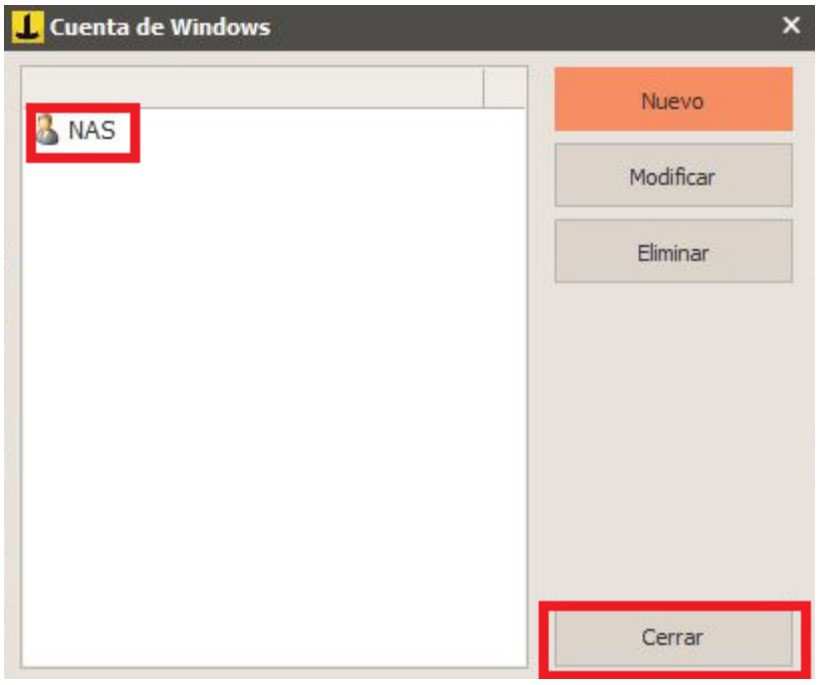

Imagen Núm. 46, Configuración inicial del *file server.*

11. En esta ventana se debe añadir la información sobre la NAS, como lo es la **"Ruta",** en la que se deberá colocar la dirección IP del equipo, seguida del nombre de la carpeta creada para almacenar los respaldos.

    Seleccionar la opción **"Utilice la siguiente cuenta de usuario para acceder a la red";** en este apartado se usarán las credenciales que se guardaron en el paso anterior.

    En la opción **"Tipo de copia de seguridad",** como recomendación se deberá seleccionar **"Mantener una copia de seguridad completa y varias copias incrementales";** y en seguida de esta selección se deberá configurar el número de copias que se desea realizar.

    Un punto muy importante es que este tipo de configuración es recomendada para tener un número determinado de copias de seguridad, con la finalidad de que, si en algún momento de la operación se necesita recuperar algún archivo, será posible hacerlo y continuar con la operación.

    Es recomendable configurar por lo menos dos (2) copias, esto con la finalidad de tener dos (2) respaldos a la semana.

    La lógica de la programación de un respaldo full + dos (2) copias incrementales es la siguiente:

    - **El respaldo full se realiza una (1) sola vez, ejemplificándolo el lunes.**
    - **A partir del día lunes las copias que se realicen serán incrementales (solamente lo nuevo que se agregó al servidor); en este caso se configura que el día miércoles y viernes, a las 00:00 hrs., se inicie una verificación automática (Iperius revisará en el respaldo full, evaluara qué información se agregó, dicha información será enviada para poder contar un respaldo actualizado del servidor).**

    Una vez establecidos los criterios de la configuración, como se muestra en la siguiente imagen se debe dar clic en la opción **"Aceptar"**

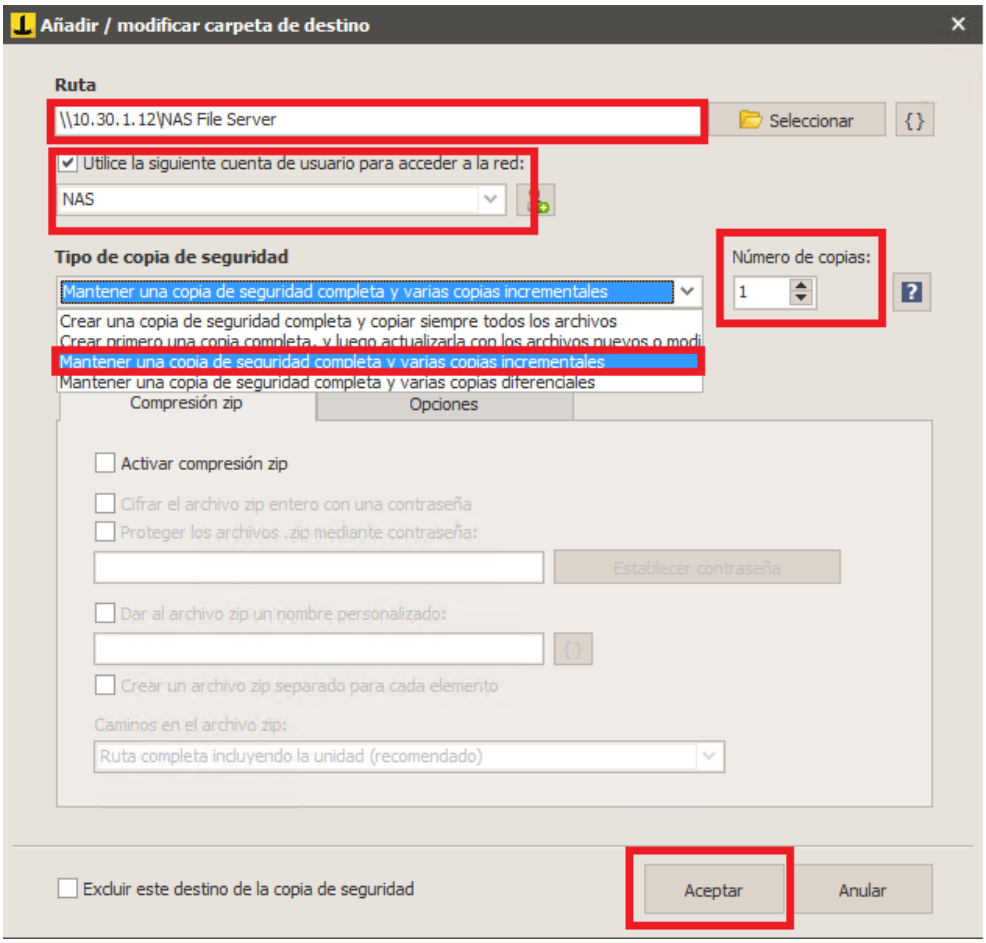

Imagen Núm.47. Configuración inicial del *file server*.

