Aranda SOFTWARE

Aranda
Data Safe

Manual de Instalación y Uso de Software

Tabla de Contenido

Control de Cambios	
Fecha de Creación	**Aranda Date Safe Manual de Instalación y Uso**
2017.Nov.22	*Versión 1*
	Elaborado por:
	Aranda Software

1. Introducción a Aranda Data Safe

Aranda Data Safe proporciona una solución simple, sólida y automatizada para realizar backup de información de manera simplificada en los equipos de escritorio y portátiles. La protección y la copia de seguridad de los datos se realiza de manera centralizada, ágil y eficiente. La solución de Backup de Aranda Data Safe tiene tres componentes principales.

La solución de Backup de Aranda Data Safe se compone de 3 componentes principales:

1.1 Componentes de Aranda Data Safe

El Servidor de Aranda Data Safe almacena y archiva de manera segura toda la información de los backups.

La Consola de Administración de Aranda Data Safe es la herramienta centralizada instalada en los equipos de los administradores de los backups, usada para controlar y gestionar todos los servidores de Data Safe en su organización. Los administradores de los backups, realizaran tareas desde la consola de administración para asegurar que se realicen backups constantemente a la información crucial de la organización.

El Agente de Aranda Data Safe es el cliente de backup instalado en los equipos de cómputo de los usuarios de backup de la organización. Este agente es responsable de los procesos de backup y restauración de la información

1.2 Retos a los cuales se enfrenta el área de IT

Las políticas de backup dentro de una organización tienen la intención de proporcionar un medio estandarizado para realizar copias de seguridad y mantener de los datos del negocio. Los Backups y restauraciones de la información son fundamentales para la viabilidad y el funcionamiento de una organización, y es esencial seguir ciertas prácticas básicas para garantizar que los datos están siendo respaldados con éxito.
Muchas compañías tienen una política de backup de datos que requiere que todos los usuarios copien sus datos relacionados con el trabajo o del negocio en un servidor central. Sin embargo, regularmente esto no se cumple, dado que no hay procesos automáticos para realizar el backup por parte del usuario. Por olvido, falta de tiempo y backups que pueden tomar mucho tiempo los usuarios no lo realizan.

En algunos casos la información a la que se le realiza copia de seguridad corresponde a imágenes, películas y música almacenadas en el servidor de archivos mientras los datos empresariales sensibles se mantienen en el escritorio o portátil debido a que no existe confidencialidad en el servidor.

Cada vez que una computadora de escritorio o portátil es robado, dañado o falla el disco duro, el usuario pierde los datos y la empresa pierde dinero e información importante. El departamento de TI por lo general es el responsable de dicha pérdida de datos.

1.3 ¿Por Qué usar Aranda Data Safe?

Al usar Aranda Data Safe, puede establecer centralizadamente una política de backup que definirá la información a respaldar del usuario final, donde se incluye el día y hora para iniciar esta tarea de manera automática. Estas y otras configuraciones son administradas y actualizadas de forma centralizada por medio de la Consola de Administración, permitiendo monitorear y tener reportes de las actividades de respaldo/restauración de la información. Los agentes de Backup pueden ser fácilmente desplegados en los equipos de los usuarios finales, sin intervención del usuario, cuando se utilizan herramientas de despliegue como Directorio Activo GPO, Aranda Software Delivery, Remote Setup, Radia y otros.

Los backups se almacenan y archivan de forma segura en el servidor de Data Safe, permitiendo restaurar cualquier versión de la información. Esto también resuelve por completo el riesgo de acceso a datos personales por parte de otros usuarios.

1.3.1. Backups Automatizados

Aranda Data Safe elimina la dependencia de realizar los respaldos de la información crítica del negocio ubicada en los equipos de los usuarios finales. El proceso de backup se realiza de manera automatizada en horas programadas sobre los archivos nuevos y modificados. Adicionalmente, todos los datos son comprimidos y cifrados durante el proceso de backup.

Al realizar el respaldo de los archivos modificados, se realiza una verificación bit a bit sobre la información modificada dentro de cada archivo de manera eficiente y reduciendo los tiempos en el momento de realizar los backups.

Las funcionalidades de verificación bit a bit y compresión de Data Safe hacen de esta la solución perfecta para usuarios móviles y oficinas remotas.

1.3.2. La Recuperación De Los Datos Es Rápida Y Sencilla

Cuando ocurra una pérdida de datos o requiera reemplazar el hardware, siga los tres pasos del asistente de restauración; el proceso puede ser realizado por el usuario ayudando a liberar tiempo y recursos.

Aranda Data Safe le ayuda a su organización con las siguientes tareas:

- Eliminar la perdida de datos.
- Reducir los tiempos de inactividad al reemplazar o migrar equipos.
- Erradicar los altos consumos de recursos requeridos para encontrar o recrear la información.
- Disminuir los costos de infraestructura en términos de uso de ancho de banda y almacenamiento.
- Permite ofrecer un mejor servicio a usuarios finales por parte del área de IT.

1.3.1 ¿Qué es DLP?

Data loss Prevention / Prevención de pérdida de datos

Aranda Data Safe ofrece potentes funcionalidades adicionales para proteger los datos de su empresa en caso de pérdida o robo de un dispositivo.

Encriptación: Aranda Data Safe protege completamente los archivos contra el acceso no autorizado cifrando de forma segura los archivos en el computador del usuario. Al cifrar selectivamente los datos sin excluir los archivos del sistema operativo, garantiza un impacto mínimo en los computadores de los usuarios en comparación con otras soluciones de cifrado de disco.

Prevención de robo de datos: La prevención de robo de datos, característica exclusiva de Aranda Data Safe, permite a las organizaciones revocar automáticamente el acceso de los usuarios a los datos después de un período de tiempo establecido. Si el equipo de un usuario no se ha conectado a la red

durante un período de tiempo definido, no se podrá acceder a los archivos del dispositivo. Si una máquina se pierde o es robada, los archivos se protegen automáticamente de acceso no autorizado.

Revocación remota: Aranda Data Safe, permite que el acceso a los archivos sea remotamente revocado de manera no destructiva, evitando que el usuario acceda a sus archivos. Esto evita el robo de datos y aumenta la protección de su organización contra el espionaje industrial y es exclusivo de Aranda Data Safe.

Borrado Remoto: Borrado remoto permite a su organización de forma remota borrar datos en un equipo perdido o robado, de forma rápida y fácil. Aranda Data Safe lleva a cabo una fase única (Proceso de borrado remotos primero revocando acceso a los datos asegurando una ventana mínima exposición de los datos y, posteriormente, realizar una eliminación y un borrado seguro de los datos.

1.3.2 Acerca de esta guía

El manual del producto Aranda Data Safe describe cómo implementar y usar este software. La guía está dirigida para usuarios básicos y experimentados; requiere de conocimientos básicos en sistemas operativos de Microsoft Windows y tecnologías de red asociadas.

1.3.3 Propósito de esta Guía

El manual del producto provee instrucciones detalladas de los procesos de implementación de cada componente de Aranda Data Safe, desde la instalación y configuración hasta el despliegue de los agentes. De esta manera podrá disfrutar los beneficios de tener una herramienta que le permitirá proteger su información de manera segura y eficiente.

1.3.4 Implementación de los componentes

El proceso de implementación de la solución Aranda Data Safe se realiza de la siguiente manera:

- Servidor de backup – Instalación del servidor de Backup.
- Consola de administración – Instalación y configuración de la consola centralizada de administración del servidor de backup
- Agentes de usuario – Crear y desplegar un agente de usuario en los equipos de escritorio y portátiles.

1.3.5 Publicaciones Relacionadas

Las siguientes publicaciones relacionadas con este manual se encuentran disponibles.

- Guía de inicio – Guía rápida de instalación de Aranda Data Safe.
- Tareas de administrador – Guía de tareas requeridas para la administración de la solución de backup de Aranda.
- Guía de Actualización – Guía para realizar actualizaciones del producto de versiones anteriores.

2. Requerimientos del sistema de Aranda Data Safe

Para un uso eficiente de Aranda Data Safe, es necesario contar en las estaciones de trabajo con los siguientes requerimientos mínimos de hardware y software. Dentro de este documento se definen dos tipos de requerimientos del sistema: Mínimos y Recomendados. Los requerimientos del sistema pueden cambiar en el tiempo debido a factores como el incremento en la cantidad de Backups almacenados, usuarios de Backups o recursos para nuevas versiones de software.

2.1 Requerimientos de hardware

Los requerimientos del Servidor de Aranda Data Safe se encuentran basados en el número de usuarios simultáneos que se encuentran ejecutando un Backup y en el tamaño total de información a ser almacenada. Máximo se pueden tener 60 usuarios concurrentes realizando un Backup en un servidor de Aranda Data Safe. Sí los Backups se procesan durante horario laboral, y cada Backup de usuario se tarda 30 minutos en ser completado, esto se traduce en:

13 horas. X 30 minutos por sesión = 26 Sesiones x 60 usuarios concurrentes = 1,560 Usuarios.

Por lo tanto, es recomendable en un solo servidor tener un máximo de 1,560 usuarios realizando respaldo de la información.

Sí se usan unidades de almacenamiento como Network Attached Storage (NAS) o Storage Área Network (SAN) es posible agregar más servidores de Data Safe y tener toda la información almacenada en la NAS o SAN. Esto le permitirá tener todos los datos en un solo dispositivo.

2.2 Requerimientos del Servidor Aranda Data Safe

Sistema Operativo	Windows Server 2012/2012 R2/2016 [32 & 64 Bits]
CPU y Memoria RAM	Los requerimientos de CPU y Memoria RAM dependen del número de usuarios concurrentes a los cuales se procesará un backup y el tamaño de los datos a almacenar en el servidor. Estas recomendaciones están sujetas a las siguientes variables: • **Servidor Categoría A** Usuarios: 50 Procesador: 2.8 GHz RAM Mínima: 2GB • **Servidor Categoría B** Usuarios: 500 Procesador: 3.0 GHz RAM Mínima: 4GB • **Servidor Categoría C** Usuarios: 1500 Procesador: Dual Xeon 3.0 GHz RAM Mínima: 8GB
Tipo de Disco y Espacio	**Requerido:** • SATA (IDE) Disk Drive con 1GB de espacio disponible más espacio para todas las cuentas de Backup en el servidor. Ejemplo: 500 cuentas de Backup, cada una con 1GB de espacio = 500GB +1GB **Recomendado:** • RAID 5 y SCSI / SATA o High Performance • Almacenamiento (SAN / NAS) con 2 GB de espacio libre y suficiente espacio en disco para todas las cuentas de Backup en el servidor.
Red	• Tarjeta de red con un ancho de banda de 100 Mbps requerida. Se recomienda usar tarjeta de red con 1Gbps. • Dirección IP fija o un nombre de dominio por DNS.

	• Conectividad a todos los equipos de escritorio o portátiles. Los puertos usados son definidos en la instalación del producto. Por defecto se utilizan los puertos 8080 y 8443.
Antivirus	Recomendamos excluir el directorio del Servidor Aranda Data Safe del análisis en tiempo real de su antivirus. « [programfiles]\Aranda\Aranda Data Safe Server* »
Otros requerimientos	CD-ROM 8x

Ambiente del Agente Aranda Data Safe

Sistema Operativo	Windows 2000, Windows XP. Todas las versiones de 32 Bits. Windows Vista [32 y 64 Bits], Windows 7 [32 y 64 Bits]. Windows 8, 8.1 [32 y 64 Bits] y 10 [32 y 64 Bits].
CPU y RAM	Los requerimientos de CPU y memoria RAM dependen de la cantidad de datos a realizar un Backup. • Sistemas Windows XP **Recomendado** CPU: Pentium IV 2.4 GHz – Procesador equivalente o superior Memoria: 1 GB o superior • Windows Vista, 7, 8, 8.1 y 10 **Recomendado** CPU: Pentium IV 2.4 GHz – Procesador equivalente o superior Memoria: 2 GB o superior
Espacio Disco Duro	100 MB más el espacio para el Cache **Cache:** 0,5% de la selección La cache es el espacio requerido para almacenar la versión previa de la información con el fin de poder calcular las diferencias entre la última y la nueva versión de un archivo.

RED	Tarjeta de red con ancho de banda de 100 Mbps. Puertos por defecto de la instalación 8081 y 8443. Estos son modificables.
Antivirus	Recomendamos excluir el directorio del Agente Aranda Data Safe del análisis en tiempo real de su antivirus. « [programfiles]\Aranda Data Safe* »

2.3 Check List de la instalación

Para continuar con la instalación de Aranda Data Safe, por favor asegúrese de contar con lo siguiente:

Instalador de Aranda Data Safe – El software debe ser descargado desde la página de Aranda o puede ser facilitado por otros medios.

Archivo de licencia del servidor – Una licencia le será suministrada por Aranda.

Se deben cumplir los requerimientos mínimos de software y hardware:

- El agente de usuario para portátiles y equipos de escritorio
- El servidor de Aranda Data Safe

El equipo donde se encuentre instalada la consola de administración, debe disponer de una conexión con el servidor de correo.

2.4 Solicitud de archivo de licencia

Cada servidor de Aranda Data Safe en su organización requiriere de una licencia valida y activada. Los archivos de licencia solo pueden ser obtenidos desde Aranda o con un Partner autorizado.

Puede solicitar su licencia y descargar el software de Aranda Data Safe de la siguiente manera:

- Para solicitar una versión demo, por favor enviar un correo a **serials@arandasoft.com**
- Para descargar los instaladores por favor ingresar a http://www.arandasoft.com.

Los siguientes datos son requeridos cuando se solicita una licencia:

- Nombre de la organización, nombre y detalles del contacto.
- Nombre o dirección IP fija del servidor. Se recomienda suministrar el nombre del servidor
- Cantidad de licencias – El número de cuentas de usuarios requeridos.
- Fecha de caducidad – Suministrar el periodo de tiempo en el cual desea usar el producto.

Luego de recibida la solicitud, el área comercial enviara un archivo de licencia sin activar en un correo electrónico.

3. Instalación de Aranda Data Safe

Cada uno de los componentes de Aranda Data Safe podrá ser instalado siguiendo los siguientes pasos. La instalación del servidor de Aranda Data Safe comienza creando una carpeta donde se almacenará toda la información de los usuarios de forma cifrada.

Antes de comenzar con la instalación, asegúrese de que su entorno de backup cumple con los requisitos mínimos según lo estipulado en **Requerimientos del servidor.**

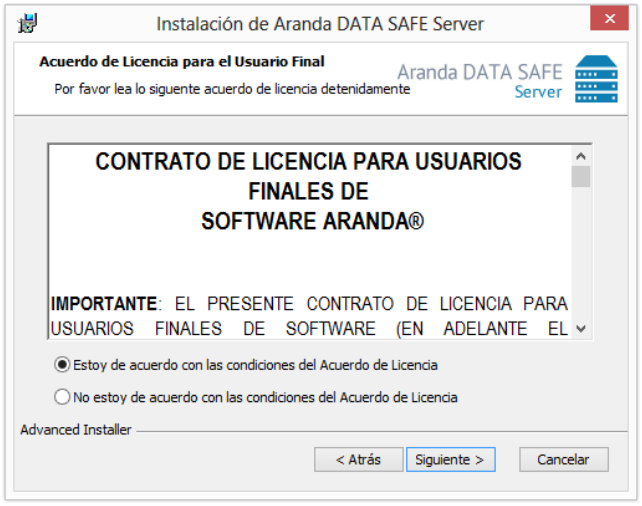
NOTA: Cuando se instala el Servidor de Aranda Data Safe, este se configura para ejecutarse como un servicio y cualquier cambio que se requiera debe ser realizado desde la consola de administración**.**

Copiar los instaladores de Aranda Data Safe en el sistema aprovisionado para su instalación.

3.1. Instalación del servidor Aranda Data Safe

Hacer clic sobre el instalador de arandasoft-server-x.x.x.msi para ejecutar el asistente de instalación del servidor de Aranda data Safe. Las “x” definidas en el nombre es la versión actual del server.

Hacer clic en “Siguiente” para proceder y desplegar el acuerdo de licencia del usuario final.



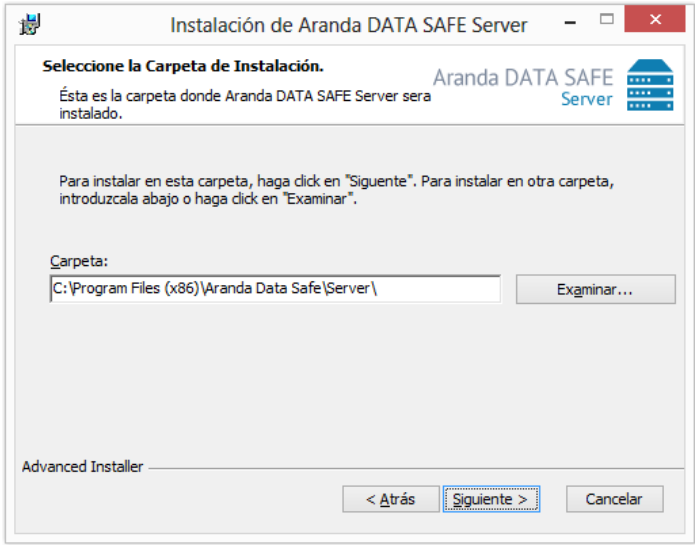
Leer el acuerdo de licencia y seleccionar la opción “Estoy de acuerdo con las condiciones del Acuerdo de Licencia” para aceptar los términos y condiciones.

Hacer clic en “Siguiente” para continuar.

Configurando carpetas de instalación

El primer paso para la instalación es determinar donde se instalará el software de Aranda Data Safe.

Se presenta la ventana “Seleccione la Carpeta de Instalación” donde muestra la ruta de instalación por defecto.



Puede cambiar la ruta de instalación dándole en el botón “Examinar…”, donde puede navegar y seleccionar una ubicación diferente.

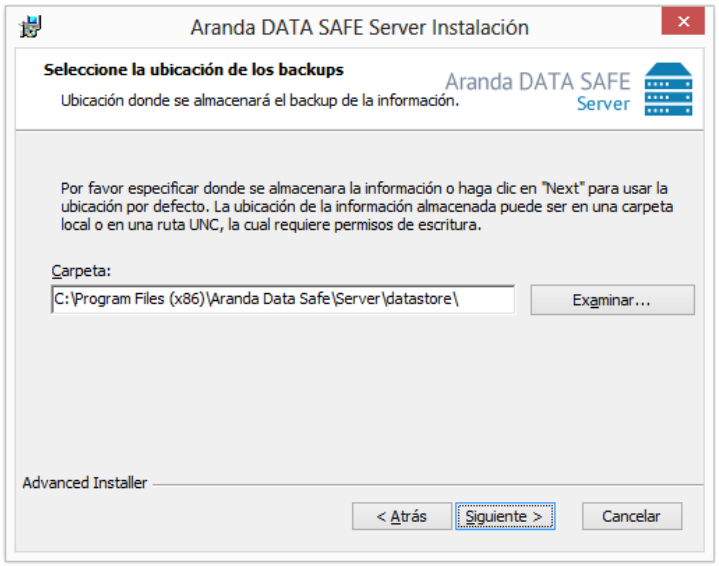
Luego de seleccionar la ruta por defecto o la alternativa, hacer clic en “Siguiente” para continuar.

En la ventana “Seleccione la Ubicación de los Backups” permite seleccionar la ubicación donde se almacenarán los respaldos de la información.

Puede usar una ruta UNC (Uniform Naming Convention) para especificar una ubicación a un disco en otro servidor o en otra red. Ejemplo “\\NombreEquipo\BackupsDiarios\Aranda\Aranda Data Safe\data\”.

- Tener en cuenta que esto únicamente aplica para la ruta del backup y no para la ruta de instalación.
- El servidor debe tener suficientes permisos de escritura en la ruta UNC o remota. Un disco mapeado asociado con la ruta UNC no debe ser usado.

Nota: El contenido de estas dos ubicaciones debe ser incluido dentro de las tareas de backup cuando se desee realizar un respaldo del servidor de Aranda Data Safe.



Puede cambiar la ruta donde serán almacenados los backups dando clic el en botón **Examinar**, donde puede navegar y seleccionar una ubicación diferente.

Si se ha seleccionado la ruta por defecto o una ruta alterna, hacer clic en **Siguiente** para continuar.

Configurando puertos del servidor de Backup

La ventana “Ingresar puertos para el servidor de backup” permite indicar los puertos que usara la aplicación para el envío de la información a través de canales seguros y las actualizaciones de políticas y de las versiones de los agentes.

Para cambiar los puertos por defecto, solo debe modificar su valor por el nuevo deseado.