12. Ya registrado el destino, solo es necesario dar clic en la opción **“Siguiente”** para continuar con la configuración.

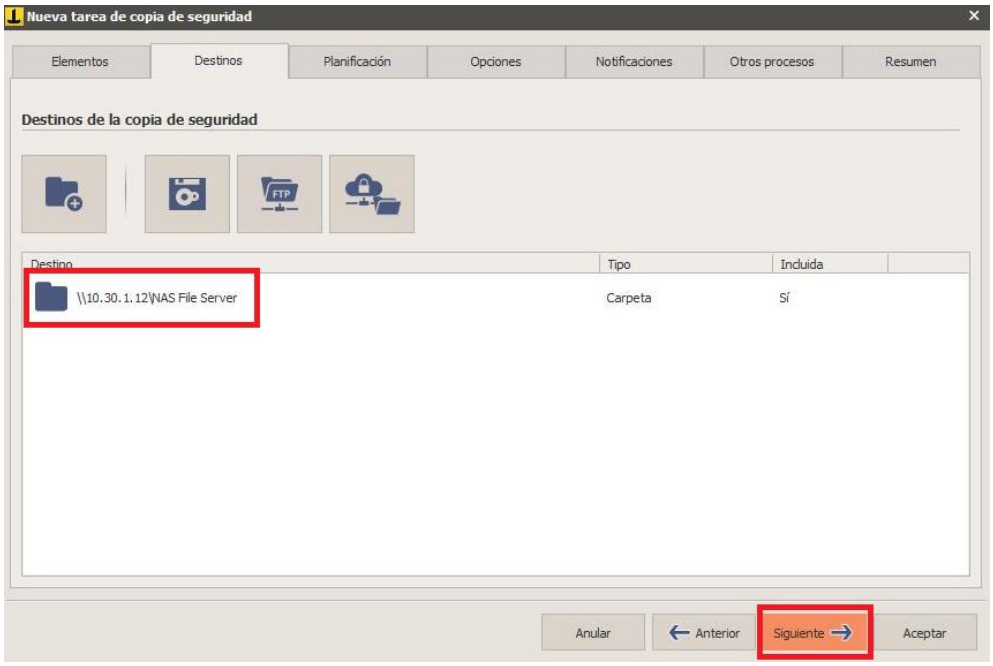

Imagen Núm.48. Configuración inicial del *file server*.

13. En la pestaña de “Planificación” sirve para automatizar las tareas, de manera que se pueden configurar tanto los días como las horas en que se necesite efectuar el respaldo, con lo cual se podrán optimizar tiempos y en caso del cliente facilitar sus actividades.

    Para automatizar esas tareas solo se debe dar clic en la opción **“Siguiente”.**

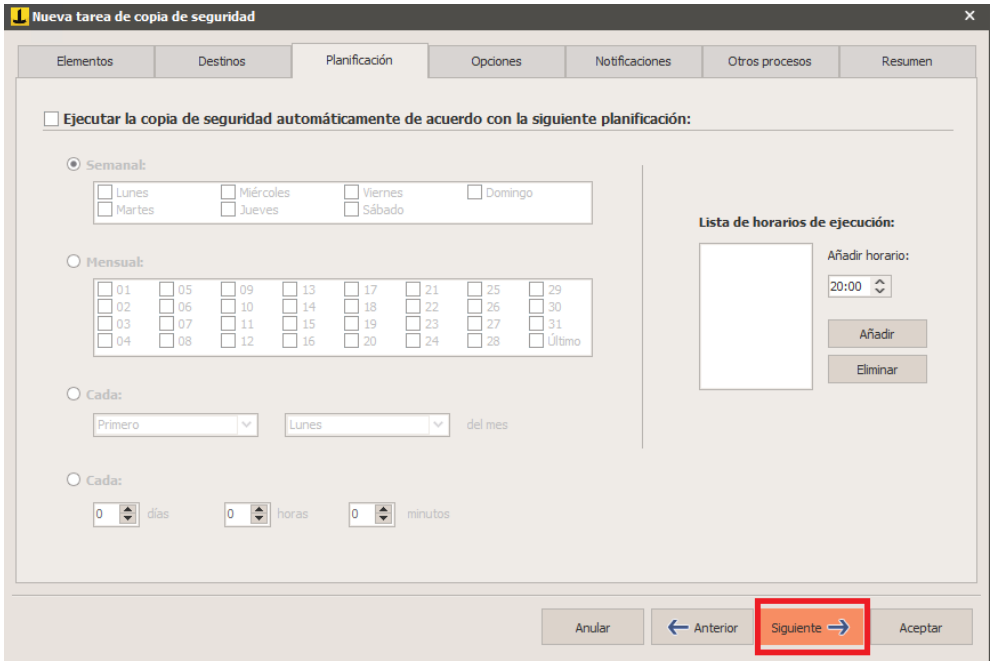

Imagen Núm.49. Configuración inicial del *file server.*

14. En la pestaña “Opciones” se recomienda configurar las tareas tal como aparecen en la siguiente imagen; y al finalizar da clic en la opción **“Siguiente”.**

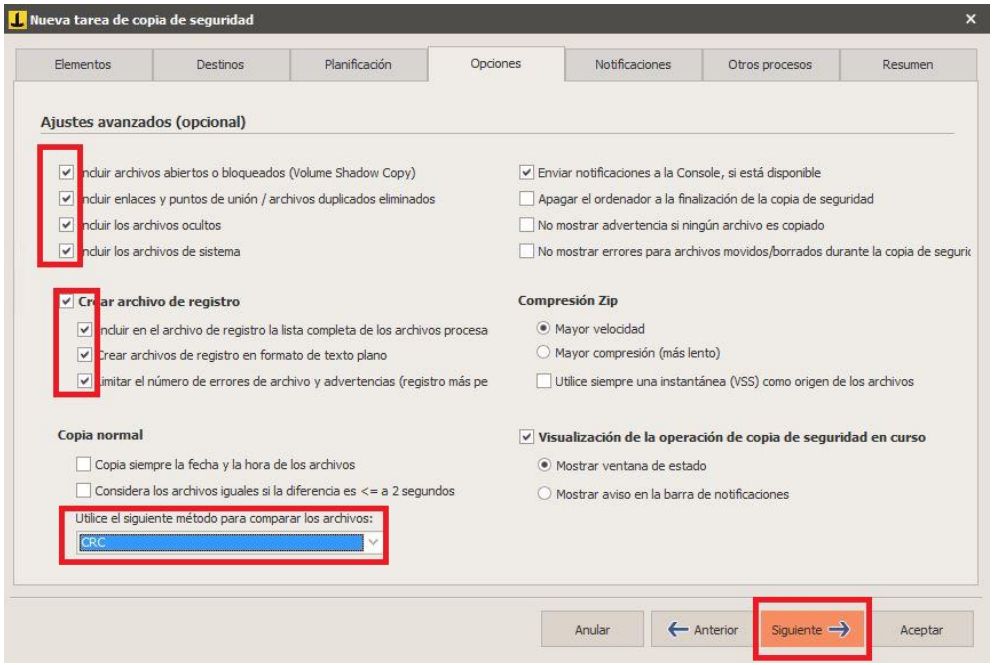

Imagen Núm. 50. Configuración inicial del *file server.*

15. La pestaña “Notificaciones” sirve para que el software Iperius mande automáticamente correos con la finalidad de informar el estatus de las tareas efectuadas, de las finalizadas con éxito y, a su vez, de las que terminan con errores.

    En este caso no se configuró nada, puesto que al cliente se le otorgó una licencia de **Iperius Console;** esta solución **“centraliza**” varias cuentas de Iperius instaladas en los servidores, muestra en tiempo real toda la información que se requiera e incluye la posibilidad de efectuar respaldos desde la consola si no han sido automatizados.

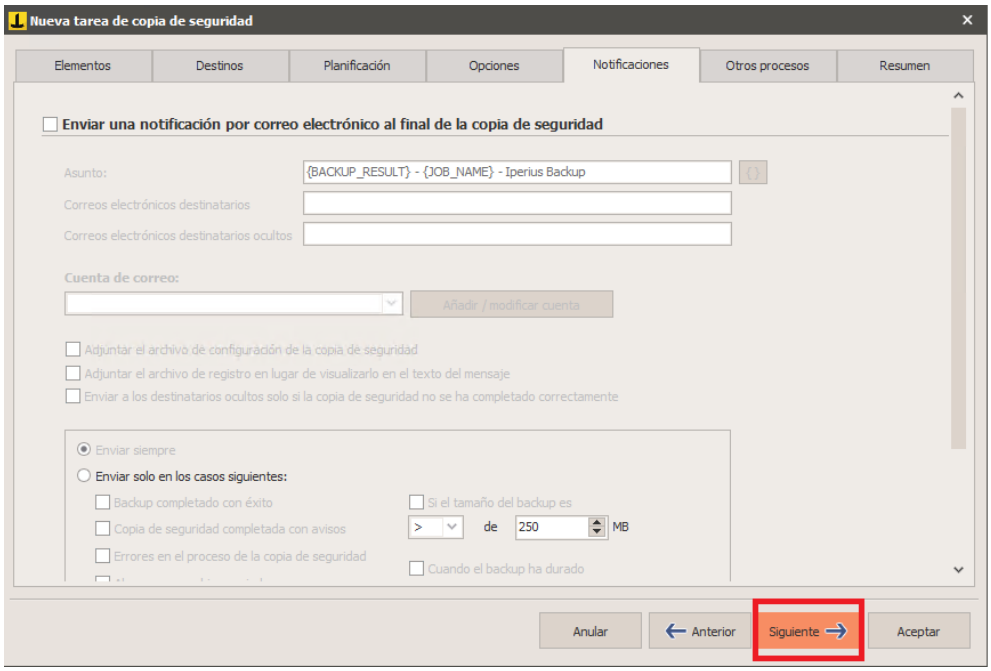

Imagen Núm.51. Configuración inicial del *file server.*

16. En la pestaña “Otros procesos” no se efectuará cambio alguno, por lo que se recomienda dar clic en la opción **“Siguiente”.**

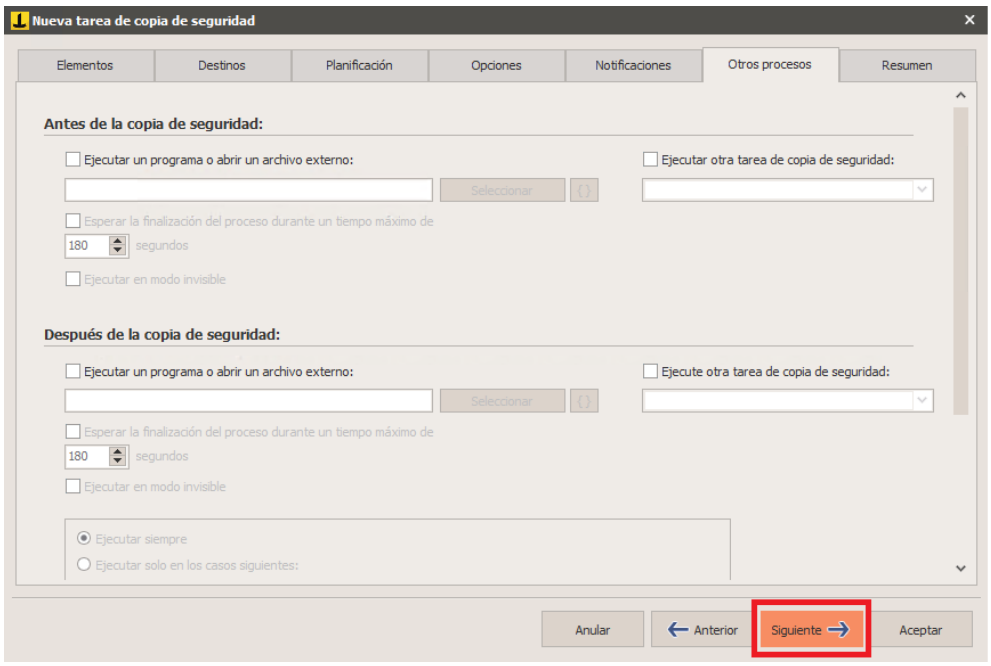

Imagen Núm. 52. Configuración inicial del *file server.*

17. En virtud de que la pestaña **“Resumen”** ofrece una breve sinopsis sobre la configuración efectuada, se recomienda asignarle un nombre a la tarea, ya que si se cuenta con diversas tareas en la aplicación será más fácil gestionarla; para este caso se le asignó el nombre de **“Prueba File Server”**. Como último paso de la configuración de las tareas en Iperius hay que dar clic en la opcion **“Aceptar”.**