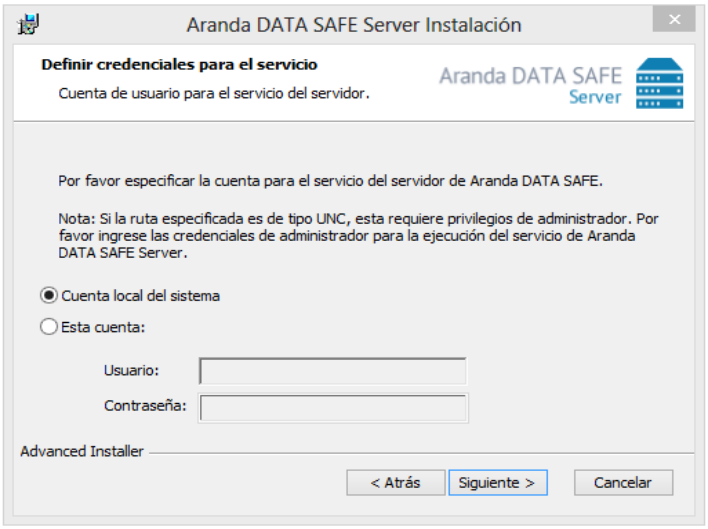
Nota: Se debe garantizar que los puertos definidos para el servidor y las actualizaciones no estén siendo usado por otras aplicaciones.

Luego de seleccionar los puertos del servidor y de las actualizaciones hacer clic en **Siguiente** para continuar.

Configurando credenciales del servidor

Por defecto, las credenciales del servicio del servidor de Aranda Data Safe están configuradas para ejecutarse con la cuenta del sistema. Sin embargo, pueden ser modificadas en caso de ser necesario, con el fin de poder ejecutar el servicio usando una cuenta con permisos de administrador en rutas remotas (UNC) especificas donde se almacenará la información.

La ventana “Definir credenciales para el servicio”, permite determinar el usuario con el cual se ejecutará el servicio del servidor de Aranda Data Safe.



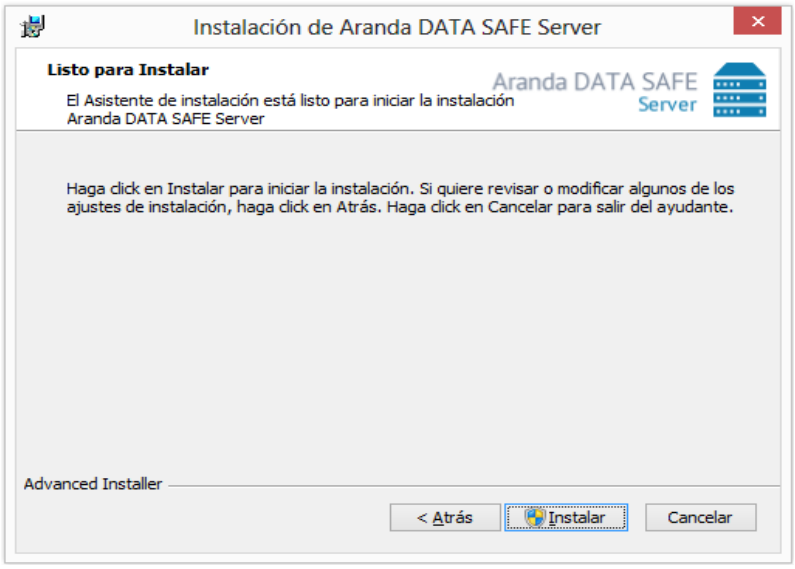
Seleccionar una de las opciones:

- Cuenta local del sistema: Ejecutará el servicio de Aranda Data Safe con la cuenta local del sistema
- Esta cuenta: Ejecutará el servicio con una cuenta definida por el administrador.

Nota: Para efectos de despliegues en esquemas de directorio activo se debe definir una cuenta de administrador de dominio.

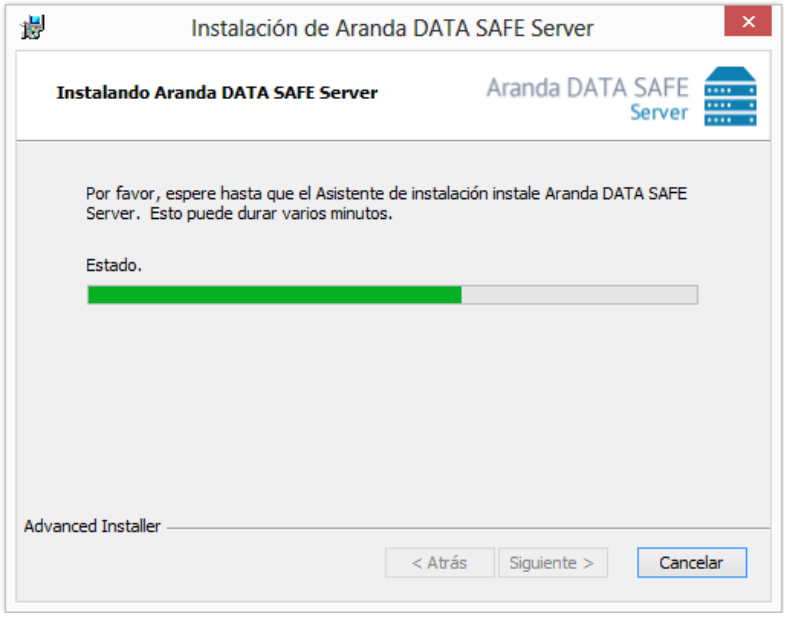
Luego de definir la cuenta con la cual se ejecutará el servicio del servidor de Aranda Data Safe, hacer clic en **Siguiente** para continuar.

A continuación, se muestra el cuadro de dialogo “Listo para Instalar”

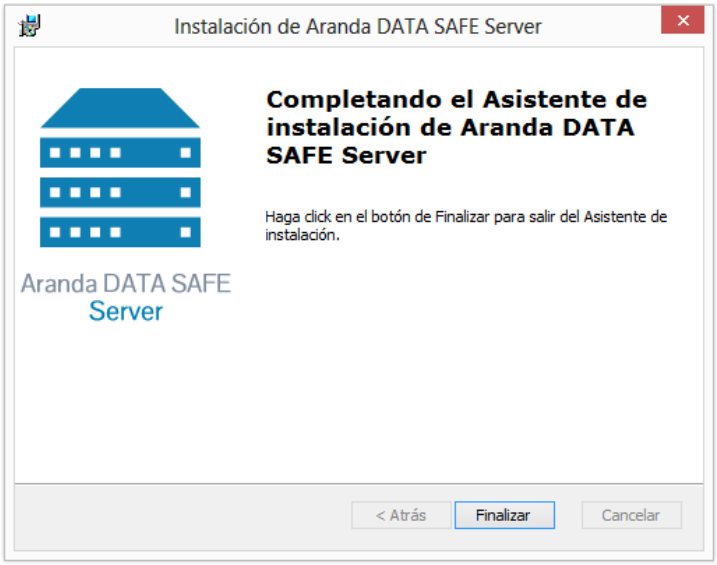


En esta etapa puede regresar para cambiar cualquiera de los parámetros de instalación configurados.

Sí la configuración es la deseada para la instalación, presionar el botón **Instalar** para proceder con el proceso de instalación.



Se muestra el cuadro de instalación del servidor de Aranda Data Safe. Se notificará cuando finalice la instalación de Aranda Data Safe.



Hacer clic sobre el botón **Finalizar** para terminar el proceso de instalación.

3.2. Administrar el servicio de Aranda Data Safe

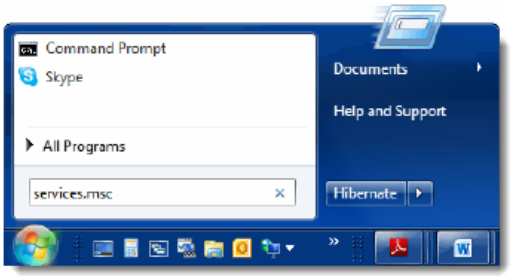
Durante la instalación del servidor de Aranda Data Safe, este es instalado e iniciado como un servicio. Sin embargo, si experimenta algún problema con el servidor de Aranda Data Safe, puede usar la consola de servicios de Windows (services.msc) para detener, iniciar o reiniciar el servicio.

Par abrir la consola de servicios, ir al botón de inicio de Windows.

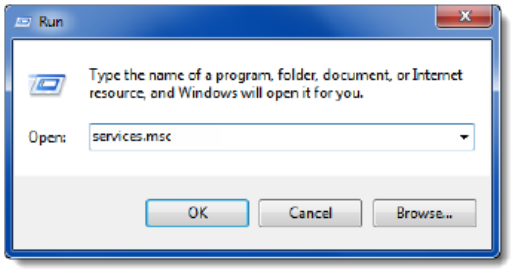
- Para Windows Vista/7/8/10, escribir **services.msc** en el espacio de búsqueda del menú de inicio y luego dar **enter**.

- Para Windows XP, seleccionar **Ejecutar** y escribir **services.msc** en el cuadro de dialogo y dar OK.

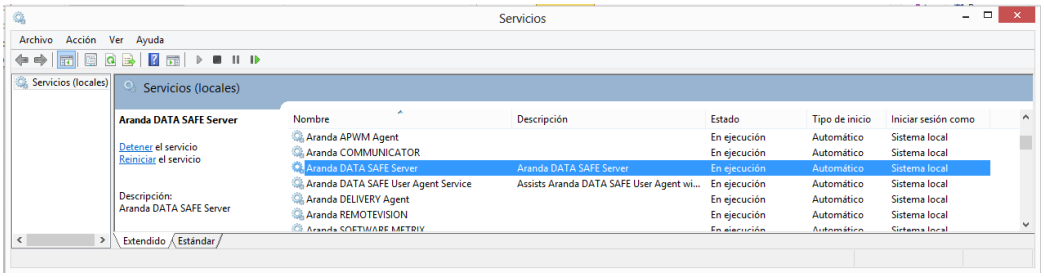
Vista / Windows 7



Windows XP



Localizar y seleccionar el servicio **Aranda Data Safe Server** para iniciarlo, detenerlo o reiniciarlo.

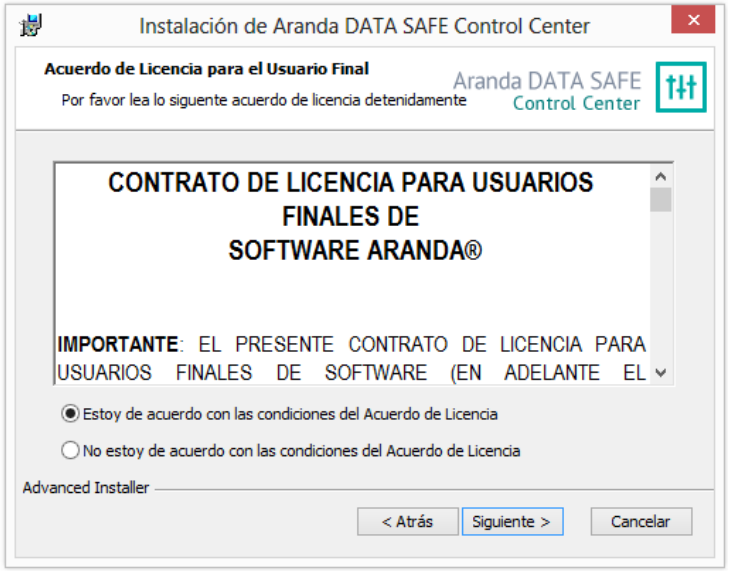


Cuando el servicio de Aranda DATA SAFE Server se encuentra iniciado, estará activo y listo para usar.

3.3 Instalación de la consola de administración

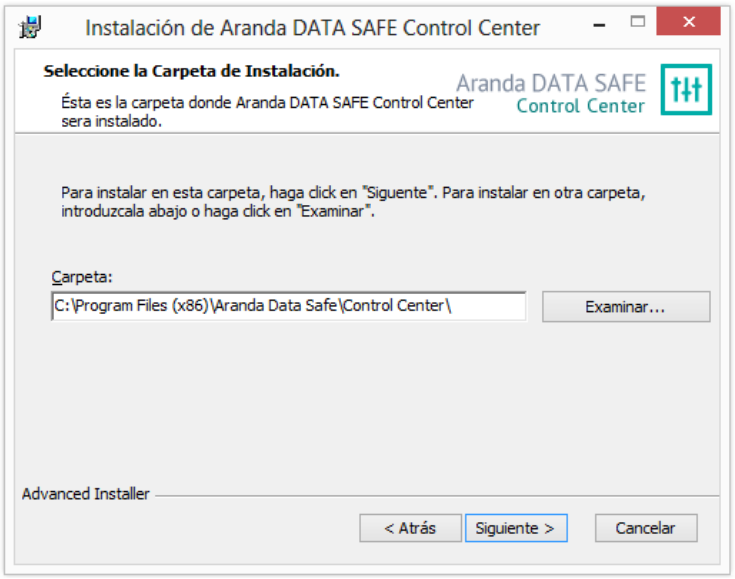
Copiar los instaladores de Aranda Data Safe en sistema aprovisionado para su instalación. Dar doble clic sobre el instalador o ir al cuadro de dialogo sobre el botón inicio del escritorio y digita ADTS_Consola.exe, mediante el cual se iniciará el asistente de instalación de la consola de administración de Aranda Data Safe. La x es la versión actual de la consola.

Presionar el botón Siguiente para continuar y mostrar el Acuerdo de licencia para el usuario final.



Leer el acuerdo de licencia para el usuario final y seleccionar la opción “Estoy de acuerdo con las condiciones del Acuerdo de Licencia” para aceptar los términos y condiciones.

Hacer clic en Siguiente para continuar.

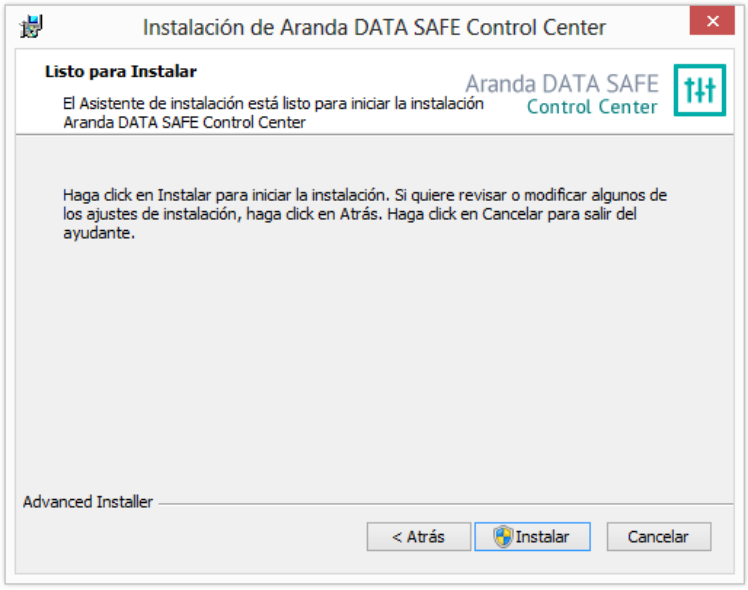


El cuadro de dialogo “Seleccione la carpeta de instalación” se visualiza mostrando una ruta por defecto.

Puede cambiar la ruta por defecto al seleccionar la opción Examinar…, donde puede navegar y seleccionar una ubicación diferente.

Luego de seleccionar la ruta por defecto o la alternativa, hacer clic en Siguiente para continuar.

La ventana “Listo para instalar” se muestra a continuación.



En esta etapa puede regresar para cambiar cualquiera de los parámetros de instalación configurados.

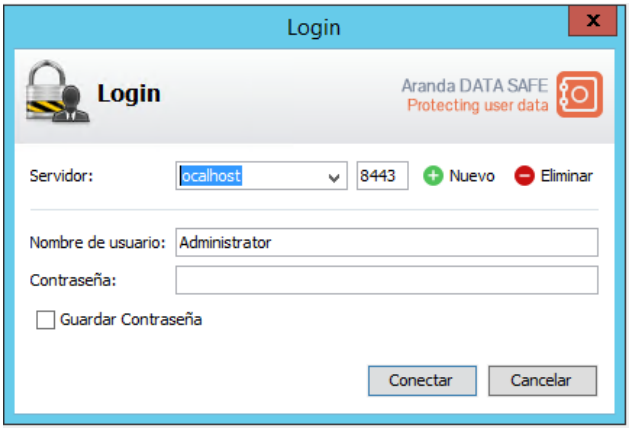
Si la configuración es la deseada para la instalación, presionar el botón Instalar para proceder con el proceso de instalación.

Se muestra el cuadro de instalación de la Consola de Administración de Aranda Data Safe. Se notificará cuando finalice la instalación de Aranda Data Safe.

Hacer clic sobre el botón Finalizar para culminar el proceso de instalación. Ha completado el proceso de instalación de la consola de administración de Aranda Data Safe.

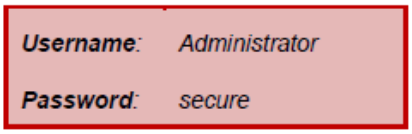
Inicio de sesión en la consola de administración

Una vez se haya completado el proceso de instalación de la consola de administración, puede iniciar sesión en el servidor de Aranda Data Safe a través de esta consola.



Para iniciar sesión en el servidor de Aranda Data Safe Ingresar el nombre del servidor o la dirección IP correspondiente del servidor de Aranda Data Safe en el campo **Servidor.** También puede seleccionar su servidor abriendo el menú desplegable.
Usar los botones de **Nuevo** y **Eliminar** para agregar o borrar servidores de la lista desplegable.

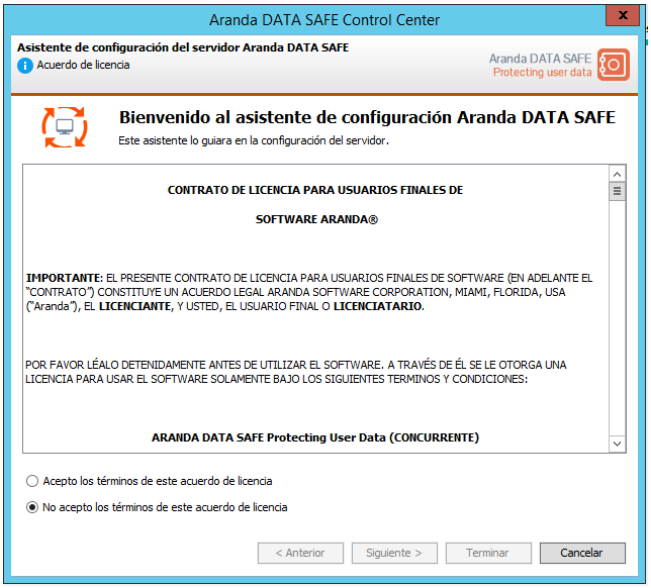
Ingresar las credenciales de usuario y contraseña y dar en el botono **Conectar** para iniciar sesión.



Nota: Esta contraseña puede ser modificada en la consola de administración.

Seleccionar el cuadro **Guardar Contraseña** si desea guardar esta contraseña para futuros inicios de sesión.

A continuación, se mostrará un cuadro de dialogo con el contrato de licencia para usuarios finales de la consola de administración. Para continuar seleccionar la opción “Acepto los términos de este acuerdo de licencia” y hacer clic en **Siguiente**.



3.4 Selección del tipo de Servidor

El servidor de Aranda Data Safe puede operar en dos modos:

- **Modo Directorio Activo – MAD**
- **Modo Independiente (StandAlone)**

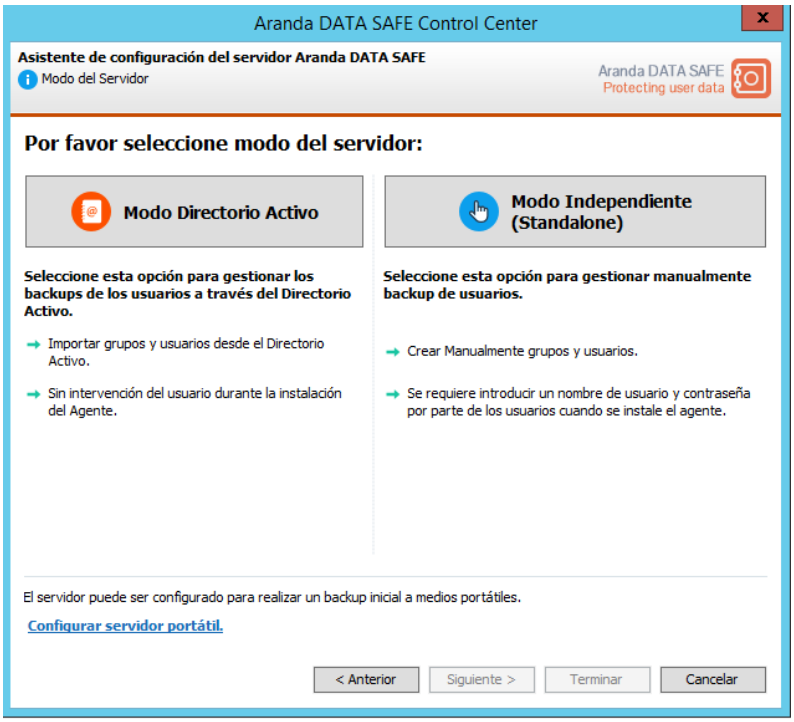
Selección del servidor en modo con Directorio Activo

El directorio activo de Microsoft es una parte integral de la arquitectura del servidor de Windows. Es un sistema centralizado y estandarizado que automatiza la administración de red de los datos de los usuarios, de seguridad, y recursos distribuidos. El directorio activo está diseñado especialmente para ambientes de red distribuidos.