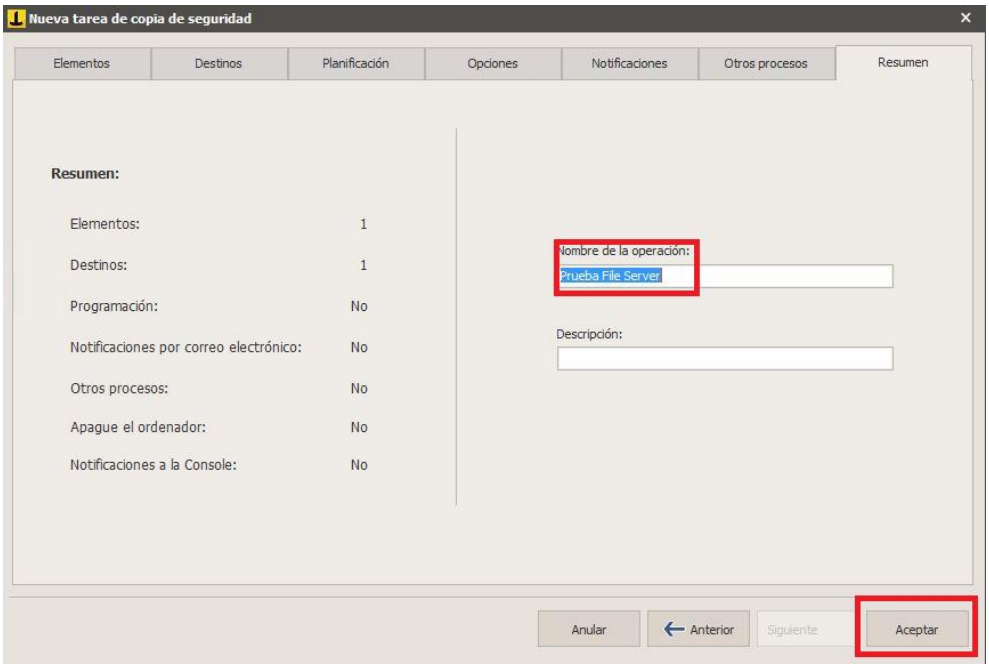

Imagen Núm.53. Configuración inicial del *file server.*

II.5. Ejecución de la Tarea para un *File Server*

Para comenzar la tarea recién configurada, en la pestaña “Inicio” se debe dar clic en la opción enmarcada en rojo en la siguiente imagen **“Ejecutar tarea”.**

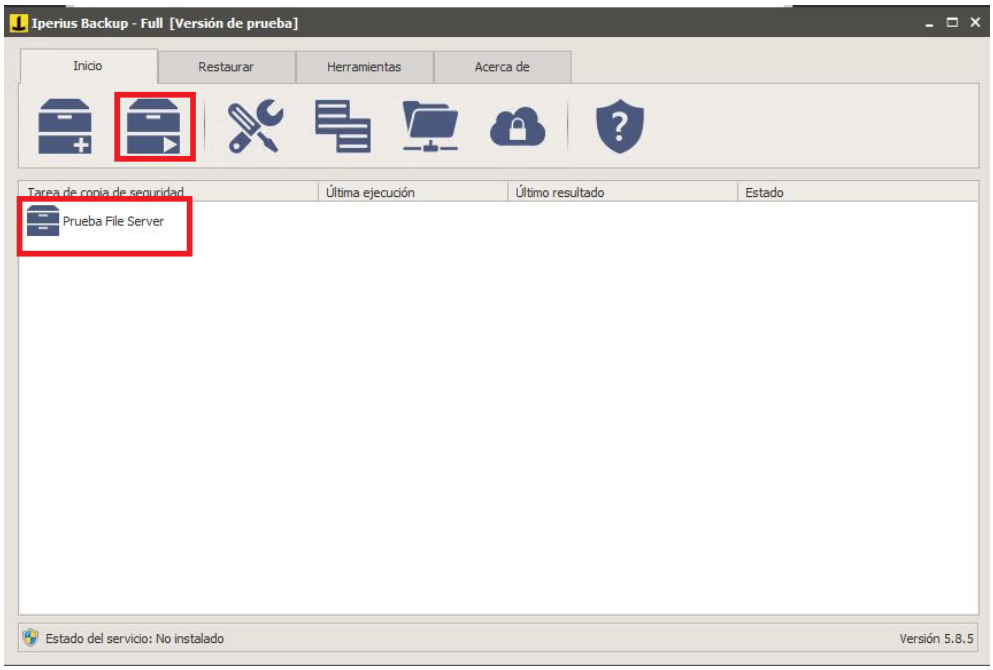

Imagen Núm. 54. Ejecución del backup *File Server.*

En seguida mostrará un aviso en el que solicitará la confirmación del usuario para poder ejecutar la tarea.

NOTA: Si las tareas fueron configuradas automáticamente, el software no pedirá dicha confirmación.

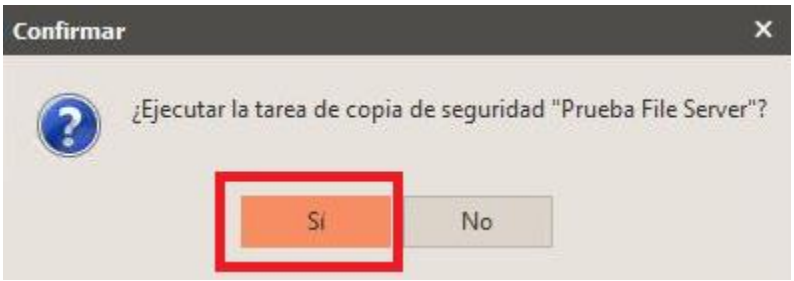

Imagen Núm. 55. Ejecución del backup *File Server.*

Si la configuración es correcta, el software realizará el respaldo correspondiente.