El servidor de Aranda Data Safe se integra con el servicio del directorio activo e importa las unidades organizacionales (OU) seleccionadas dentro del servidor.

Los usuarios que se encuentren dentro de estas Unidades organizacionales y en grupos de seguridad, automáticamente serán agregados a estos grupos tan pronto como el agente sea desplegado en la estación del usuario final.

Los usuarios normalmente residen en Unidades organizacionales y en grupos de seguridad. Si ambos grupos de usuarios son importados en la consola de administración, aquellos usuarios en los grupos de seguridad tomaran precedencia sobre usuarios en las unidades organizacionales cuando el agente active la cuenta del usuario. Seleccionar el modo del servidor que desee usar:



Para guardar backups en dispositivos removibles, seleccionar la opción **Seleccionar servidor portátil**.

Nota: Configurar y administrar un servidor portátil no se encuentra dentro del alcance de esta guía.

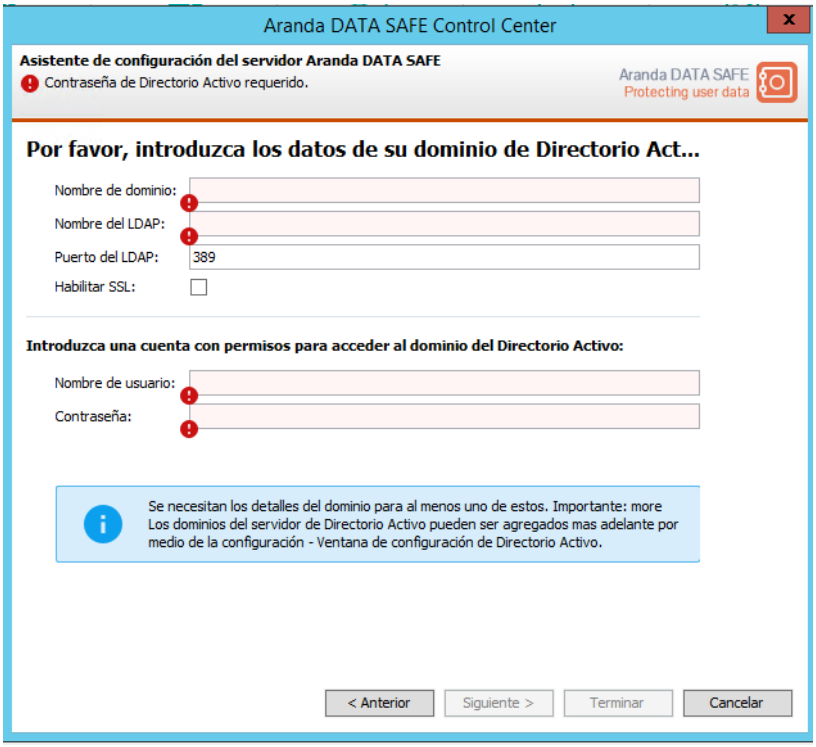
Para más detalles de esta funcionalidad, por favor revisar las notas de versión.

Hacer clic en **Siguiente** para continuar.

Al seleccionar el modo directorio activo, se solicitan las cuentas del directorio activo, las cuales son requeridas para habilitar la comunicación entre el servidor de Aranda Data Safe y los controladores de dominio. El LDAP (Lightweight Directory Access Protocol) es el protocolo estándar de acceso al directorio usado por el directorio activo.

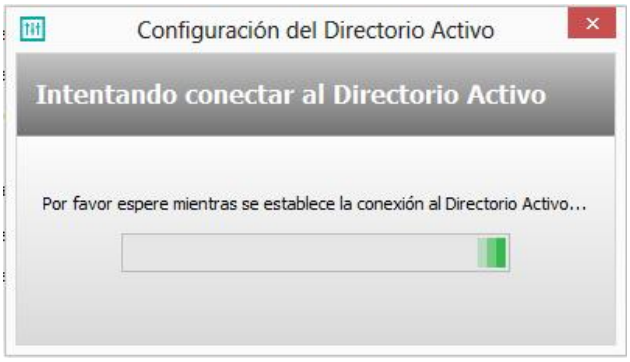
3.4.1 Configuración de los valores del directorio activo (LDAP)

Ingresar el nombre de dominio, el nombre del equipo servidor de LDAP y el puerto del LDAP. El puerto por defecto del LDAP en el TCP/389, el cual puede ser modificado sí el puerto es diferente al puerto por defecto.



Hacer clic en Siguiente para continuar.

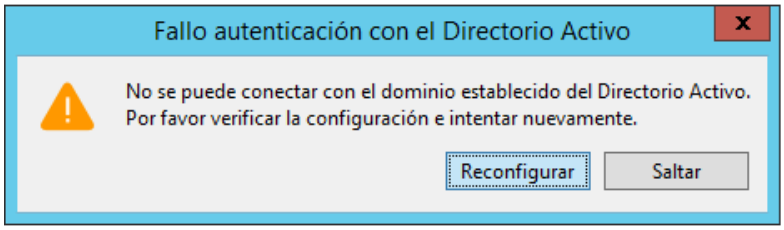
Se intentará realizar una conexión contra los servicios del directorio activo.



Si la conexión es exitosa, el proceso continuara a la selección de las Llaves de encriptación.

Sin la conexión no fue exitosa, se solicitará revisar la configuración y reintentar u omitir el proceso.

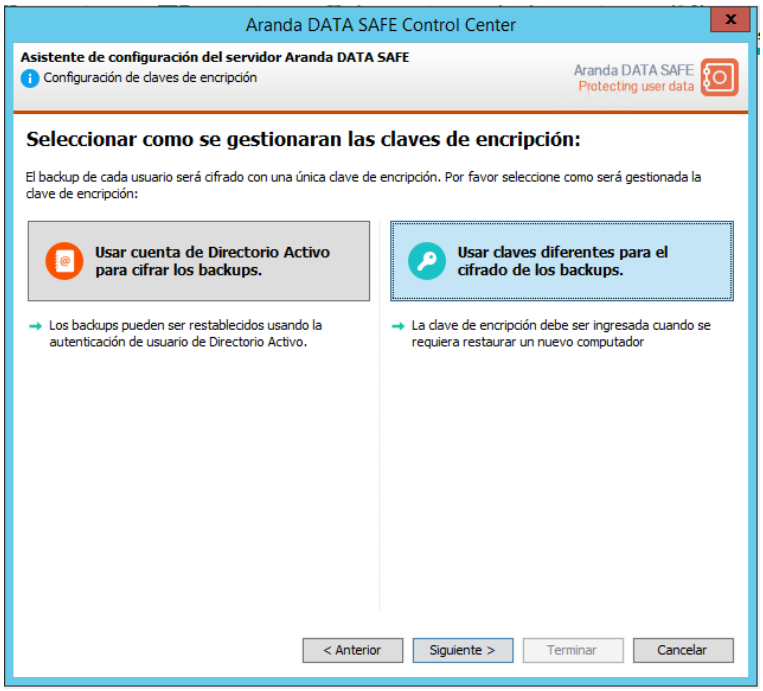
Hacer clic en Reconfigurar para verificar la configuración y reintentar, o hacer clic en Saltar para omitir este proceso y continuar a la selección de las Llaves de encriptación.



3.4.2 Selección del servidor en modo independiente (StandALone)

Los grupos y usuarios pueden ser agregados al servidor de Aranda Data Safe manualmente. Debe seleccionar esta opción si los servicios de directorio activo no están presentes en su organización.

Seleccione la opción de *Modo independiente (StandAlone)*



Para guardar backups en dispositivos removibles, seleccione la opción **Seleccionar servidor portátil**.

Hacer clic en el botón **Siguiente** para proceder y seleccionar el modo encriptación.

3.5 Selección de llaves de Cifrado

El cifrado es el proceso criptográfico, el cual mediante el uso de algoritmos se puede transformar la información, de modo que pueda ser legible únicamente para aquellas personas que tienen una llave especial. Dentro de Aranda Data Safe, esta llave es creada usando uno de tres métodos de diferentes de manejo de llaves.

Opciones de llaves de Cifrado
Las tres opciones de manejo de las llaves de cifrado disponibles son:

- Manejo de llaves a través del directorio activo.
- Manejo de llaves de cifrado separadas (Manual).
- Manejo de las llaves por cada usuario.

Manejo de llaves por directorio activo

Al usar el método de gestión de llaves por directorio activo, se genera llave de cifrado relacionada con la cuenta de usuario del directorio activo. Esta llave de cifrado no requiere ser administrada y los usuarios pueden acceder a su información siempre y cuando la cuenta exista en el directorio activo.

Nota: La gestión de llaves por directorio activo, solo se encuentra disponible al usar el modo Directorio activo al configurar el servidor de Aranda Data Safe.

Manejo de llaves separadas

El manejo separado de llaves permite que las llaves de cifrado sean creadas manualmente por los usuarios o, si es seleccionado, que sean generadas automáticamente por Aranda Data Safe y luego ser almacenadas en la caja de seguridad de llaves de cifrado del servidor.

Nota: La caja de seguridad solo puede ser ingresada por el oficial de seguridad, a quien se le confió una clave de acceso. Si el usuario quisiera restaurar su información en un nuevo equipo o ha olvidado su clave de cifrado, el oficial de seguridad está en la capacidad de recuperarla desde la caja de seguridad de llaves**.**

Manejo de las llaves por parte de los usuarios

Aranda Data Safe no realiza una administración de las llaves de cifrado con esta opción. Aunque aún es necesaria una llave de cifrado, esta debe ser creada por el usuario, quien es el único responsable.

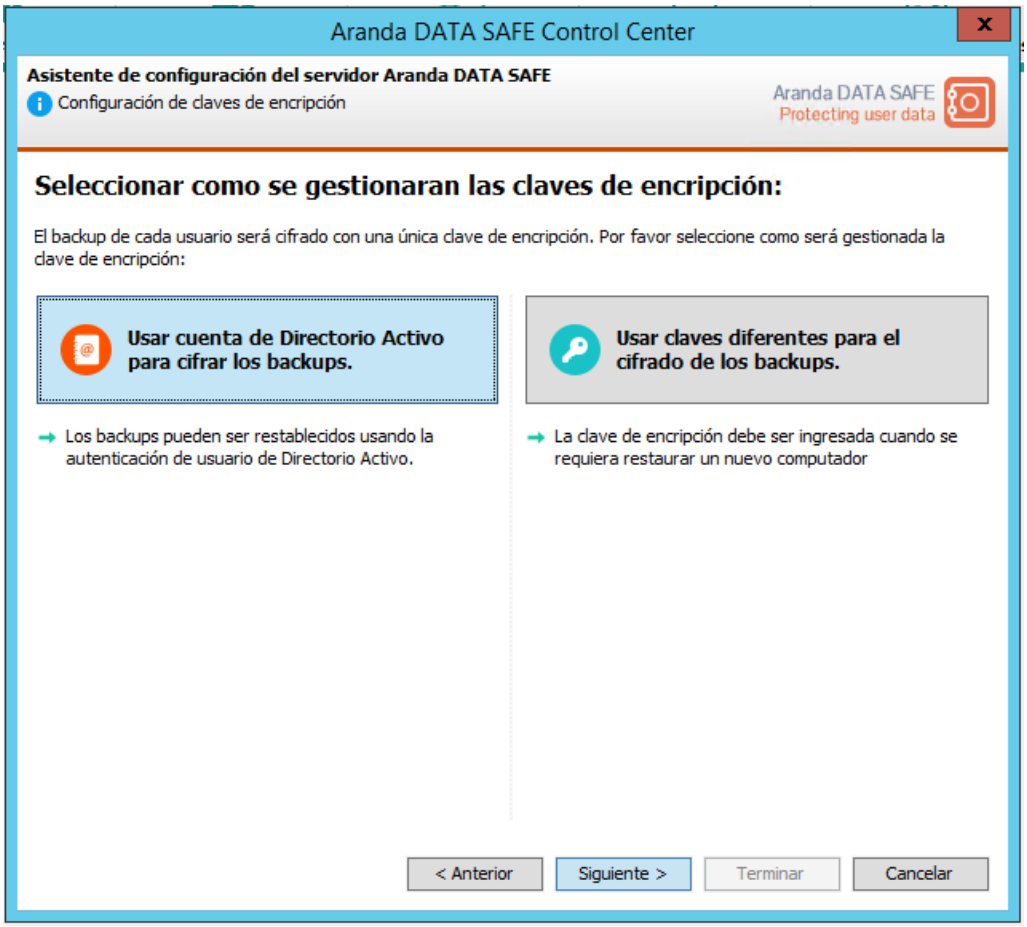
Advertencia: Sin la clave de cifrado, no se podrá acceder a la información del usuario.

Seleccionando la opción de manejo de las llaves de cifrado.

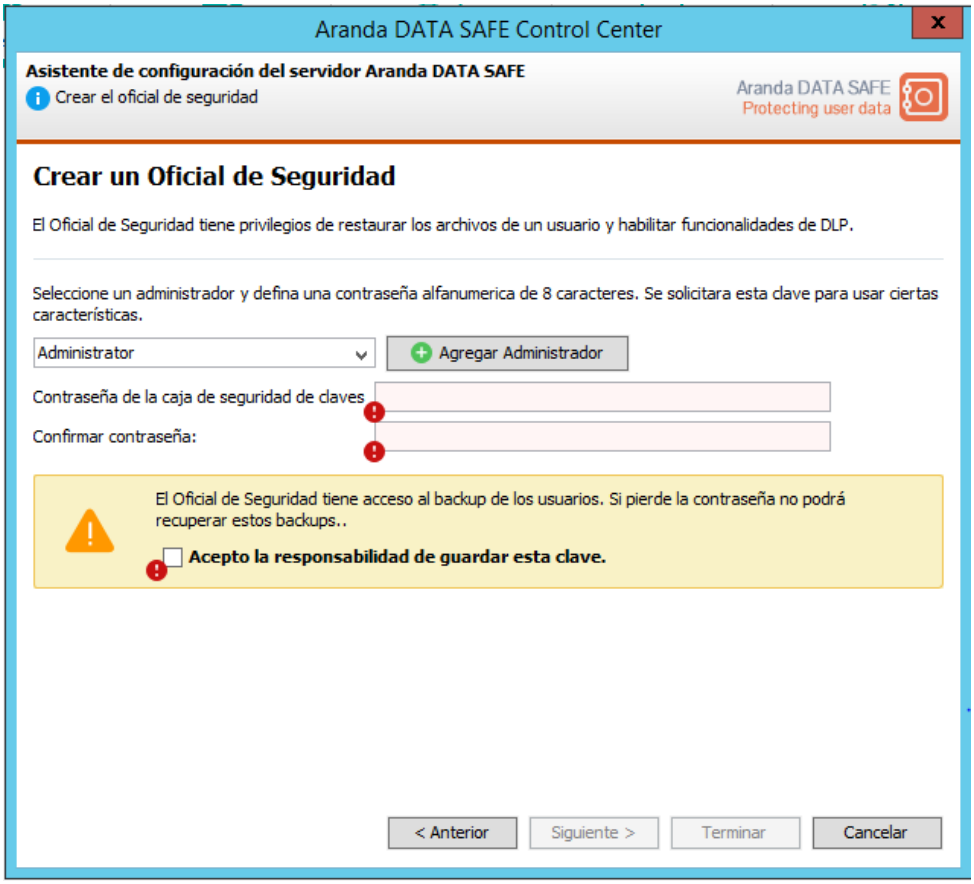
En el asistente de configuración de manejo de llaves de cifrado:

Opción 1:

Selección opción “Usar cuenta de Directorio Activo para Cifrar Backups”, presionar Siguiente.



Especificar contraseña de oficial de seguridad, y aceptar la responsabilidad.



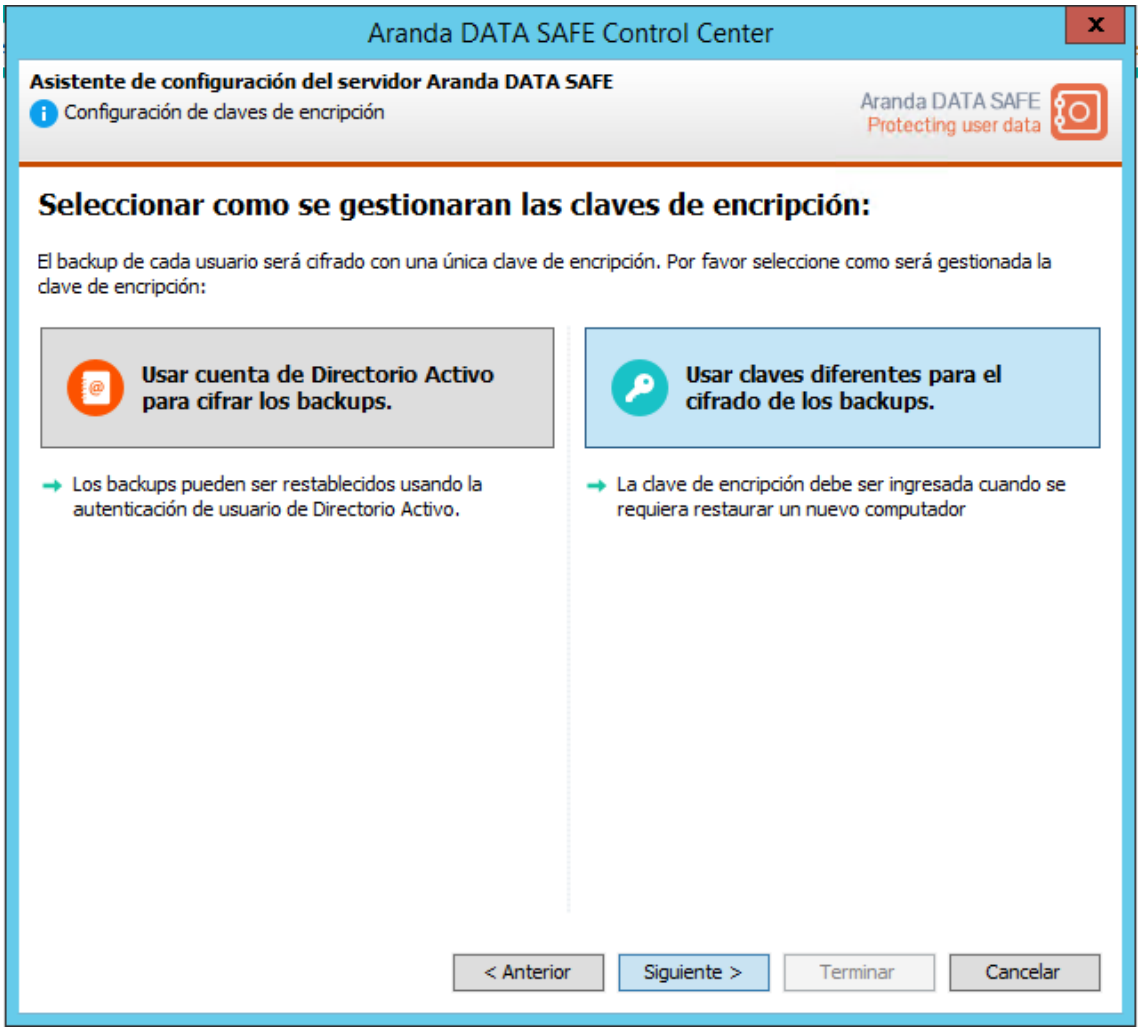
Seleccionar la opción que desea usar para gestionar las llaves de cifrado y luego hacer clic en **Terminar**. Usar cuenta de Directorio Activo para cifrar los backups.

En este ejemplo, se seleccionó el modo de integración con el servidor de Directorio Activo, por lo tanto, se selecciona la opción Usar cuenta de Directorio Activo para cifrar los backups.

Nota: No se le habilitará la opción de gestión de llaves automáticamente a menos que hubiese seleccionado el modo directorio activo para su servidor de Data Safe.