Cabe mencionar que, en el escenario del cliente, los respaldos se tardaron más de dos semanas solamente en finalizar el primer respaldo **“Respaldo Full”**; los siguientes respaldos variaron en su tiempo de ejecución.

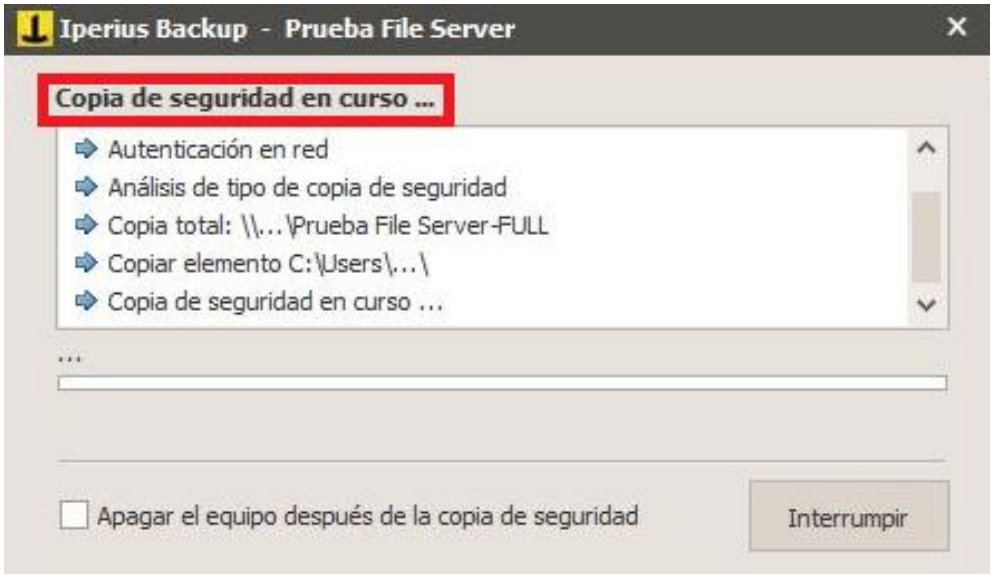

Imagen Núm. 56. Ejecución del backup *File Server.*

Al cabo del tiempo requerido y una vez finalizado el respaldo de la información, mostrará el mensaje que aparece en la **imagen núm. 58.**

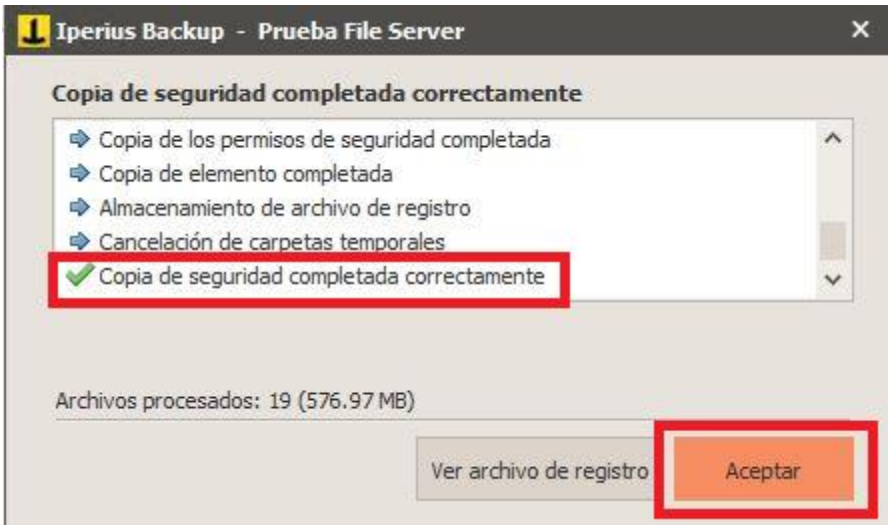

Imagen Núm. 57. Ejecución del backup *File Server.*

Esta imagen muestra los distintivos entre un respaldo Full y una respaldo incremental y con ella confirmo que el respaldo de la información fue correcto.

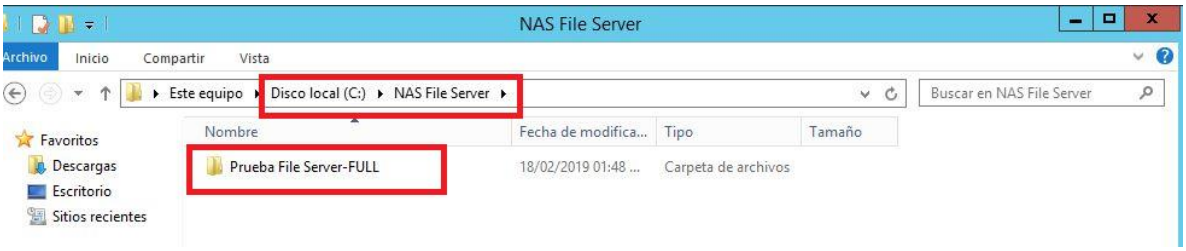

Imagen Núm. 58. Ejecución del backup *File Server.*

Capítulo III. Implementación de Iperius

¿Por qué usar Iperius?

Como se ha descrito en este documento de titulación, Iperius es una herramienta liviana enfocada al sistema Windows que ayuda a realizar de manera automática copias de seguridad.

Primeramente, llevé a cabo varias pruebas a diferentes software conforme a una lista que el cliente me proporcionó previamente de ciertas especificaciones, en las cuales me basé para tomar una decisión y cumplir con los requerimientos que se tenían.

Entre una de sus características analicé que fuera “liviana”, es decir, que no consumiera tantos recursos, como la memoria RAM o la velocidad de procesamiento de los servidores, ya que no era posible tener alguna falla en los sistemas y menos aun cuando estos sistemas son productivos (en el caso del *file server* está en operación las 24 horas y se tiene información en constante cambio).