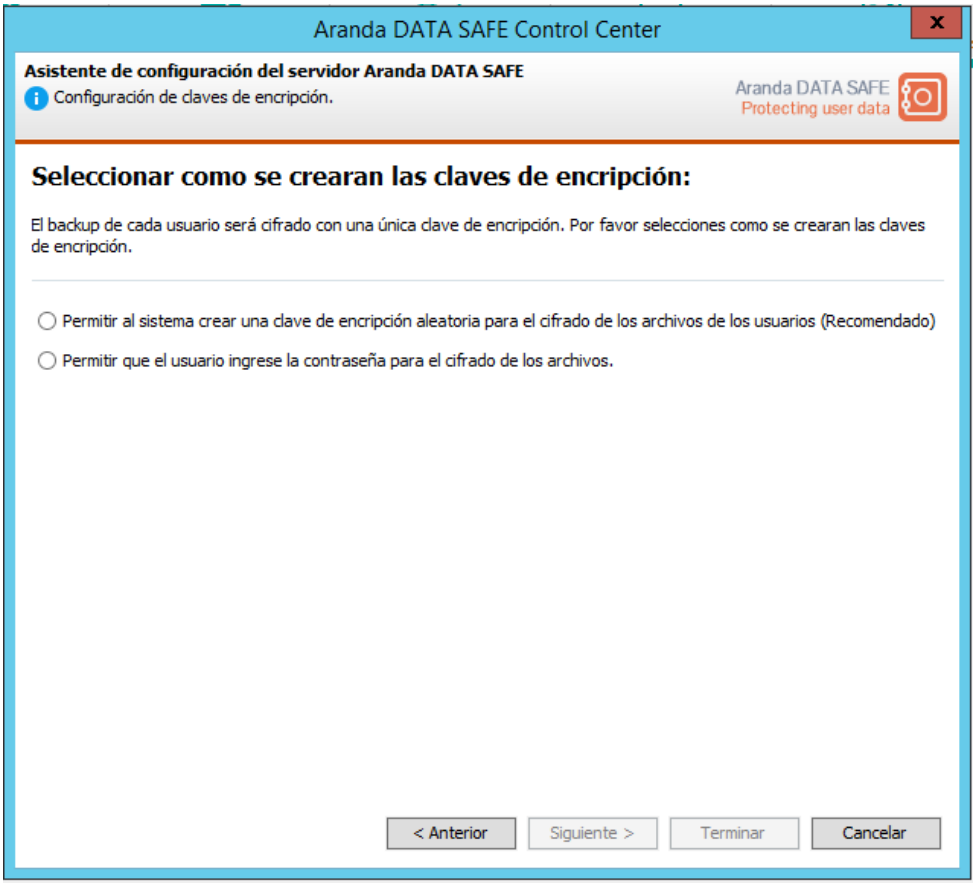
Hacer clic en el botón finalizar para continuar. Aranda Data Safe crea y aplica la llave a la cuenta del usuario.

Opción 2:
Selección opción “Usar claves diferentes para el cifrado de los backup”, presionar Siguiente.



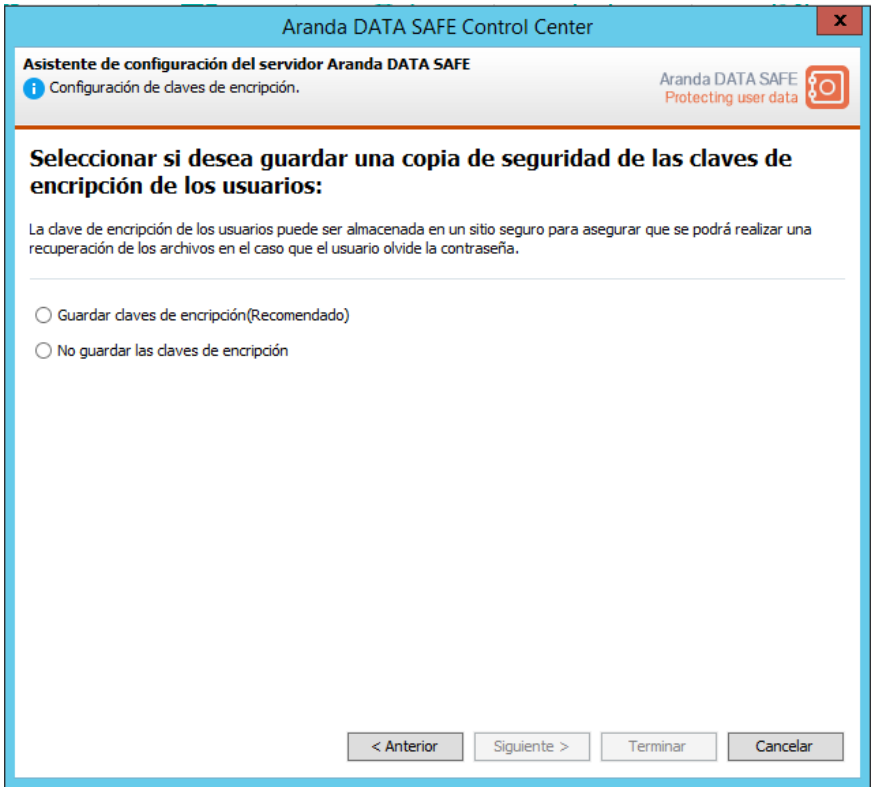
Seleccionar una de las siguientes dos opciones, y hacer clic en Siguiente para continuar.

- Permitir al sistema crear una clave de encriptación aleatoria para el cifrado de los archivos de los usuarios. Opción recomendada.
- Permitir que el usuario ingrese la contraseña para el cifrado de los archivos.



Puede seleccionar sí los usuarios mantienen sus claves de manera segura o si le permite a Data Safe guardar las claves de encriptación en la caja de seguridad.

Nota: Se recomienda que se permita guardas las claves de encriptación en la caja de seguridad de Data Safe.



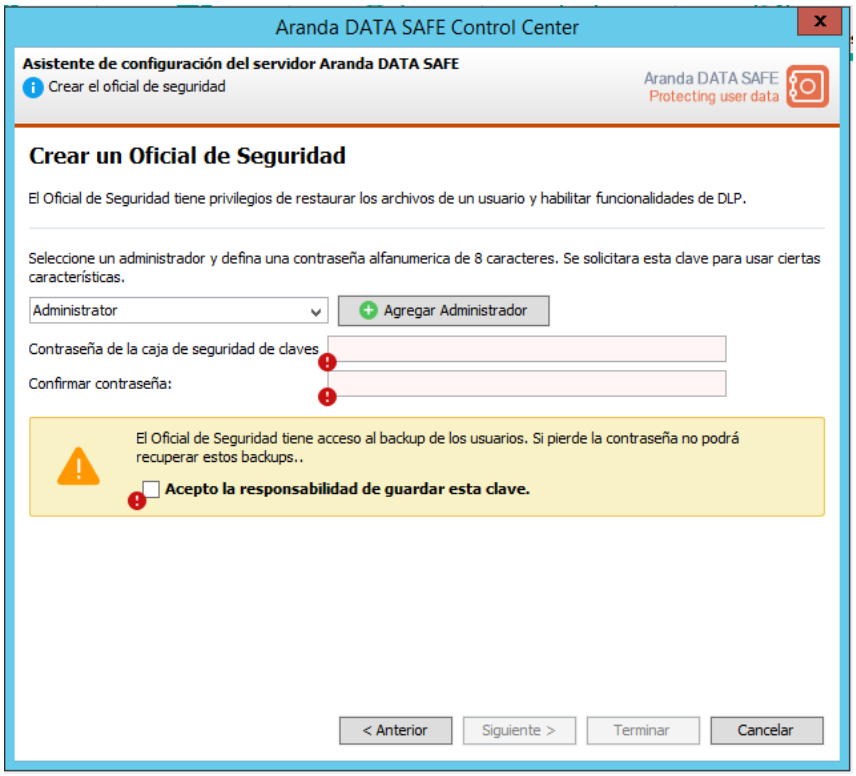
Presione Terminar para guardar sus opciones y continuar.

3.6 Oficial de Seguridad

El oficial de seguridad es la única persona autorizada para recuperar las claves de encriptación.

Recuperando claves de encriptación

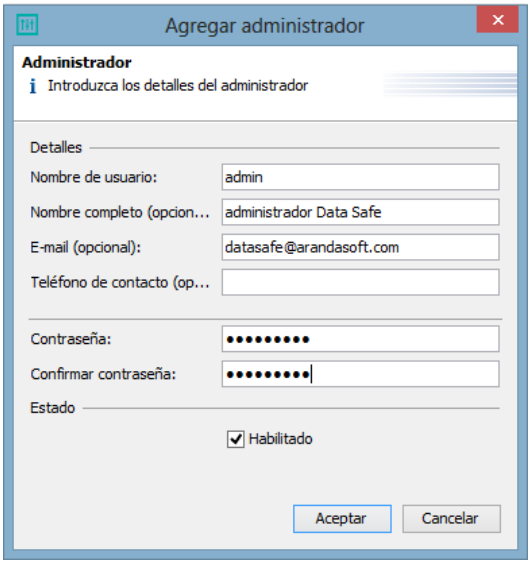
Para crear un oficial de seguridad y asignar una contraseña para la caja de llaves de seguridad se debe:



Seleccionar el usuario Administrador al cual desea designar como oficial de seguridad de la caja de seguridad e introducir una contraseña para la caja de seguridad de claves. Aceptar la responsabilidad de guardar esta clave y luego presionar Terminar para guardar y continuar.

Agregar un administrador para el rol de oficial de seguridad

En la ventana de “Crear oficial de seguridad”, existe una opción para agregar a un administrador como oficial de seguridad.
Oprimir el botón Agregar administrador para agregar un nuevo administrador de su servidor de Data Safe.



Ingresar los detalles del nuevo administrador y luego hacer clic en **Aceptar** para continuar.

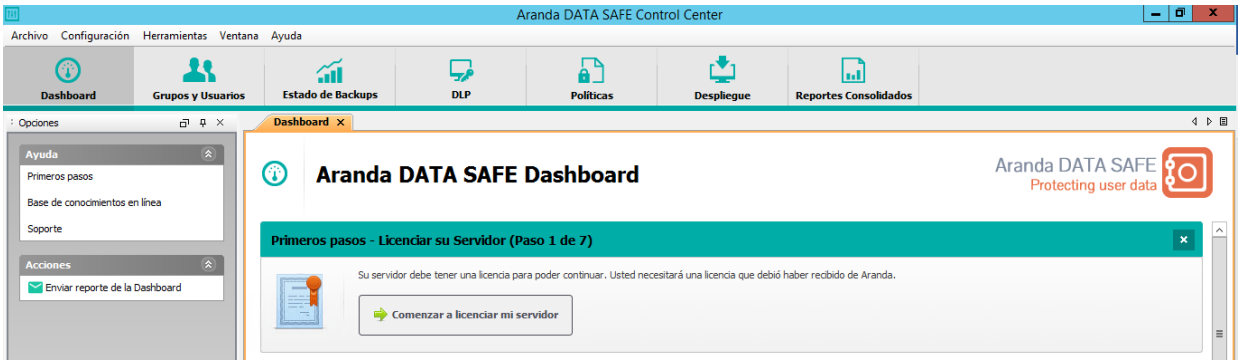
3.7 Licenciamiento servidor de Aranda Data Safe

Cada servidor de Aranda Data Safe en la solución de backup debe ser licenciado y activado. El licenciamiento inicial del servidor de Aranda Data Safe es procesado mediante el asistente de configuración de la consola de administración en Primeros pasos – Licenciar su Servidor. Los requerimientos para el licenciamiento del servidor de Data Safe son:

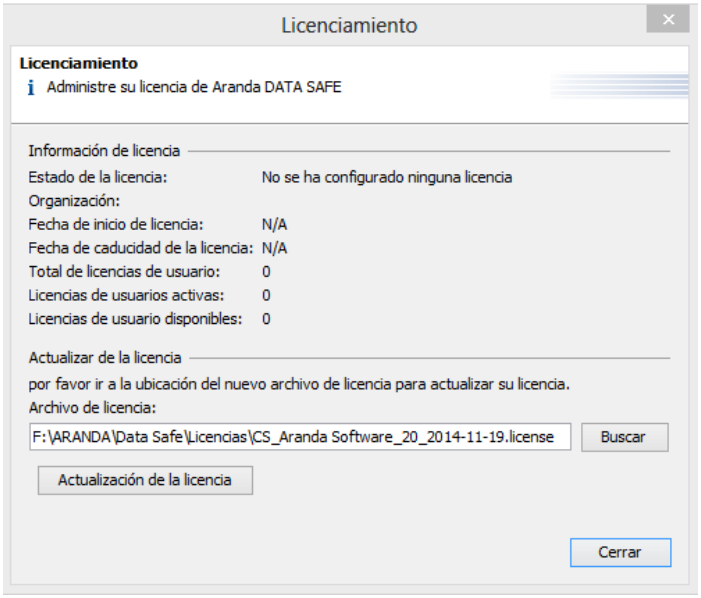
- **Licencias comerciales**. Todas las licencias comerciales requieren de una solicitud de licencia y una activación, conforme se mostrará a continuación.
- **Licencias demos o prueba**. Ya se encuentran pre activadas y no requieren de activación.

Solicitud de archivo de licencia

Para licenciar su servidor de Aranda Data Safe.



Hacer clic en el botón ***Comenzar a licenciar mi servidor*** para abrir la ventana de licenciamiento.

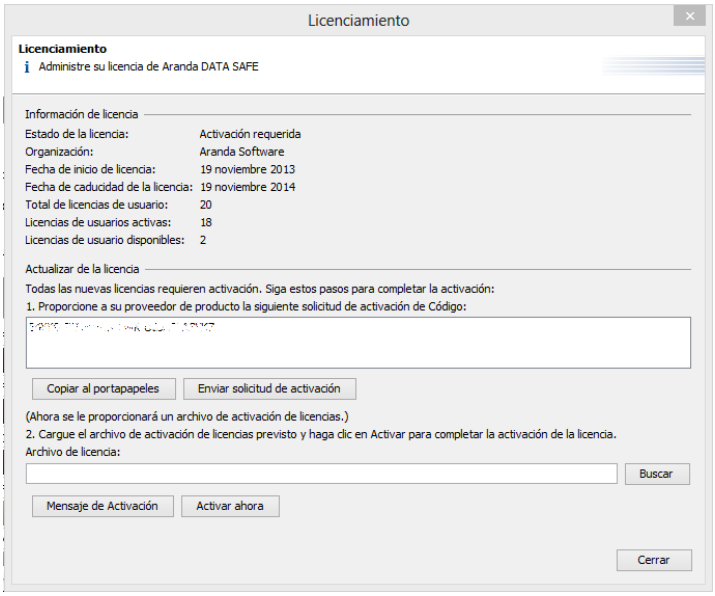


Al solicitar la licencia a través de la página de Aranda o por correo electrónico se recibirá un archivo sin activar. Si aún no tiene este archivo por favor ver Obtener licenciamiento.

Nota: El archivo de licencia tiene una extensión.license. Los archivos de licencia recibidos para demos y pruebas del producto ya se encuentran pre activados y no requerirán activación. Sí la licencia es comercial siga los siguientes pasos.

Ingrese la ruta y nombre del archivo de licencia o hacer clic en Buscar para navegar a la ubicación del archivo.

Hacer clic en Actualización de la licencia para asociar el archivo de licencia al servidor de Data Safe.



Para todas las licencias comerciales un código de activación es proporcionado.

Para solicitar la activación de la licencia desde Aranda por favor hacer clic en Enviar solicitud de activación.

Un correo electrónico será enviado al área encargada solicitando la activación de su licencia. El archivo de activación será enviado a usted por correo electrónico.

Nota: El servidor o equipo desde donde está realizando la activación debe estar en la capacidad de enviar correos electrónicos**.**

Puede copiar el código de activación, pegarlo en un correo electrónico y agregar la siguiente información:

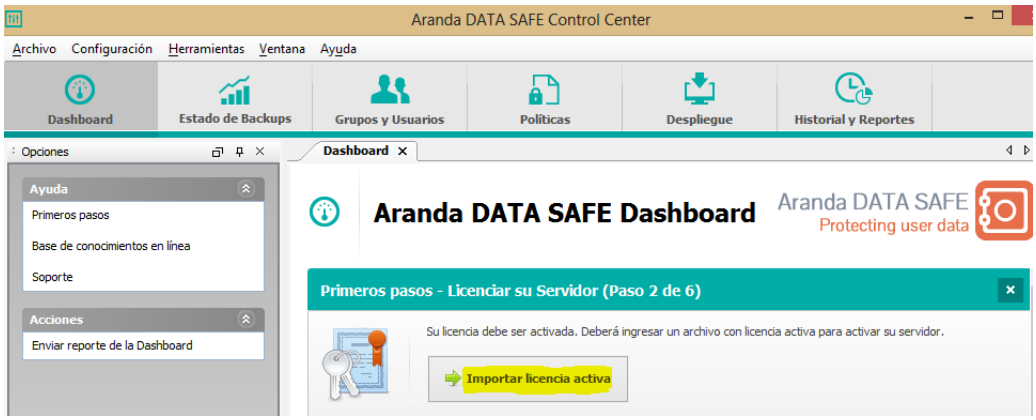
Nombre de la organización, nombre cliente y detalles de contacto. Nombre del servidor o la IP fija – Preferiblemente el nombre del equipo. Número de licencias por usuario requeridas.

Enviar la solicitud a **seriales@arandasoft.com**

Aranda le enviará el archivo de activación de la licencia como un adjunto en los días siguientes.

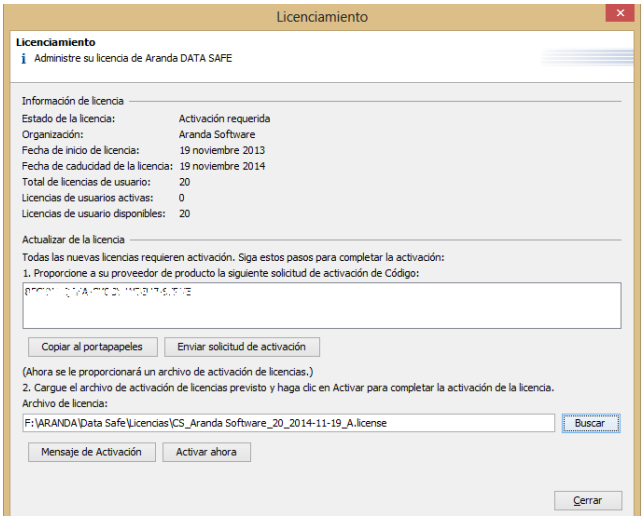
Activación de la licencia

Cuando reciba la licencia activada, deberá iniciar la consola de administración e ir al Dashboard. El asistente para licenciar su servidor automáticamente avanzara al siguiente paso – Importar licencia activa.



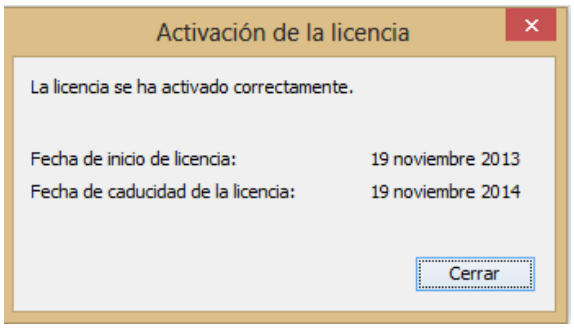
Hacer clic en el botón de **Importar licencia activa**

Ingresar la ruta del archivo de licencia o hacer clic en el botón **Buscar** para ubicar el archivo.



Hacer clic en el botón **Activar ahora** para activar la licencia del servidor de Aranda Data Safe

Si la licencia es activada con éxito, le será informado inmediatamente.



A partir de este momento ha activado satisfactoriamente la licencia del servidor de Aranda Data Safe.

Reactivación y renovación de la licencia

Las licencias pueden ser renovadas o reactivadas por una o dos razones:

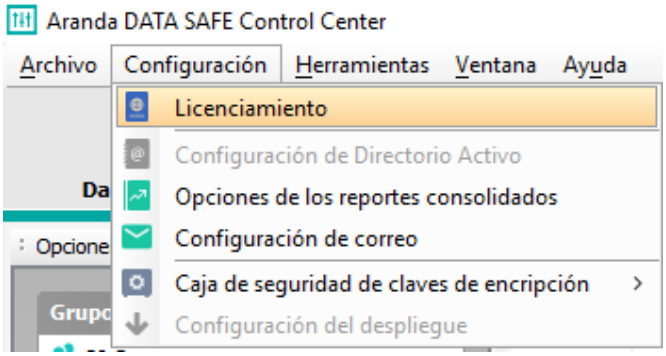
- Sí experimenta problemas con el hardware de su servidor de Data Safe y se reemplazan algunos componentes de hardware, puede ser necesario reactivar la licencia.
- Cuando su licencia caduque luego del periodo de tiempo licenciado.

Reactivación de la licencia

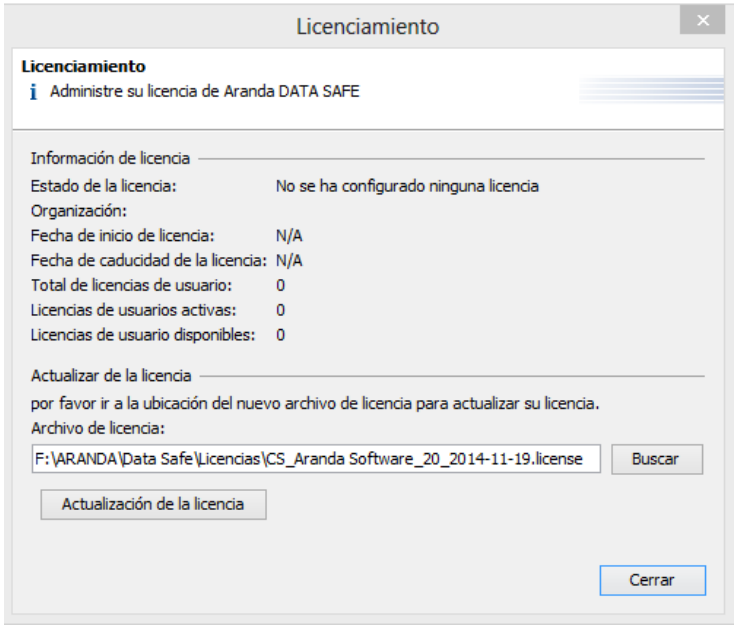
Cuando se reemplazan componentes de hardware esto requiere una reactivación de su licencia actual.

Para abrir la ventana de licenciamiento:

Seleccionar en el menú la opción **Configuración** y seleccionar la opción **Licenciamiento**.

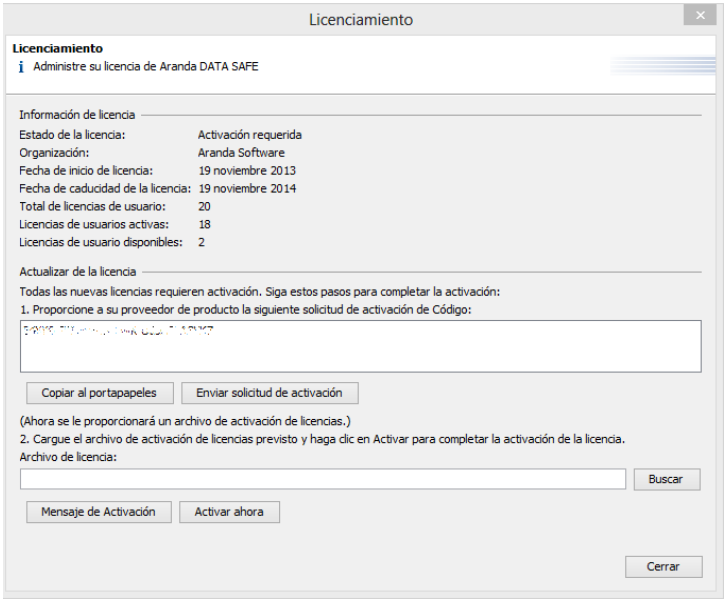


Se abrirá la ventana para licenciar el servidor.



Ingresar el archivo de licencia original o seleccione el botón **Buscar** para navegar a la ubicación del archivo.

Hacer clic sobre el botón **Actualización de la licencia** para asociar el archivo de licencia al Servidor de Data Safe.



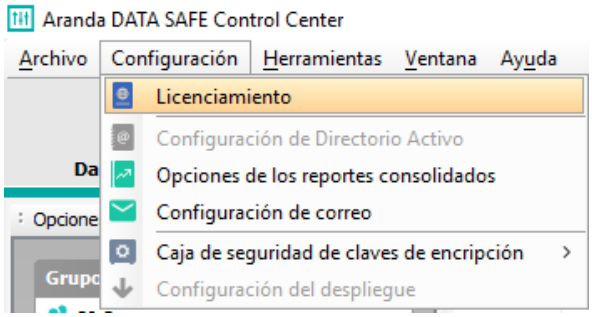
Un nuevo código de activación es generado.

Renovación de la licencia

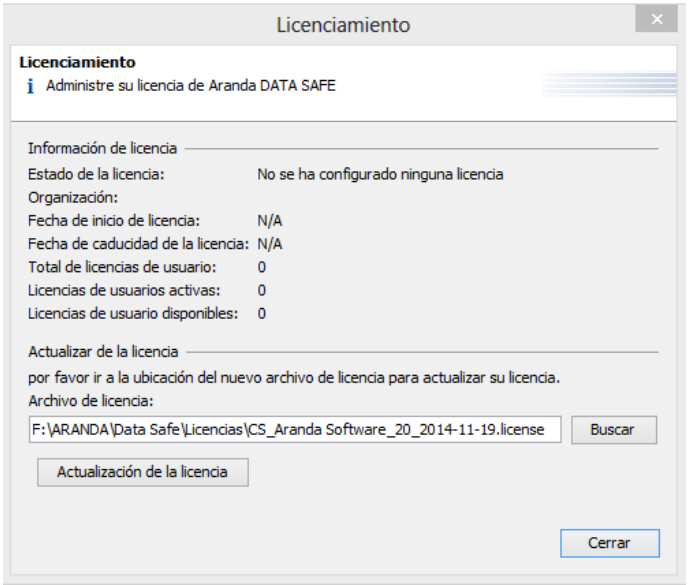
Cuando caduque su licencia deberá renovarla antes de poder continuar.

Para abrir la ventana de licenciamiento:

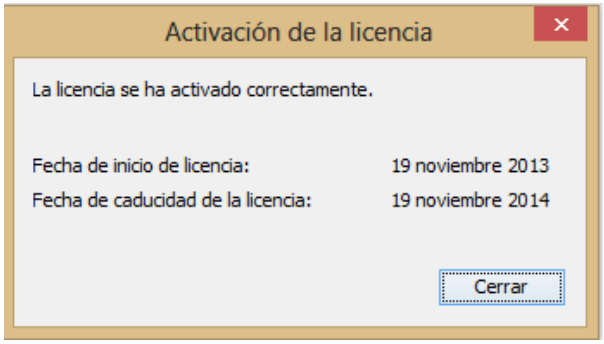
Seleccionar en el menú la opción **Configuración** y seleccionar la opción **Licenciamiento**.



Se abrirá la ventana para licenciar el servidor.



Ingresar su archivo de renovación de la licencia recibido o seleccionar el botón buscar para navegar a la ubicación del archivo. Si la licencia se cargó con éxito, se avisará en una nueva ventana.



4. Consola de administración

La consola de administración es el componente centralizado de la solución de Backup & Recovery de Aranda y es usada para controlar y administrar todos los servidores de Aranda Data Safe instalados en su organización. Los administradores de la solución pueden ejecutar muchas funciones en la consola, garantizando que la información crucial de su organización está siendo respaldada constantemente.

4.1 Creación de las políticas de Backup

Las políticas de backup son las reglas de negocio que controlan el proceso de respaldo para cada grupo o usuario asignado. Puede mantener de forma centralizada todos los elementos de un backup en la pestaña de Políticas dentro de la Consola de administración, en términos de selección de datos, programación, configuraciones generales de grupos y usuarios asignados del backup. Como administrador usted puede:

- Configurar y bloquear ciertos elementos de cada política.
- Permitir al usuario controlar y configurar ciertos elementos de su política individual.
- Las políticas de backup pueden ser asignadas a grupos enteros o usuarios individuales.
- Una política de backup asignada a un usuario individual anulará la política de backup asignado al grupo del usuario.
- Se incluyen tres políticas integradas con Aranda Data Safe.

Política incorporada por defecto: Esta política es una plantilla por defecto y no contiene ninguna de selección a realizar respaldo, horario o configuración recomendada. Usted puede utilizar esta política de backup como una plantilla para crear una nueva política y configurarla para que se adapte a sus necesidades específicas.

Usuario Ejecutivo: Esta política es una plantilla predefinida más adecuada para un usuario ejecutivo.

Hay una amplia gama de selecciones de backup predefinidas y una amplia gama de archivos excluidos globalmente, una programación automática de los backups dada para una ventana de tiempo y ajustes de configuración predefinidos

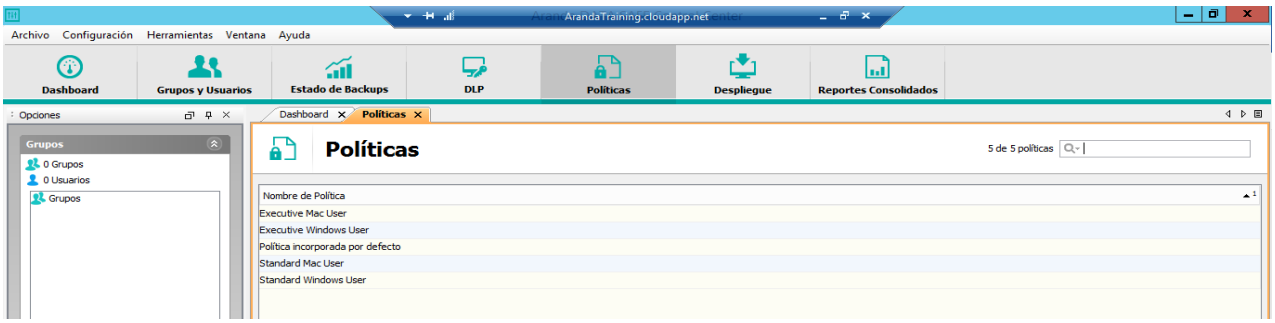
Usuario Estándar: Esta política es una plantilla predefinida más adecuada para los usuarios generales. Hay una variedad de opciones predefinidas de backup, una serie de archivos excluidos globalmente, una programación de backup predefinida en una ventana de tiempo, y configuraciones de visualización y rendimiento.

Creación de nueva política

Al crear una nueva política de backup, seleccione una de las políticas, por ejemplo, la Política incorporada por defecto y copie la configuración existente en la política definida dentro de la nueva política creada.

Para crear una nueva política o copiar una existente realice lo siguiente:

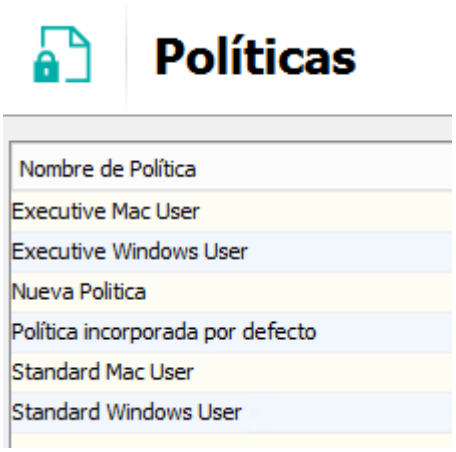
Seleccionar la pestaña de Políticas.



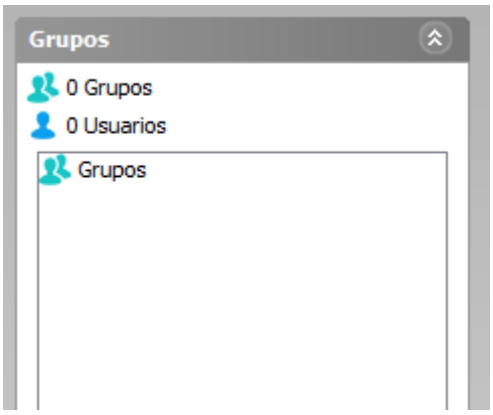
Hacer clic derecho sobre la política incorporada por defecto. Seleccionar la opción Copiar Política

Definir un nombre para la política, ejemplo – Presidencia, para la nueva política, luego hacer clic en el botón **Aceptar**

La nueva política se mostrará dentro de la lista de políticas.



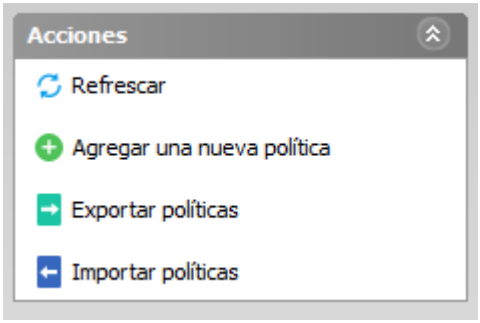
Otras opciones de las políticas están disponibles en el panel izquierdo de la ventana dentro de **Grupos** y **Acciones.**



Grupos

El panel de grupos muestra la siguiente información.

- El número de grupos y usuarios disponibles en la consola de administración
- La asignación de políticas a los diferentes grupos.



Acciones

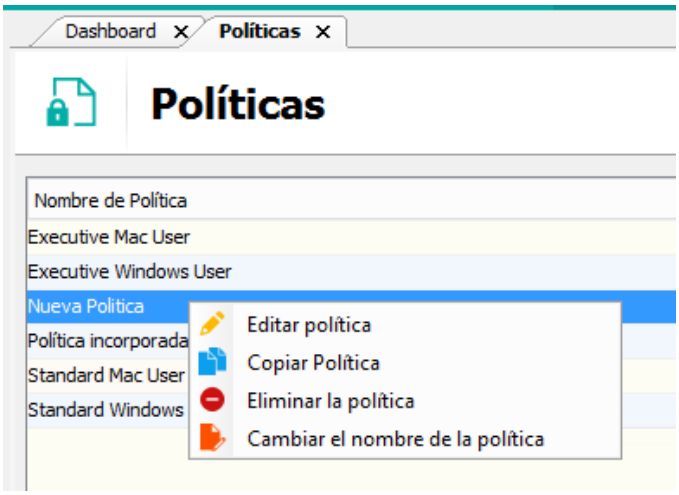
El panel de acciones dispone de las siguientes opciones.

- Refrescar.
- Agregar una nueva política
- Exportar políticas, las cuales pueden ser importadas en otro servidor de Data Safe.
- Importar políticas.

Nota: Exportar e importar políticas es conveniente cuando tiene múltiples servidores de Data Safe.

Configurando la política de Backup

Seleccionar la política “Data Safe” creada previamente.



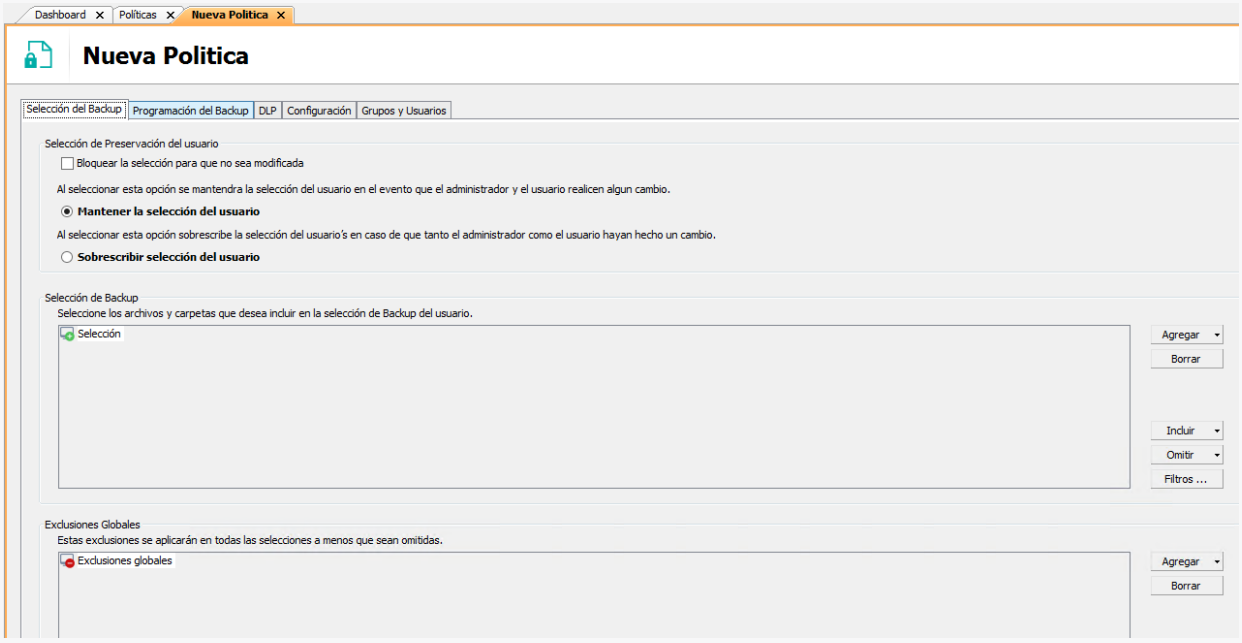
Hacer clic derecho y seleccionar **Editar política** para poder comenzar a configurar esta política.

La ventana de las políticas consiste en 5 pestañas usadas para definir y configurar los diferentes elementos de cada política:

- Selección del Backup: Seleccionar la información que será respaldada en los backups
- Programación del Backup: Definir los horarios para la automatización de los procesos de backup.
- DLP (Data Loss Prevention): Configurar acciones de Cifrado, prevención ante perdida de datos y geolocalización de la estación.
- Configuración: Opciones de configuración, notificaciones y rendimiento.
- Grupos y usuarios: Asignar grupos o usuarios a las políticas de backup.

Selección del Backup

La pestaña de selección de los backups permite escoger la información que se respaldará.



- Cuando todos los elementos hayan sido definidos, hacer clic en **Guardar** en el panel de *opciones de edición de políticas*.
- Para guardar los cambios como una nueva política hacer clic en **Guardar como nuevo** e ingrese un nombre para la nueva política.

- Hacer clic en **Deshacer** para devolver los cambios realizados.

Nota: Puede descartar los cambios realizados a una política antes de aplicar los cambios. Una vez los cambios han sido aplicados, no se pueden deshacer.

Selección de preservación del usuario

Las políticas pueden ser gestionadas tanto en la consola de administración como en el agente de usuario, lo que podría causar un conflicto cuando se realizan cambios.

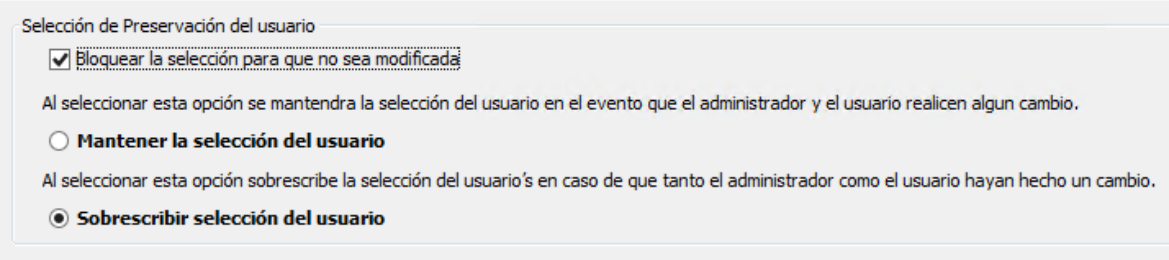
La opción de Selección de Preservación del usuario en la consola evita este conflicto cuando el administrador hace que cualquier cambio de la política.

Existen las siguientes opciones cuando se definen los permisos:

- Bloquee la selección para que no sea modificada. Seleccionar esta opción para prohibir cualquier cambio en el agente del usuario.

- Mantener la selección del usuario. Seleccionar esta opción para conservar los ajustes realizados en el agente del usuario en el caso que se realicen cambios en la consola de administración.

- Sobrescribir la selección del usuario. Seleccionar esta opción para sobrescribir los ajustes realizados en el agente del usuario cuando se realizan cambios en la consola de administración.



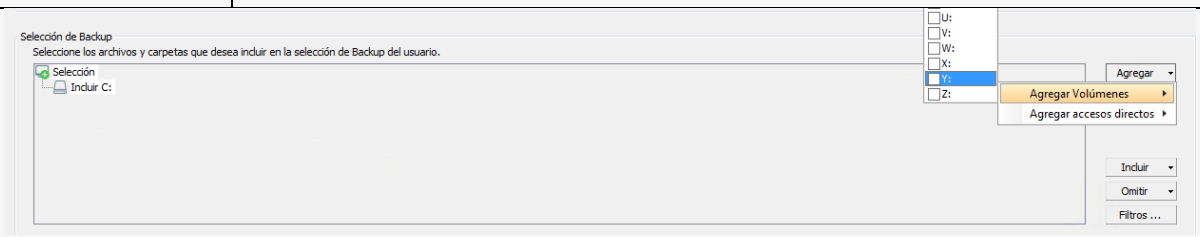
La imagen anterior muestra la selección del backup en un estado de bloqueo y sobrescrito, el cual prohibirá que el usuario cambie la selección del backup.