La siguiente característica fue el tipo de licencia; en este caso, se compararon software como Veeam Backup, Cobian Backup e inclusive con el asistente de copias de seguridad que tiene la particularidad de configurarse dentro del mismo Windows Server (Windows Server 2012 R2, versión usada en el MDF del cliente).

Llegué a la conclusión de que Iperius era la mejor opción en costos, ya que, al adquirir la licencia de la versión que se requiera, ésta es de por vida, con actualizaciones gratis y soporte cuando sea necesario.

Imagen Núm. 59. Ediciones de Iperius Backup.

En comparación con los otros programas, la licencia de éstos se debe renovar cada año y sus costos pueden ser un poco más elevados que el de la licencia Iperius.

El siguiente requisito consistió en que realizará copias de seguridad de tipo “incremental”.

Como he expuesto en este documento, la copia de seguridad incremental necesita como primer punto una copia de tipo “Full” a fin de poder comparar desde el archivo origen la nueva información y los cambios efectuados en ella para enviarla a la copia de seguridad antes efectuada (se realiza una actualización de la copia full para poder tener la versión más reciente, sin duplicar la información).

Esto con el propósito de contar con la información más reciente; y en caso de que se presente pérdida de información o falla de algún sistema, se realice su recuperación y la puesta en marcha de sistemas lo antes posible para no afectar las operaciones que el cliente lleva a cabo.

Uno de los requisitos más importantes solicitado por el cliente fue que los equipos donde se almacenaría la información estarían cambiando constantemente de ubicación, lo que obligaba a efectuar frecuentes cambios de direcciones IP y afectaba la continuidad en la realización de las copias de seguridad. Para resolver esta situación, lo que se hizo en laboratorio fue probar con los diferentes software cuál de ellos podría servir para continuar con la realización de las copias de seguridad desde el punto en que quedaron pendientes, sin importar que se cambiarán de ubicación y de dirección IP.

El resultado fue que los programas no encontraron el identificador de la información nueva que enviaría a través de la red para ejecutar el **“Respaldo Incremental”.**

Al tener un primer respaldo full y tratar de ejecutar un respaldo incremental agregando un cambio de la dirección IP, los programas probados dieron como resultado que, como no identificaban el respaldo full para realizar el respaldo incremental, ejecutaba un respaldo full, lo que no cumplía con las especificaciones del cliente, ya que enviar un respaldo full por la red era una pérdida de tiempo y un gasto innecesario de recursos, como el ancho de banda.

Al realizar las copias de seguridad con la herramienta Iperius, efectuando cambios físicos y cambios en la configuración, como en la dirección IP, me mostró como resultado que la herramienta Iperius cumplía con las especificaciones mencionadas del cliente.

La herramienta permitía realizar respaldos incrementales por la red del cliente a los equipos asignados, sin importar los cambios de direcciones IP o de ubicación dentro de la red.

Seguía realizando copias incrementales sin ningún problema.

La herramienta Iperus tiene además versatilidad como administración vía remota desde una consola **(Iperius Console).**

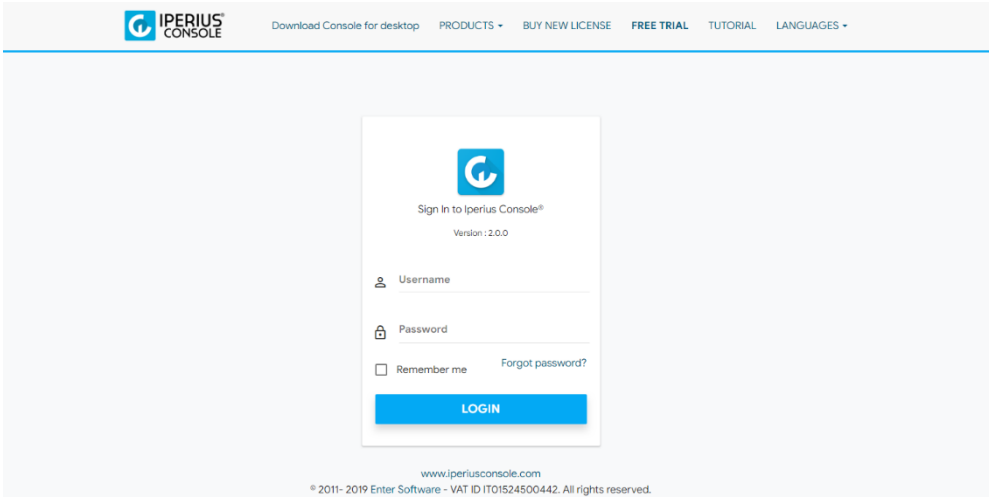

Imagen Núm.60 Interfaz principal de Iperius Console.

Iperius Console: lo que hace esta herramienta es centralizar todas las licencias Iperius adquiridas y muestra un resumen de las actividades de cada uno de los equipos que tengan el software instalado.

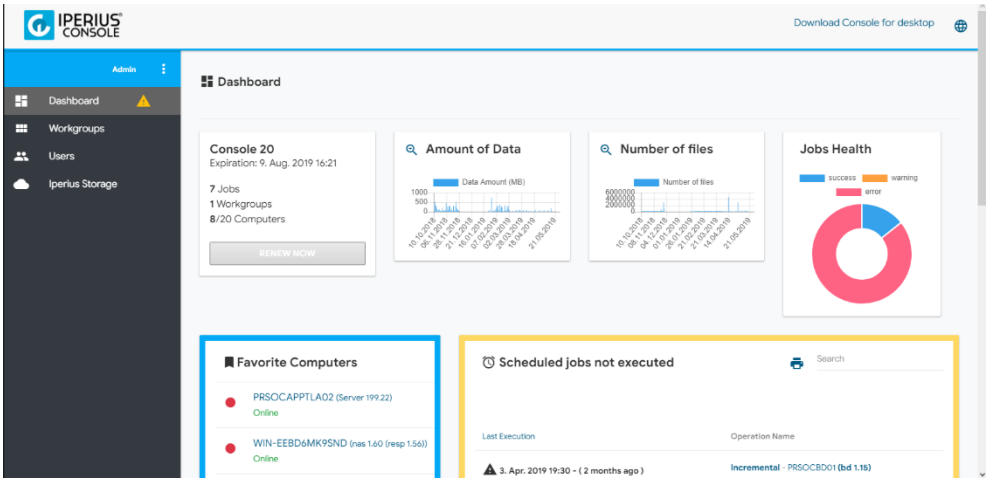

Imagen Núm. 61. Menú principal de Iperius Console.