Selección del Backup

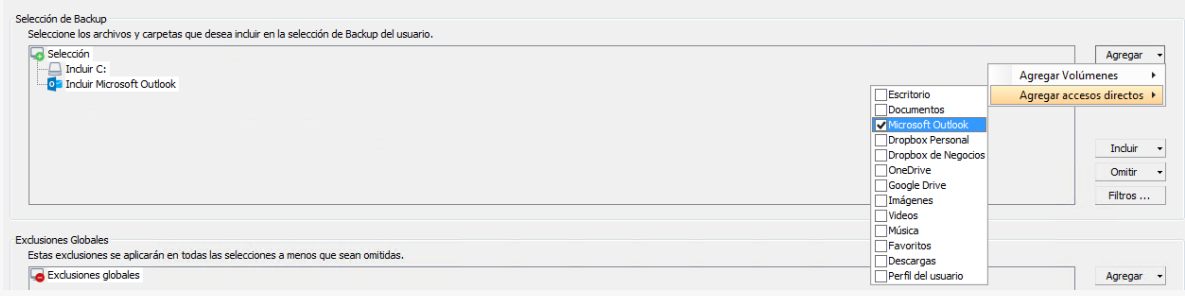
La selección del backup se puede configurar usando los siguientes criterios:

- Accesos directos predefinidos. Los accesos directos están incorporados por defecto, donde se tienen predefinidos filtros de archivos y carpetas para plataformas Windows.
- Volúmenes de disco. Estas son las referencias lógicas a unidades físicas.
- Expresiones de archivos y carpetas. Estos son los criterios de selección de archivos y carpetas específicas definidas por el usuario mediante un enfoque usando comodines (Wildcards).
- Filtros de extensiones de archivos. Estas son las selecciones basadas en extensiones de archivos para los distintos tipos de archivos.

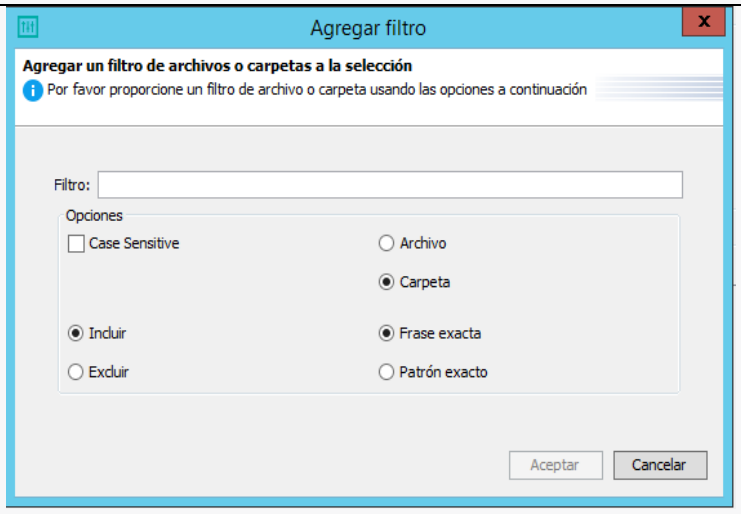
La siguiente lista de características describe las opciones disponibles para definir la selección del backup.

Característica	Opción	Descripción
Agregar Volúmenes	Usar esta opción para agregar los diferentes volúmenes de disco.	
		
	Any Volume	La opción de Any Volume dicta que cualquier volumen fijo de la A: a la Z: disponible en el equipo será incluido en la selección. • Al escanear volúmenes enteros, el agente de usuario es capaz de escanear el diario NTFS para archivos nuevos o modificados. Esto reduce el tiempo de exploración de volúmenes completos de minutos a segundos. • Los datos ocultos de la papelera de reciclaje, así como todos los datos en unidades flash, las acciones de CD-ROM y la red no están respaldados.

	Volúmenes Seleccionados	Los volúmenes seleccionados dictan que la información contenida en cualquiera de los volúmenes seleccionados debe ser incluida. • Los archivos y/o carpetas deben ser seleccionados en los volúmenes para evitar que los usuarios inadvertidamente incluyan los discos enteros.
Agregar Accesos directos	Utilice esta función para incluir cualquiera de los accesos directos predefinidos para las selecciones de backup. La opción de acceso directo respalda los archivos y carpetas de sus ubicaciones predeterminadas	

Característica	Opción	Descripción
Agregrar Accesos directos	Utilice esta función para incluir cualquiera de los accesos directos predefinidos para las selecciones de backup. La opción de acceso directo respalda los archivos y carpetas de sus ubicaciones predeterminadas	
		
	Outlook	Las carpetas personales de Outlook activos (. PST de) están incluidos. Lo que hace Outlook es realizar un cambio a todos los archivos PST activos cada vez que este es abierto y normalmente hace que los archivos PST sean marcado como modificado, a pesar de que no haya cambios a nivel del correo electrónico. Esta traerá como resultado que se realice un backup del PST innecesariamente.

		C cuando se utiliza el acceso directo de Outlook, los archivos PST son supervisados, revisando los cambios que ocurren en los mensajes de correo electrónico, entradas del calendario, notas y tareas dentro del archivo PST y sólo marcan un archivo PST para ser respaldado cuando genero un cambio real en este. Esto puede reducir significativamente los tiempos de backup. También se incluyen en el backup los archivos de la firma de Outlook y Autocompletar NK2 del usuario ubicados en los archivos de cache.
	Perfil del usuario	Las carpetas y los archivos de los perfiles seleccionados que se encuentran en la carpeta de perfil del usuario C:\Users\<nombre del usuario>\ están incluidos.
	Escritorio	Solo archivos y carpetas que se encuentren en el escritorio del usuario son incluidos en el backup
	Descargas	Todos los archivos descargados que se encuentran en la carpeta de descargas están incluidos
	Favoritos	Todos los favoritos de internet Explorer están incluidos
	Documentos	Solo carpetas y archivos que se encuentren en la carpeta Documentos/Mis documentos será incluidos
	Música	Todos los archivos de música que se encuentren en esta carpeta serán incluidos
	Imágenes	Todas las imágenes que se encuentren dentro de la carpeta imágenes serán incluidas
	Videos	Todas los videos que se encuentren dentro de la carpeta videos serán incluidas

<table>
<tr><td colspan="2">Borrar</td><td>Hacer clic en el botón Borrar que se encuentra adyacente al panel de selección quitara el elemento seleccionado</td></tr>
<tr><td colspan="2">Incluir/Excluir</td><td>Hacer clic en el botón incluir adyacente al panel de selección incluirá o excluirá el elemento seleccionado de manera local</td></tr>
<tr><td>Omitir</td><td>Omitir Exclusiones</td><td>Hacer clic en el botón ignorar adyacente al panel de selección para seleccionar las exclusiones globales a ser ignoradas.
Nota: Las exclusiones globales serán discutidas más adelante</td></tr>
<tr><td>Filtros</td><td>Agregar & Borrar Filtros
Agregar & Borrar extensiones
Mayúsculas/ minúsculas</td><td>La opción de filtros es usado para agregar nuevas o borrar existentes filtros de archivos y sus respectivas extensiones</td></tr>
<tr><td>Agregar Carpetas/Archivos</td><td colspan="2">La opción de Agregar es usada para agregar archivos o carpetas de un volumen o un acceso directo usando patrones exactos o similares.</td></tr>
<tr><td></td><td>Filtro</td><td>Introduzca una expresión en el campo Filtro de las carpetas o archivos específicos a respaldar dondequiera que residan en el volumen seleccionado.</td></tr>
<tr><td></td><td></td><td> 
</td></tr>
</table>

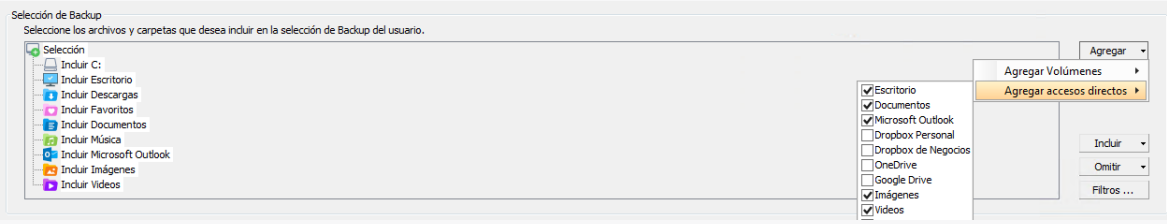
	Case Sensitive	Esta opción es seleccionada para indicar si el contenido del filtro se diferencia de mayúsculas y minúsculas o no. Esto puede ser importante cuando se requieren coincidencias exactas de los filtros.
	Archivo/Carpeta	Selección para indicar si el filtro representa un archivo o una carpeta.
	Incluir o excluir	Selección para indicar si el archivo o carpeta debe ser incluido o excluido.
	Frase exacta o patrón exacta	Selección para indicar si el filtro es una coincidencia exacta o un patrón exacto. Los patrones permiten usar expresiones. Un ejemplo sería si el nombre exacto del archivo o carpeta no se conoce, y una parte del nombre se utiliza junto con un símbolo de comodín para realiza el respaldo de cualquier archivo o carpeta que coincida con el patrón definido.

Aplicando accesos directos a la selección del backup

Microsoft Windows es a menudo la plataforma de elegida para muchas organizaciones y, por esta razón Aranda Data Safe ha incluido accesos directos predefinidos que ayudan a definir la selección del backup. Para agregar accesos directos a la selección del backup:

Hacer clic en el botón Agregar junto al panel de selección del backup.

Mover el puntero del ratón sobre la opción de agregar accesos directos mostrados a continuación, seleccionar cualquiera de las casillas de verificación de acceso directo disponibles que sean requeridas.

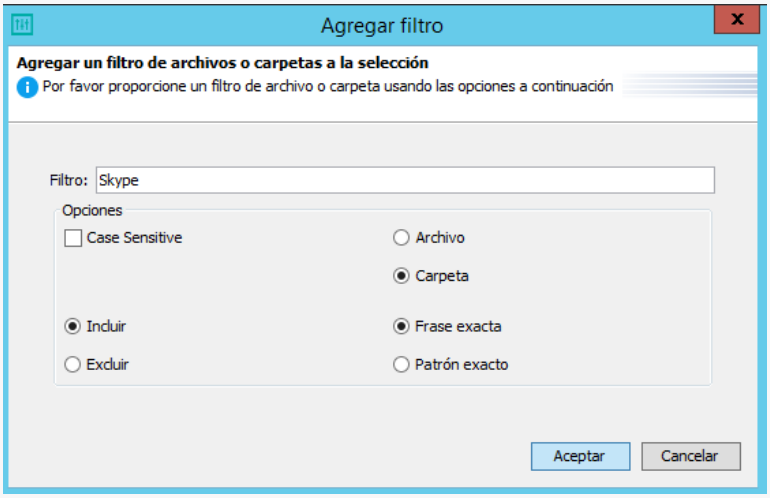


Los siguientes accesos directos adicionales están disponibles.

- Música, Videos, Descargas, Imágenes.

- El acceso directo del perfil de usuario también está disponible para realizar los backups en donde se encuentra la información contenida dentro del perfil de usuario. La ruta de acceso de los perfiles de usuario en:
- Windows Vista, Windows 7 o Windows 2008 se encuentra en el directorio C:\Users\<Carpeta con el Nombre del Usuario>.
- Windows XP o Windows 2003 se encuentra en el directorio.
- Accesos directos de aplicaciones de almacenamiento en nube como Dropbox, One Drive y Google Drive.

C:\Documents and Settings\<Carpeta con el Nombre del Usuario>. Usted puede proporcionar los detalles del perfil en términos de un filtro de archivo/carpeta específico. Por ejemplo, escriba la palabra de Skype en el campo Filtro para realizar un backup de la carpeta de configuración de Skype y el historial de conversaciones.



Eliminar accesos directos

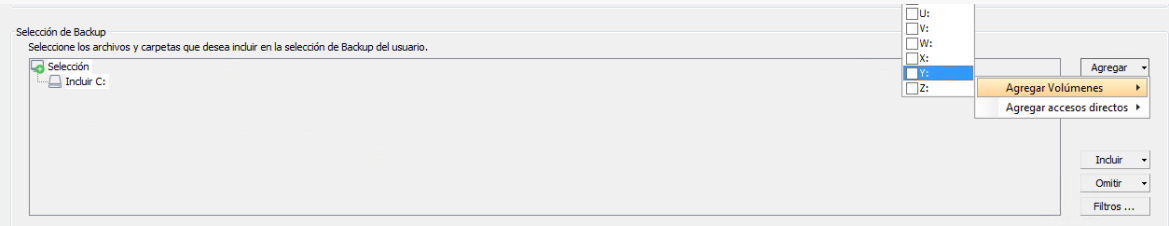
Para borrar un acceso directo: Seleccionar el acceso directo a eliminar, y hacer clic sobre el botón **Borrar** junto al panel de selección de Backup.

La entrada será borrada.

Agregar volúmenes de disco a la selección del backup

La información que requiera ser respaldada y no reside dentro de los accesos directos predefinidos, puede ser seleccionada mediante la inclusión de un volumen de disco y añadiendo las carpetas, Archivos y filtros pertinentes.

Para agregar volúmenes a la selección del backup: Hacer clic sobre el botón Agregar junto a la ventana de selección del backup.



Seleccionar la opción Agregar Volúmenes y luego seleccionar los volúmenes de disco que desde incluir.

Seleccionar los volúmenes específicos requeridos o seleccionar la casilla Any Volume para automáticamente agregar todos volúmenes disponibles.

Hacer clic fuera del cuadro para cerrar las opciones.

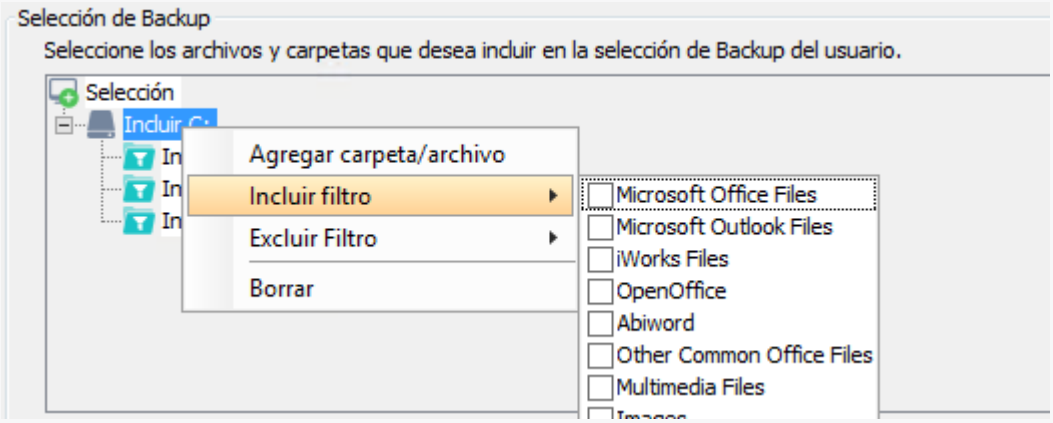
Nota: Sí no agrega los criterios requeridos para un volumen, el volumen será ignorado y no se realizará backup.

Eliminar un volumen

Para eliminar un volumen de disco debe realizar lo siguiente: Seleccionar el volumen que desee borrar. Seleccionar el botón **Borrar** junto al panel de la **Selección de Backup.** La selección será eliminada.

Agregar archivos y carpetas en accesos directos o volúmenes

Archivos y carpetas adicionales pueden ser agregados a los volúmenes y los accesos directos seleccionados. Estos se pueden agregar utilizando las opciones de filtro para incluir o excluir archivos y carpetas específicos como se describe en la siguiente característica.

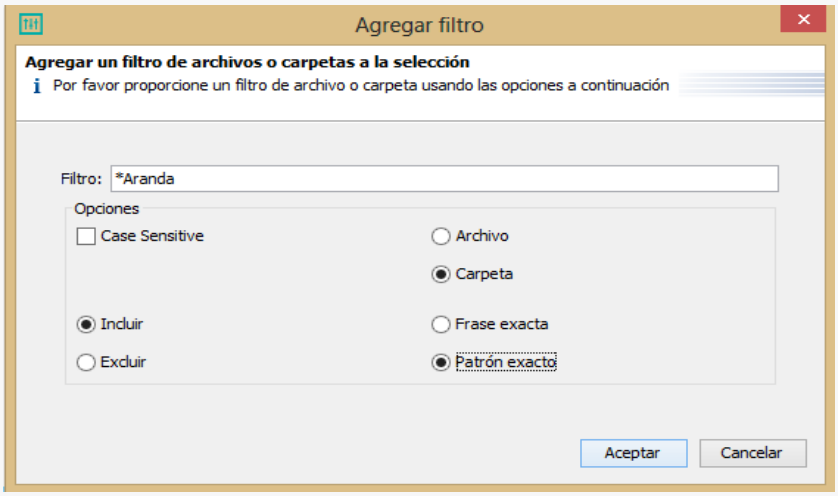


Hacer clic en Agregar carpeta/archivo.

Ingresar la expresión a buscar en el cuadro de dialogo Filtros. Seleccionar la opción Archivo o Carpeta, Incluir o Excluir y Frase exacta o Patrón Exacto. Para finalizar, selección o no la casilla de Case Sensitive para diferenciar entre mayúsculas y minúsculas.

El siguiente proceso es un ejemplo de patrón exacto y muestra cómo agregar cualquier carpeta que termina con la palabra "Aranda" para la selección del backup en el volumen C.

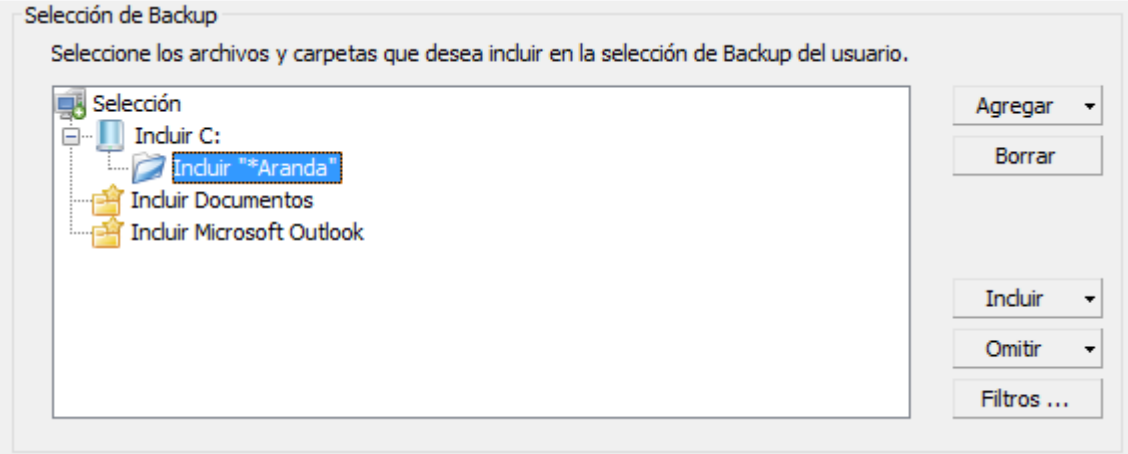
Supongamos que existen diferentes carpetas, como "ArandaSoft", "Aranda", o "Software Aranda" y desea hacer backup de esas carpetas específicas.



Ingresar el carácter * como comodín seguido de la palabra Aranda. Seleccionar las opciones de Carpeta, Incluir y Patrón exacto.

Nota: Como regla, se recomienda que siempre seleccione la opción de patrón exacto cuando utilice el carácter (*) como comodín.

Hacer clic en Aceptar para agregar el archivo o carpeta en la selección del backup.



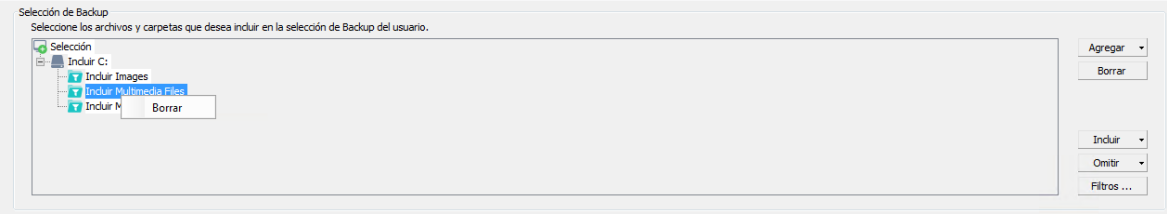
Hacer clic en la opción Guardar en el panel de opciones de edición de Política para guardar el cambio.

Ejemplos del uso del carácter comodín (*) para definir patrones alternativos:

Expresión	Descripción	Ejemplo
*Patrón	Cualquier archivo o carpeta cuyo nombre termine con el patrón definido será seleccionado	Incluir o Excluir archivos, tal como "Software **Aranda**.doc", "Data Safe **Aranda**.xls", etc.
Patrón*	Cualquier archivo o carpeta cuyo nombre comience con el patrón definido será seleccionado	Incluir o excluir archivos, tal como "**Aranda** Software.doc", "**Aranda** Data Safe.xls", etc.
Patrón	Cualquier archivo o carpeta cuyo nombre contenga el patrón definido será seleccionado	Incluir o excluir archivos, tal como "**Aranda** Software.doc", "Data Safe **Aranda**.xls", etc.