Otra característica que se tomó en cuenta es que permite la copia de seguridad de bases de datos como son SQL server, Oracle, PostgreSQL, MySQL, etc.

La versatilidad y la facilidad del entorno que tiene Iperius fueron unas de las principales razones que se tomaron en cuenta para proponer que esta herramienta realizara las tareas que solicitó el cliente, sobre todo el soporte brindado por la empresa que comercializa Iperius es muy útil en caso de requerir ayuda en alguna tarea o duda que se presentara.

Capítulo IV. Solución e Implementación

Al contar con información de suma importancia para el cliente, se determinó que era importe realizar un proyecto DRP en los servidores principales, así como respaldar un total de siete (7) equipos.

El área comercial de Global Cybersec adquirió siete (7) licencias Iperius Essential y una (1) licencia Iperius Console 20.

La licencia Iperius Essential es el tipo de software que permite realizar las tareas de respaldo, en comparación con las versiones Base, Free y Desktop.

- **La limitante con la versión Free es que no se puede conectar a la consola, lo que da como resultado que la administración de las demás licencias no se pueda realizar de manera adecuada.**
- **Con Iperius Free se tiene la limitante de días para poder usarla con sus características y módulos configurados.**
- **Con respecto a la licencia Desktop, la principal deficiencia es que solo se usa para sistemas operativos como Windows XP, Windows 7, 8, 10, etc.; en este caso, el sistema operativo que se utiliza en los servidores es Windows Server 2012 R2, por lo que se determinó que la opción más viable en el listado de las versiones de Iperius es usar la versión Essential.**
- **Las demás versiones podrían ser otra alternativa, pero con las características con que cuenta el cliente no se aprovecharían al máximo las licencias y quedarían limitadas en sus funciones.**

Las licencias adquiridas se distribuyeron de la siguiente manera:

- **Cinco (5) licencias Iperius Backup Essential a servidores de correo, servidores web, servidores que contienen base de datos, etc.**
- **Dos (2) licencias Iperius a los *File Server* y los dispositivos más críticos de toda la organización.**
- **Iperius Console 20 se instaló en un servidor virtualizado dentro de un segmento de red específico, equipo desde el cual se monitorea la actividad de las siete (7) licencias Iperius.**

Asimismo, se crearon “Jobs” con la finalidad de programar los respaldos de seguridad.

Con relación a las cinco (5) licencias mencionadas, se determinó efectuar las copias de seguridad de la siguiente manera:

- **Diariamente, programando su ejecución a partir de las 19:00 hrs.; esto se llevaría a cabo en un lapso de entre 45 minutos y 3 horas como máximo.**

Con respecto a las dos (2) licencias de Iperius que se asignaron a los *file server,* se determinó realizar los respaldos de seguridad de la manera siguiente:

- **Cuando se trata del primer respaldo que se realiza, el "shot inicial" se debe efectuar de manera local en las oficinas centrales hacia los equipos designados para su almacenamiento, esto con la finalidad de no utilizar todo el ancho de banda del internet con el que la institución cuenta.**
- **Cuando se trata de respaldos incrementales se puede realizar mediante el uso del ancho de banda para poder enviar la información desde la oficina central a los diversos lugares donde se encuentran los equipos designados para almacenar la copia de seguridad.**
    - **Para el file server de 4 TB se configuró que la ejecución de la tarea se realizará los miércoles y viernes a partir de las 00:00 horas y como límite las 7 a. m.; esto con la finalidad de realizar la copia de seguridad en horarios en que no se afecten las operaciones de la institución y de garantizar la disponibilidad de la información en los horarios laborales.**
    - **Para el file server de 17 TB se configuró que la ejecución de la tarea se llevara a cabo los fines de semana, comenzando con el "shot incremental" los viernes a las 23:55 horas con la finalidad de que se cuente con el fin de semana para completar la tarea.**
- **Es muy importante señalar que el "shot inicial" se debe realizar siempre de manera local, ya que el cliente ejecutó la tarea sin notificar a Global Cybersec, lo que dio como resultado que las comunicaciones en sus instalaciones de Tlalpan se interrumpieran por la saturación del ancho de banda.**

Actualmente se encuentra en operación y cada mes se elabora un informe, el cual se entrega con la finalidad de cumplir los acuerdos pactados en la propuesta laboral que se tiene con el cliente.

En este documento se presenta parte del proceso de un DRP, teniendo en cuenta que se necesitará un proceso de BCP (Business Continuity Plan) para garantizar la disponibilidad de la información en los servidores de la institución.

Lo recomendable es que se lleve a cabo una planeación de los equipos y servicios; y establecer tres niveles de criticidad para identificar qué equipos son los más riesgosos en la operación con la finalidad de contar con un plan en caso de desastre.

Después, se tiene que considerar la tecnología más adecuada para las necesidades de la organización.

Respecto a la estructura principal de un DRP, en la norma ISO-27001 se describe cómo se debe realizar la gestión de seguridad de la información en una organización.

Para explicar lo relacionado con los DRP, en el punto 17 que se describe a continuación se analizará lo establecido en dicha norma:

- **A.17.1.1. Planificación de la continuidad de la seguridad de la información**
    - En este apartado se evalúan los requisitos de la seguridad de la información y se analizan los activos de la empresa, catalogándolos en tres severidades (Alta, Media y Baja), siendo la alta equipos críticos y de suma importancia, en los cuales se debe poner mayor atención para realizar las copias de seguridad y analizar que podrían ser afectados en caso de que la operación se detenga por falta de energía eléctrica, comunicaciones, red o hasta por el posible colapso de la infraestructura.