Borrar archivos o carpetas

Para borrar un archivo o una carpeta usted debe: Seleccionar la entrada incluida a borrar.



Seleccionar el botón **Borrar** junto al panel de la Selección de Backup. La selección será eliminada. O clic derecho sobre la Selección que desea eliminar y **Borrar.**

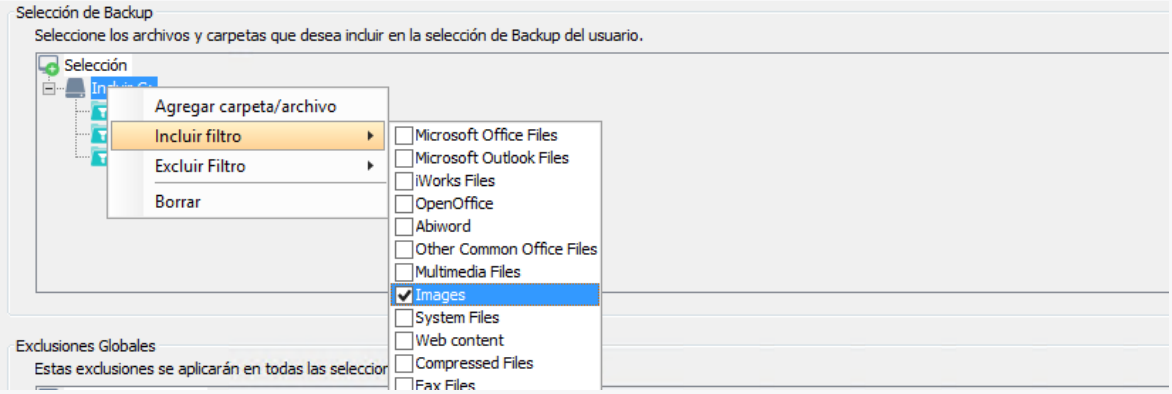
Agregando filtros de extensiones a accesos directos, volúmenes y carpetas. Las grandes organizaciones a menudo sólo requieren respaldar archivos con determinadas extensiones.

- Los filtros de extensión se utilizan para incluir los datos críticos del negocio como Microsoft Word, Excel, etc.
- Los Filtros de extensión también pueden utilizarse para excluir los datos que pueden no ser necesarios, como archivos multimedia, etc.

Se han predefinido Filtros de extensión comunes dentro de la herramienta. También puede definir sus propios filtros de archivos, si es necesario. Consultar Definición de filtros de extensión personalizados.

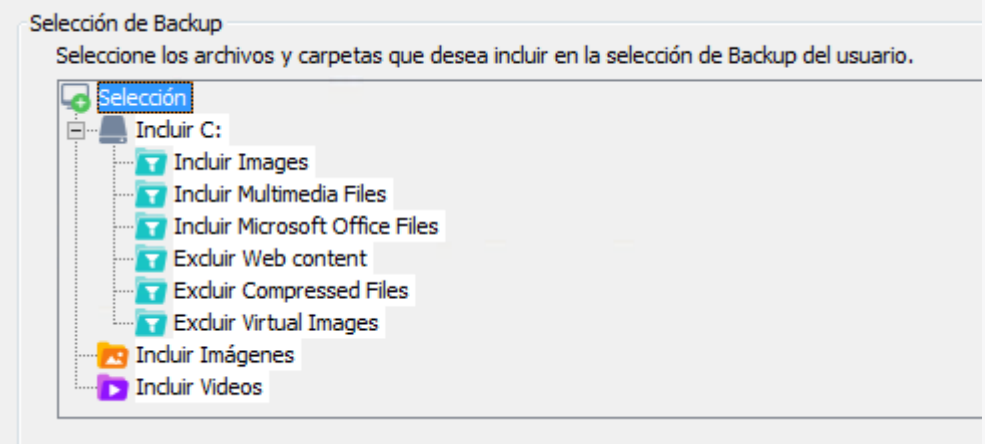
Para agregar filtros de extensión en volúmenes y carpetas debe:

Hacer clic derecho sobre un volumen o una carpeta



Ubicar el puntero sobre cualquiera de las dos opciones **Incluir filtro** o **Excluir filtro** para mostrar un menú contextual de los filtros de extensión disponibles ya predefinidos. Seleccionar cada acceso directo que desea incluir en la selección.

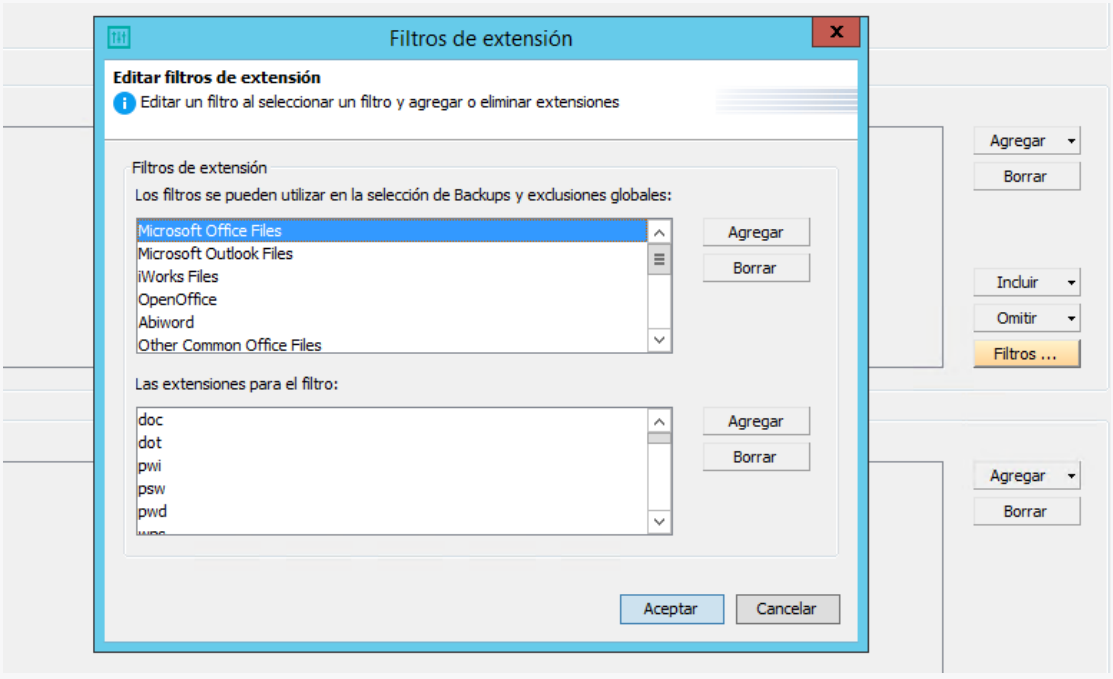
Nota: Sí se agrega un filtro de inclusión dentro de un acceso directo, volumen o carpeta, sólo se incluirán los archivos de las extensiones seleccionadas. Se excluirán todas las otras extensiones. O sí se agrega un filtro de exclusión, serán excluidos sólo los archivos de esa extensión seleccionada y todas las demás extensiones serán incluidas. Hacer clic fuera del cuadro para cerrar las opciones.



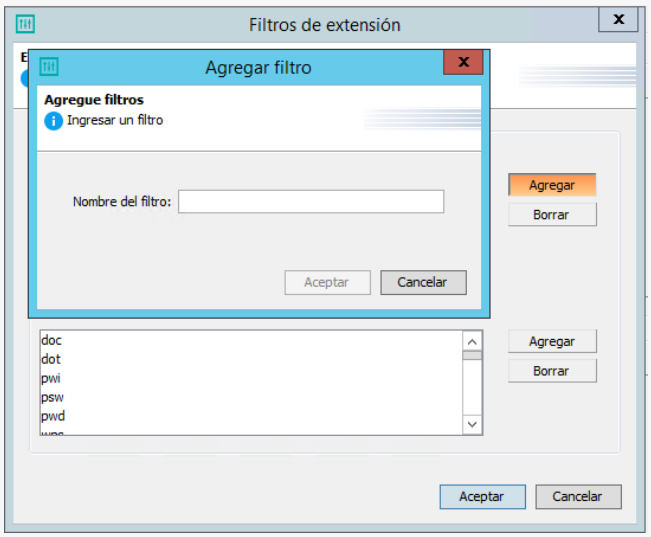
Definición de filtros de extensión personalizados

En ocasiones, los filtros de extensión predefinidos no cumplen con las necesidades de la organización y se deben crear filtros personalizados. Para agregar una nueva extensión debe:

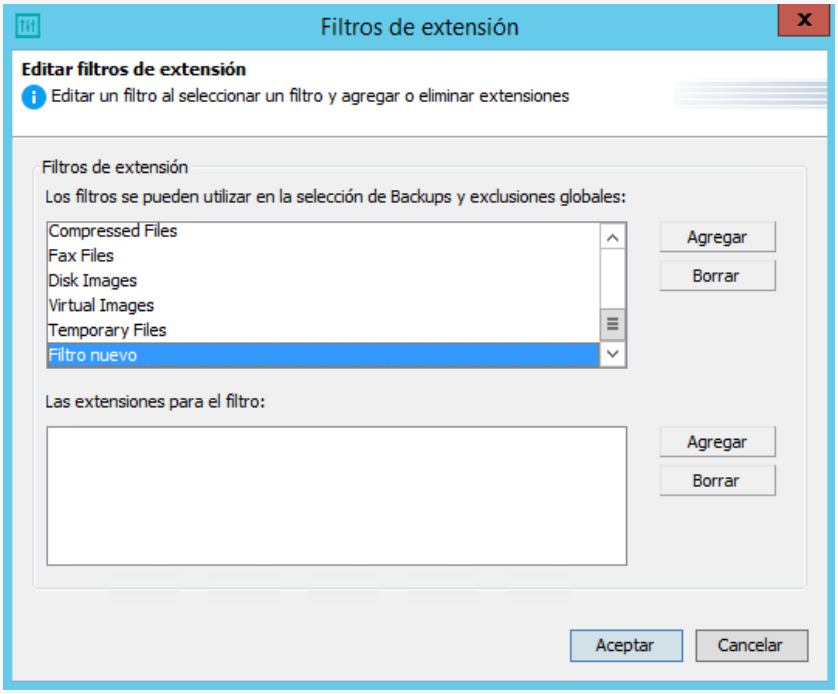
Hacer clic en el botón Filtros, junto al panel de selección del backup.



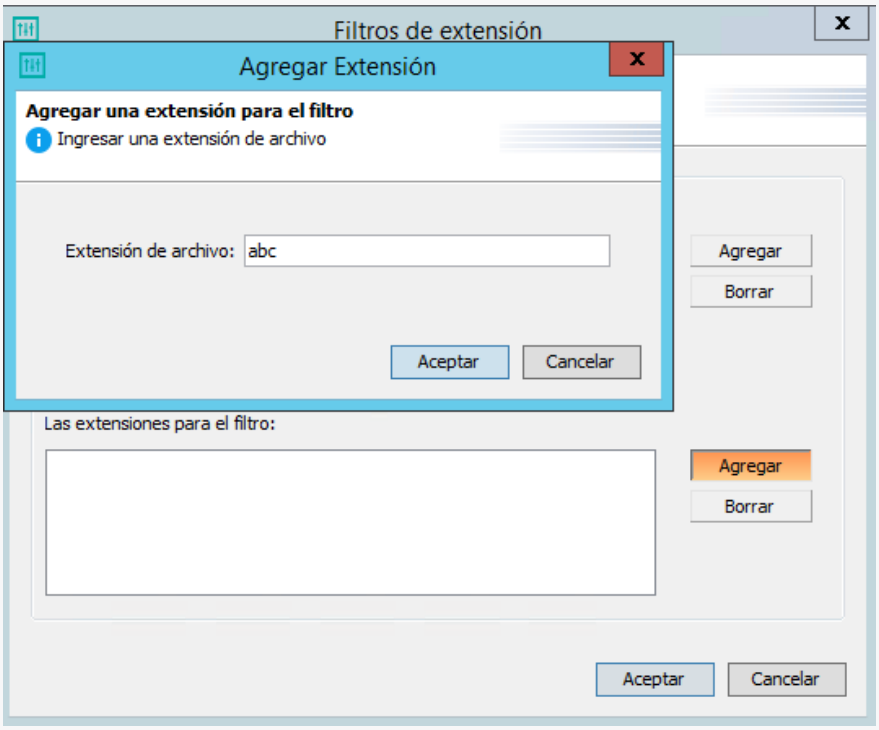
La ventana de filtros de extensión es desplegada. Hacer clic en el botón Agregar junto al panel de los filtros de extensión.



Ingresar un nombre para el nuevo filtro de extensión personalizado y luego dar Aceptar para agregar el filtro.



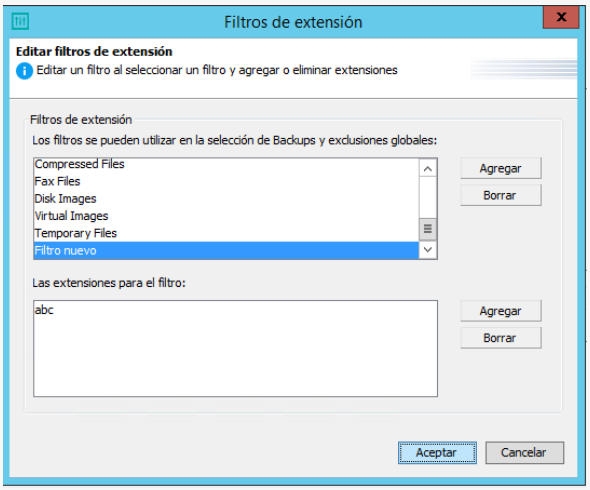
Seleccionar el filtro agregado recientemente, luego hacer clic en el botón Agregar al lado del panel de filtros de Extensión.



Introducir la extensión de archivo para el filtro.

Nota: Sólo introduzca la extensión de un archivo. Por ejemplo, escriba "ABC" y no " .ABC" o " * .ABC".

Hacer clic en Aceptar para agregar la nueva extensión en el filtro.



Repetir estos pasos cada vez que requiera agregar una nueva extensión de un archivo requerido para los Filtros de Extensión.

Cuando se han creado todas las extensiones de archivos, hacer clic en Aceptar para guardar.

Borrar Filtros de extensión

Para borrar un filtro de extensión usted debe: Seleccionar la entrada del filtro que desea eliminar. Hacer clic en el botón **Borrar** al lado del panel de filtro de extensión. La entrada se eliminará.

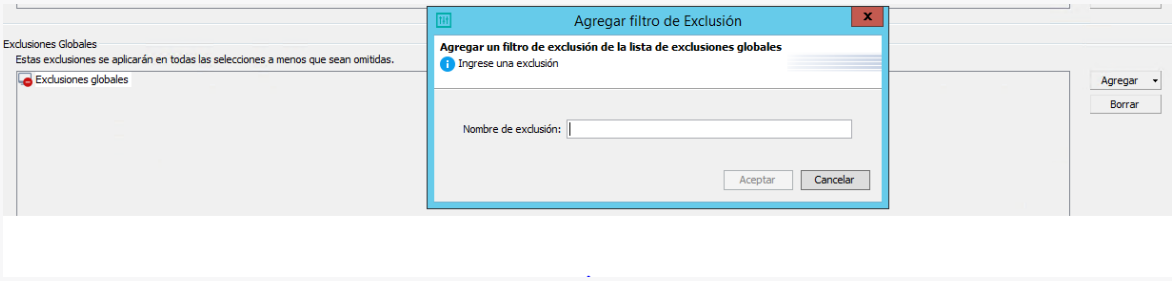
Exclusiones Globales

Al aplicar exclusiones globales, todas las extensiones dentro de la exclusión global serán aplicadas a la selección del backup. Esto ayuda a garantizar que dentro de la selección del backup definido no se incluyan los archivos que no deben ser respaldados.

Algunas organizaciones no requieren realizar backups de archivos multimedia. En lugar de aplicar un filtro de exclusión en cada acceso directo, volumen o carpeta, el administrador puede aplicar una exclusión global para no permitir el backup de los archivos multimedia.

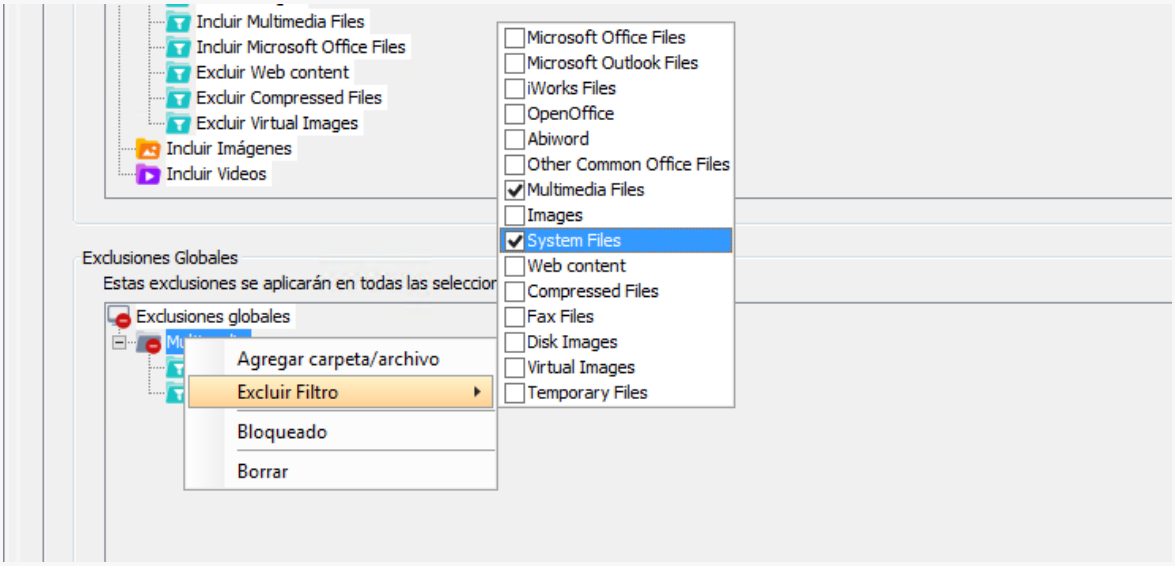
Agregar una exclusión global

Para agregar una exclusión global debe seleccionar la opción Exclusiones Globales Hacer clic en Agregar ubicado junto al panel de las Exclusiones Globales.



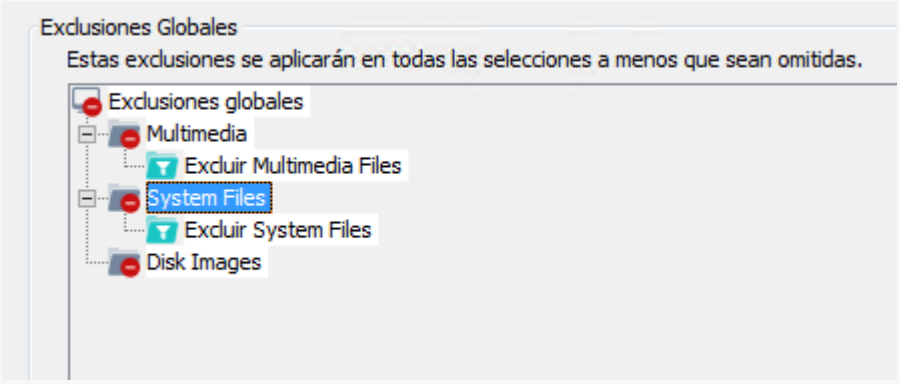
Dentro del cuadro desplegado, ingresar el nombre de la carpeta que contendrá la exclusión global, por ejemplo “Multimedia”

Hacer clic en Aceptar para continuar.



Hacer clic derecho dentro de la carpeta recién creada de exclusiones globales, seleccionar Excluir Filtro y luego seleccionar los filtros de extensión deseados a excluir del backup. Para este ejemplo se seleccionaría Multimedia Files.

Hacer clic en cualquier otro lado de la ventana para visualizar la exclusión agregada. Se agregarán más filtros a medida que se vayan seleccionando.