- **A.17.1.2. Implementación de la continuidad de la seguridad de la información**
    - Este apartado se enfoca en implementar la gestión de la continuidad ante situaciones de emergencias inesperadas.
    - Ejemplos de cómo actuar en caso de pérdida del site principal.
    - Ejemplo de cómo actuar en caso de desastre natural.
    - Ejemplo, y no menos importante, de cómo actuar en caso de error humano.
    - Contar con planes en los cuales se tengan respuestas antes esas emergencias.
    - Establecer una estructura de gestión donde se definan responsabilidades en la continuidad y la recuperación; y designar a las personas que desempeñarán las distintas funciones dentro del plan de continuidad.
    - Los niveles son:
        - Gestionar de los incidentes de seguridad.
        - Mantener los niveles de seguridad de la información.
        - Recuperar los sistemas informáticos.
- Creación de la documentación y de los procedimientos siguiendo tres aspectos básicos:
    - Cómo se va a gestionar un evento destructivo.
    - Cómo se va a mantener la seguridad de la información en un nivel mínimo planificado.
    - Asegurarse de que se cuenta con los objetivos mínimos para la continuidad de la información (se definen en el apartado A.17.1.1).

- **A.17.1.3. Verificar, revisar y evaluar la continuidad de la seguridad de la información**
    - Este apartado sirve para que se continúen aplicando las políticas descritas anteriormente y se asegure que los equipos y la operación se mantengan protegidos ante cualquier desastre.
        - La aplicabilidad de los controles.
        - Los nuevos activos que se adquieran deben ser considerados para formar parte del plan de continuidad.
        - Verificar que el personal asignado para la recuperación esté al tanto de las responsabilidades asignadas.

- **A.17.2.1. Disponibilidad de las instalaciones de procesamiento de información**
    - En este apartado se proporciona la idea de tener sistemas redundantes que permitan reaccionar en tiempo real a la caída de sistemas o activos de información estratégicos.
    - Analizar la viabilidad de sistemas redundantes.
    - Identificar qué sistemas de información por su arquitectura no pueden garantizar la disponibilidad.
    - Realizar pruebas de funcionamiento, así como pruebas de transición sin interrupciones de un sistema principal a un sistema redundante.

:

Conclusiones

Como expuse y se puede observar en este documento de titulación, el uso de la herramienta Iperius en las organizaciones representa una solución eficaz, accesible y de gran utilidad.

Como comprobé en la práctica, la funcionalidad de la herramienta puede ayudar a realizar copias de seguridad en las organizaciones sin importar si tienen o no información sensible.

Al utilizar estas herramientas, las organizaciones deben considerar desde un inicio la creación de un DRP para poder garantizar la continuidad de la operación y la disponibilidad de la información en cualquier momento.

Algo que se debe tener en mente al realizar un DRP es que exista más de un lugar en donde se almacene dicha información; en pocas palabras, se deben tener por lo menos tres servidores donde se realicen las copias de seguridad.

Asimismo, se debe disponer de una segunda o tercera ubicación en caso de que por alguna razón, ya sea que se trate de un desastre natural o de alguna crisis en la población, se impida la continuidad de las operaciones en la ubicación principal.

Además, se debe tener información actualizada de la capacidad de los servidores para evitar el llenado de discos de manera rápida, lo que redundaría en pérdidas de tiempo para adquirir un nuevo servidor y durante ese lapso no se mantendría actualizada la información.

De acuerdo con mi experiencia laboral, podría recomendar que se tengan en cuenta dos aspectos de suma importancia:

- Tener un adecuado control de los permisos asignados a los usuarios, esto con la finalidad de que, si tienen un ***File Server*** compartido en la institución, los usuarios no tengan acceso a carpetas que podrían ser de otra área.

    - Poder acceder a carpetas de otra área puede representar un grave problema, ya que el usuario podría eliminar carpetas que no sean de su área, lo que significaría la pérdida de información o en casos más importante la extracción de información sensible de la empresa.

- Automatizar las tareas con la finalidad de optimizar los tiempos; para ello, Iperius permite automatizar las tareas conforme a las necesidades de la institución a la vez que se puede enviar un correo electrónico al final de cada tarea para su seguimiento, esto desde la configuración básica de cada tarea.

Pudiera ocurrir que al llevar a cabo las copias de seguridad en alguna institución el personal de redes bloquee la comunicación de algunos puertos o inclusive los equipos de seguridad no permitan desde la simple actualización del software (la conexión del software Iperius al servidor para validar la licencia con el proveedor) o actualizar el software a la versión más reciente, como la transferencia vía enlace de las copias de seguridad.

También se debe considerar qué “servicios” son los más críticos para la organización y cuánto tiempo se llevará restaurarlos.

Igualmente, es muy importante revisar siempre la salud de los equipos, puesto que, al tratarse de un equipo mecánico, en algún momento de su vida operacional fallará y esto podría provocar una pérdida significativa de información.

Por último, se debe conocer con exactitud cómo funcionan los diferentes tipos de raid y, a su vez, cómo restaurar uno en caso de que algún disco llegara a dañarse (cosas que no es normal que sucedan, pero que pudieran pasar).

Bibliografía y Mesografía

- **LIMONCELLI, Thomas,**
  The Practice of System and Network Administration, Volume 1: Devops and Other Best Practices for Enterprise It, Editorial Addison-Wesley Professional, 3era. Edición, 2016.

- **SOOD, Aditya,**
  Targeted Cyber Attacks: Multi-staged Attacks Driven by Exploits and Malware, Editorial Syngress, 1era. Edición, 2014.

- **SCHMIDT, Klaus;**
  High Availability and Disaster Recovery: Concepts, Design, Implementation, Editorial Springer, 2006.

Mesografía:

- https://latam.kaspersky.com/resource-center/definitions/what-is-ransomware
- https://ciberseguridad.blog/como-prevenir-los-ataque-insiders/
- https://sicrom.com/blog/tipos-ataques-informaticos/
- https://searchdatacenter.techtarget.com/es/cronica/Copia-de-seguridad-completa-incremental-o-diferencial-como-elegir-el-tipo-adecuado
- https://www.codigomaestro.com/general/diferentes-tipos-de-raid/
- https://www.welivesecurity.com/laes/2014/10/14/plan-de-recuperacion-ante-desastres/
- https://normaiso27001.es/a17-aspectos-de-seguridad-de-la-informacion-en-la-gestion-de-continuidad-del-negocio/
- https://www.iperiusbackup.es/backup-windows-server.aspx