Borrar exclusión global

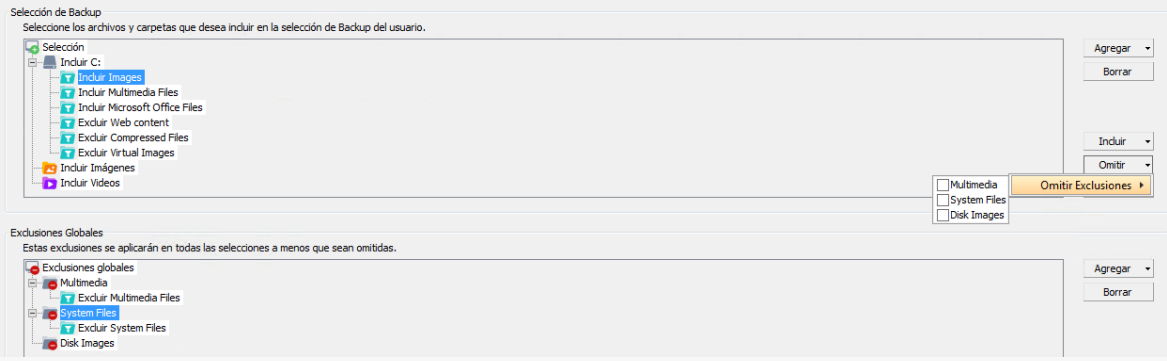
Para borrar una exclusión global se debe seleccionar la opción que se desea borrar dentro de las exclusiones globales. Hacer clic en el botón Borrar ubicado junto al panel de exclusiones globales. La entrada será eliminada.

Hacer clic en la opción Guardar en el panel de opciones de edición de Política para guardar el cambio.

Ignorar una exclusión global

En algunos casos es necesario ignorar una exclusión global sin tener que eliminar la condición en las exclusiones globales. Para ignorar una exclusión global en la selección del backup se debe:

Seleccionar el volumen o acceso directo.

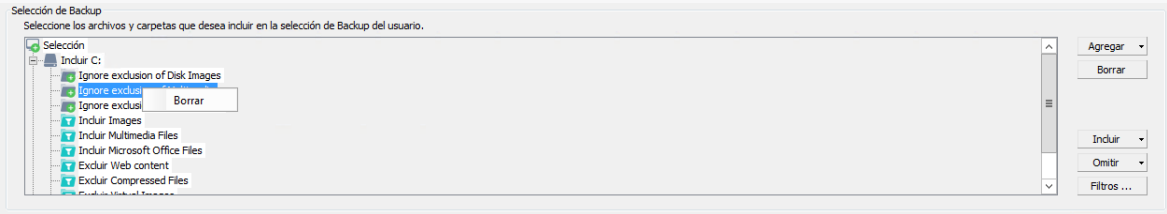


Hacer clic en el botón Omitir junto al panel de selección del backup y luego seleccione la casilla de Omitir exclusiones que se requiere que sea omitida de las exclusiones globales.

Nota: Esta opción puede ser deshabilitada al bloquear las exclusiones globales, permitiendo no omitir ninguna de las opciones definidas en las exclusiones globales.

Deshacer omitir exclusiones

Las exclusiones globales seleccionadas para ser omitidas, pueden ser eliminadas. Seleccionar la entrada Ignore exclusión of Multimedia. Hacer clic en el botón Borrar junto al panel de Selección del Backup.

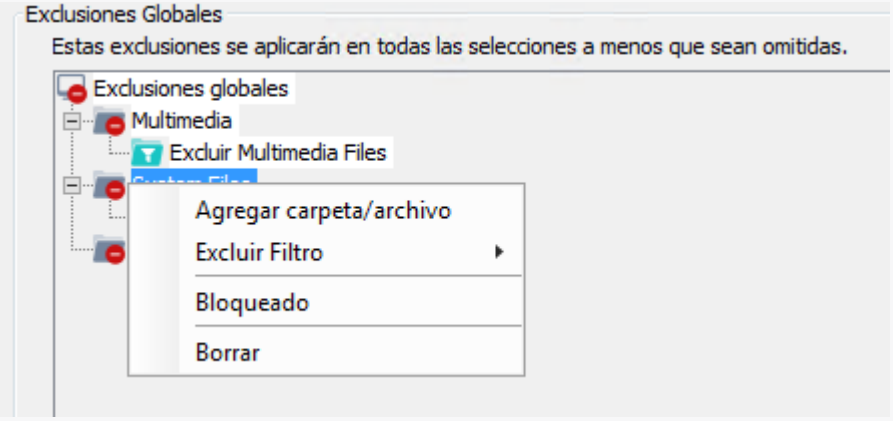


La opción seleccionada será eliminada.

Bloquear exclusión global

Bloquear una exclusión global asegura que un usuario no omita o elimine exclusiones en el agente del usuario. Para bloquear una exclusión global se debe:

Hacer clic derecho en el ítem de la exclusión global.



Seleccione la opción **Bloqueado**, para bloquear este estado.

Nota: El administrador puede permitir que el usuario defina su backup, pero la opción de bloqueo de las exclusiones globales previene que la exclusión sea omitida o eliminada en la selección del backup del agente**.**

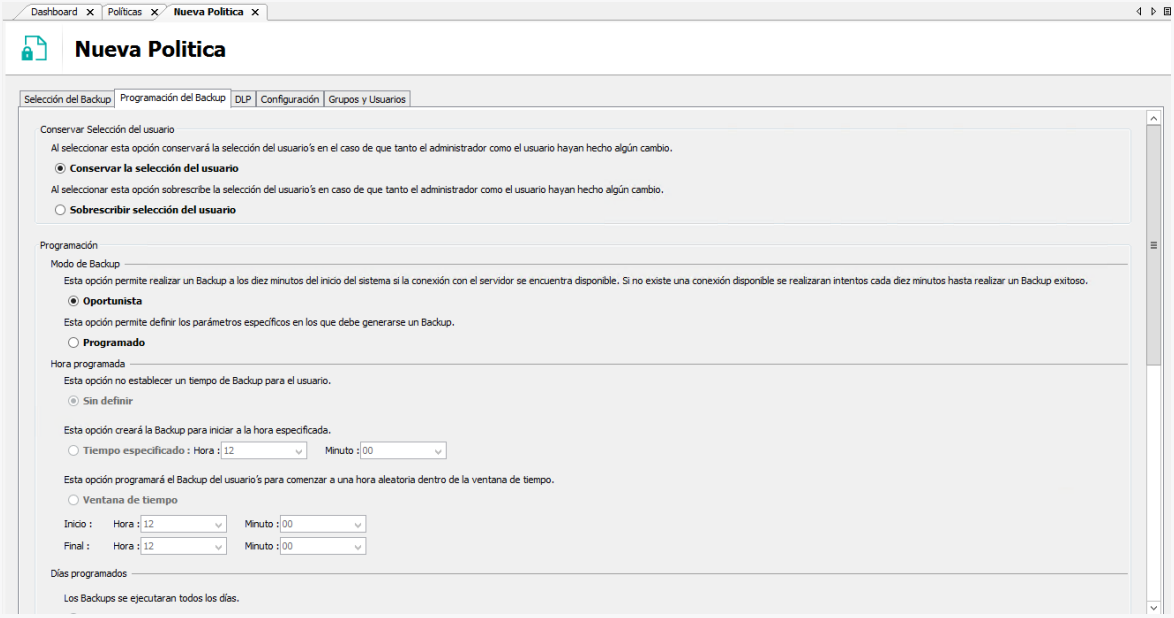
Programación de los backups

La opción de programación, automatiza el proceso de backup para ejecutarse en un tiempo específico que determine el usuario, ya sea diariamente o semanalmente; la programación del backup está definido para ser Oportunista, es decir que el backup se ejecutará cuando se identifique conexión con el servidor.

Características de la programación

Seleccionar la pestaña **Programar** en la política de backup.

Para definir una programación para los backups se debe:

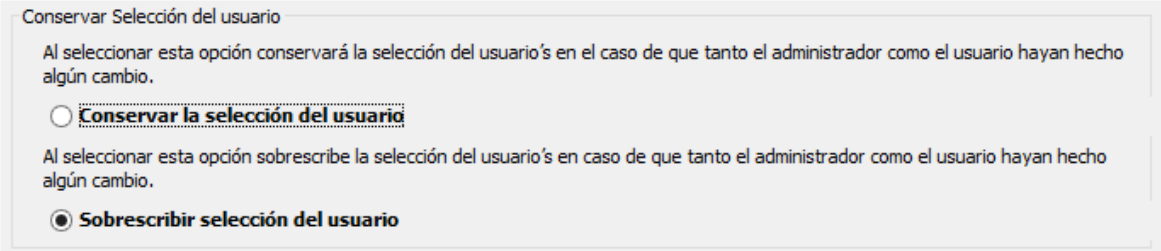


Conservar selección del usuario

La funcionalidad de las políticas pueden ser administrados en la Consola de Administracion y en la consola del usuario final. Esto podría causar algún tipo de conflicto cuando se realizan los cambios. La opcion de **Conservar Selección del usuario** en la Consola de Administracion impide que se presente conflicto cuando el administrador realiza cualquier cambio en la política.

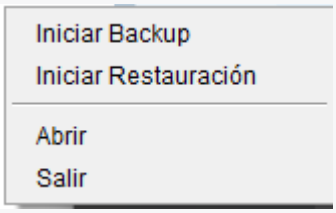
Se presentan las siguientes opciones para esta caracteristica:

- **Conservar selección del usuario**: Seleccionar esta opción para conservar las modificaciones realizadas por el usuario final. No se tomaran los cambios realizados en la consola de adminsitracion.
- **Sobrescribir selección del usuario**: Seleccionar esta opción para sobrescribir las modificaciones realizadas por el usuario final cuando se modifique la politica en la consola de administracion.



Las siguientes características describen las opciones disponibles al definir la programación de un backup. Modo del Backup:

Característica	Opción	Descripción
Tipo de backup	El tipo de backup puede ser seleccionado para ser Oportunista o programado	
	Oportunista	El backup Oportunista está destinado a realizar al menos un backup exitoso por día. El proceso ejecutado es el siguiente:
		1. El primer backup iniciara a los 10 minutos que el usuario inicie sesión. 2. Si no existe conexión con el servidor en una hora específica, se intentará nuevamente cada 10 minutos hasta que se realice el backup de manera satisfactoria. 3. En el caso que se presenten transitorios, como, sin conexión, máximo de conexiones al servidor, desconexión del cliente, etc. El backup terminara de manera silenciosa (No se generan reportes) y será reprogramado para intentar nuevamente realizar el backup nuevamente en 10 minutos. 4. En el evento de presentarse reportes persistentes, tales como cuota insuficiente, backup cancelados, etc., el proceso de backup se dará por terminado, se generará un reporte y será reprogramado para ejecutarse nuevamente a las 12:00 AM del siguiente día. 5. Al hibernar un equipo no afectara la programación del backup. 6. El icono de la consola del agente indicara la fecha y hora para el próximo backup oportunista. Para ver el estado, hacer clic derecho en el icono de la consola del usuario final en la barra de tareas.

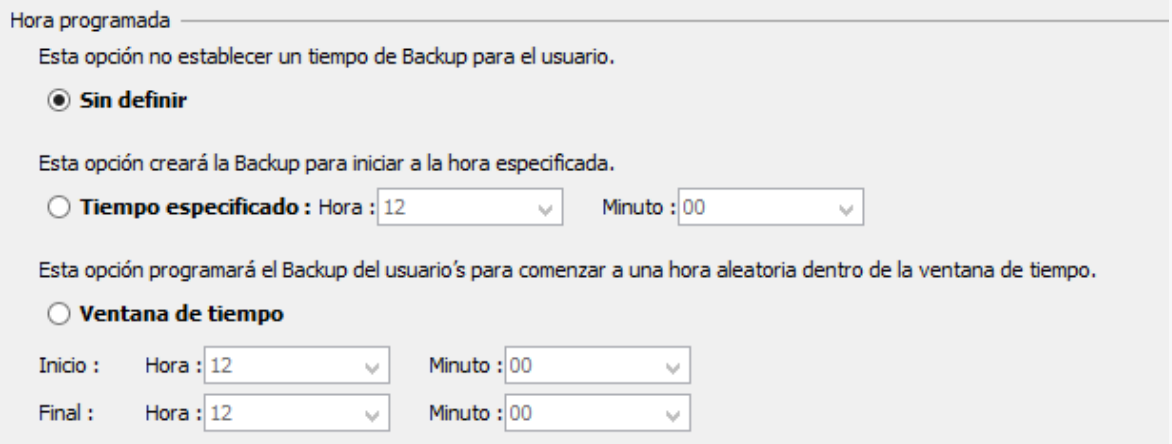
Característica	Opción	Descripción
		 Los siguientes puntos son de importancia relevante para los backups oportunistas: - Los backups oportunistas siempre intentarán procesar un respaldo en la primera oportunidad disponible del día y por lo tanto reducir el riesgo de saltarse el horario de backup. - Los Backup oportunistas no pueden ser usados con la opción de procesamiento por lotes. - Se puede activar desde la política de backup o en la consola del usuario dentro de la configuración de programación. - Se encuentra habilitado por defecto en la política incorporada por defecto. - Puede ser habilitado en todas las políticas existentes.
	Programado	El modo programado permite definir opciones de programación específicos como se verá a continuación.
Hora Programada	Las opciones de programación por horas se pueden establecer en un tiempo determinado, dentro de una ventana de tiempo específico o se pueden dejar sin definir.	
	Sin definir	Aunque no se recomienda, los horarios pueden ser dejados sin definir. Se requiere que los usuarios especifiquen su propio horario de backup.

Característica	Opción	Descripción
		Nota: Esto no podrá ser realizado si la programación se encuentra bloqueada.
	Tiempo especifico	Defina una hora para el inicio del backup
	Ventana de tiempo	El administrador puede seleccionar una ventana de tiempo en el que el servidor de Aranda asignará los horarios de backup a todos los grupos y usuarios asignados a la política de backup. Esta opción extiende las horas de inicio de backup entre los grupos y los usuarios asignados a través de la ventana de tiempo. Esto equilibra la carga de la programación de backups mediante la reducción en el número de conexiones simultáneas, y por consiguiente aliviar la carga en el servidor.
Días Programados	Seleccione los días de ejecución de los backups.	
	Diario	Los backups se ejecutan todos los días de lunes a domingo.
	Días de la semana	Los backups se ejecutan todos los días de lunes a viernes.
	Especificado	El administrador puede seleccionar los días específicos que se debe ejecutar el backup, donde seria cualquier día de lunes a domingo,
Programar Bloqueos	Configura bloqueos disponibles para la programación.	
	Desbloqueado	El estado de desbloqueo permite al usuario alterar el tiempo de programación del backup
	Permitir al usuario elegir un tiempo dentro de la ventana	El usuario puede seleccionar una hora de programación de backup dentro de la ventana de tiempo especificada.

Característica	Opción	Descripción
	Bloqueado	Bloquea la programación del backup y prohíbe que el usuario cambie la programación del backup en la consola de usuario.
Horario Pausado	Habilita que la programación del backup sea pausada	
	Seleccionado	Permite al usuario hacer una pausa en su horario programado de backup. Tenga en cuenta que si la programación del backup se encuentra en el estado de pausa, el backup no se ejecutará a la hora programada.
	No Seleccionado	Prohíbe al usuario pausar la programación del backup.

Hora Programada

Para definir la programación por horas:

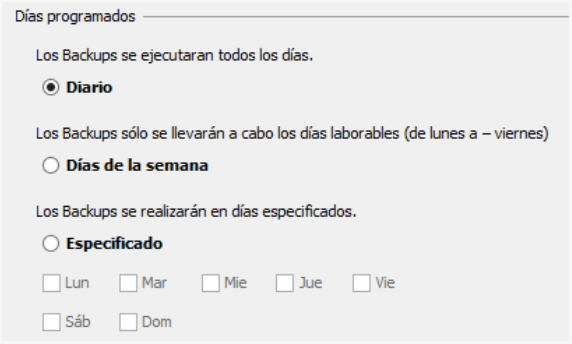


Seleccionar una de las opciones de programación que desea implementar.

- **Tiempo especificado**: Esta opción permite ajustar el momento en hora y minutos exactos en que desea que comience a ejecutarse el backup.
- **Ventana de tiempo**: Esta opción permite establecer un plazo determinado de tiempo (Hora inicial y final) en el cual se desea que comience el respaldo de la información.

Días programados

Para definir la programación por días:

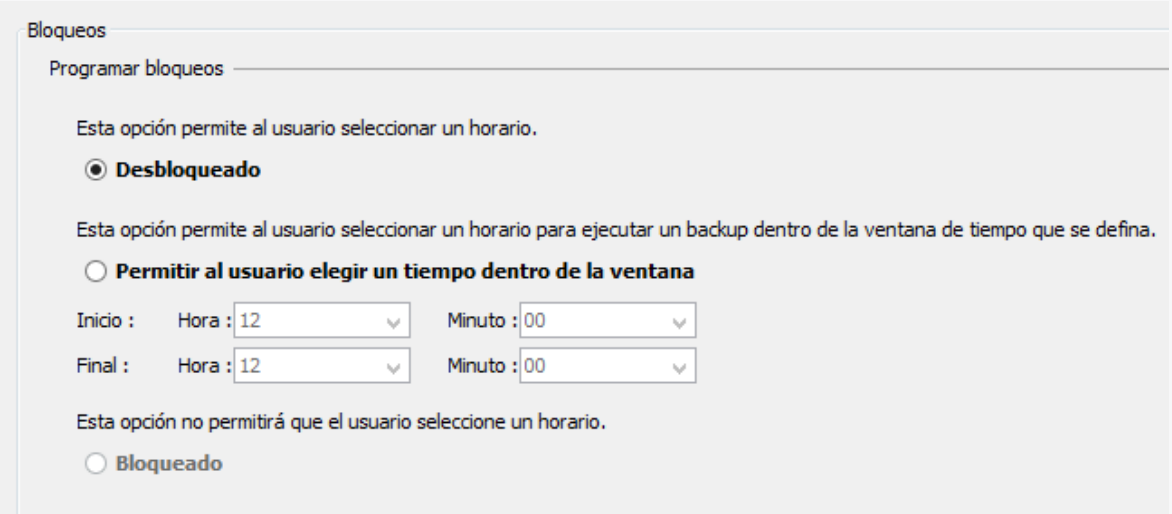


Seleccionar la opción deseada para el backup, ya sea por “Todos los días”, “Días de Semana”, “Especificado”.

- Todos los días: Se ejecutará una tarea de backup todos los días de lunes a domingo.
- Días de la semana: La tarea de backup se ejecutará de lunes a viernes.
- Especificado: Se definen los días en los cuales se ejecutará un backup. Seleccione las casillas de los días en que desea ejecutar un backup.

Programar Bloqueos

Para definir la programación de bloqueos:



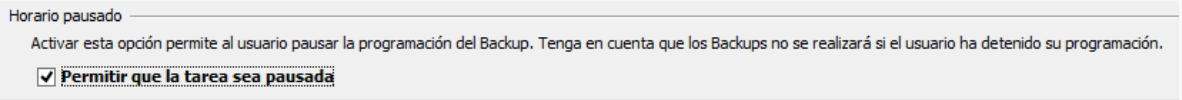
Seleccionar la opción deseada: Desbloquear, permitir que el usuario escoja un momento dentro de la ventana de tiempo o bloquear para que el usuario no pueda realizar cambios.

- La opción Desbloqueado permite que los usuarios seleccionen una programación para el backup.
- La opción Permitir al usuario elegir un tiempo dentro de la ventana permite al usuario definir una ventana de tiempo en la cual iniciara su backup.
- La opción Bloqueado no permite al usuario seleccionar una programación.

Pausar la tarea de backup

Una programación puede ser puesta en un estado de pausa, la cual no permitirá la ejecución de un backup programado.

Seleccionar el cuadro de la opción Permitir que la tarea sea pausada para permitirle a un usuario pausar la programación de los backups.



Nota: Si la tarea de programación se encuentra en un estado pausado, la tarea de backup no se ejecutará hasta que esta sea permitida nuevamente. Generalmente no se recomienda que se permita a un usuario pausar la programación de los backup.

DLP
Las opciones de DLP o Data Loss Prevention de los backups consisten en alternativas de cifrado de archivos, revocación de permisos antes perdida de datos y geolocalización de estaciones.

4.2 ¿Cómo configurar DLP?

Cifrado
Más información sobre cifrado de Aranda Data Safe.

1. Aranda Data Safe aprovecha el sistema de archivos cifrado de Microsoft (EFS) estándar de la industria.

2. Compatible con todas las versiones de Microsoft Windows (no disponible en Mac y Linux)
3. Encriptación / descifrado sin necesidad de interacción del usuario.
4. Cifrar los archivos casi en tiempo real (El proceso de cifrado supervisará los archivos que se ejecutarán y se cifrarán cada 10 minutos).
5. El cifrado selectivo excluye el sistema operativo del cifrado, eliminando así el impacto en el rendimiento
6. No se requiere despliegue de software adicional ya que el cifrado es administrado por un único Agente de Aranda Data Safe.
7. Habilitado directamente desde la política central lo que un despliegue en minutos.

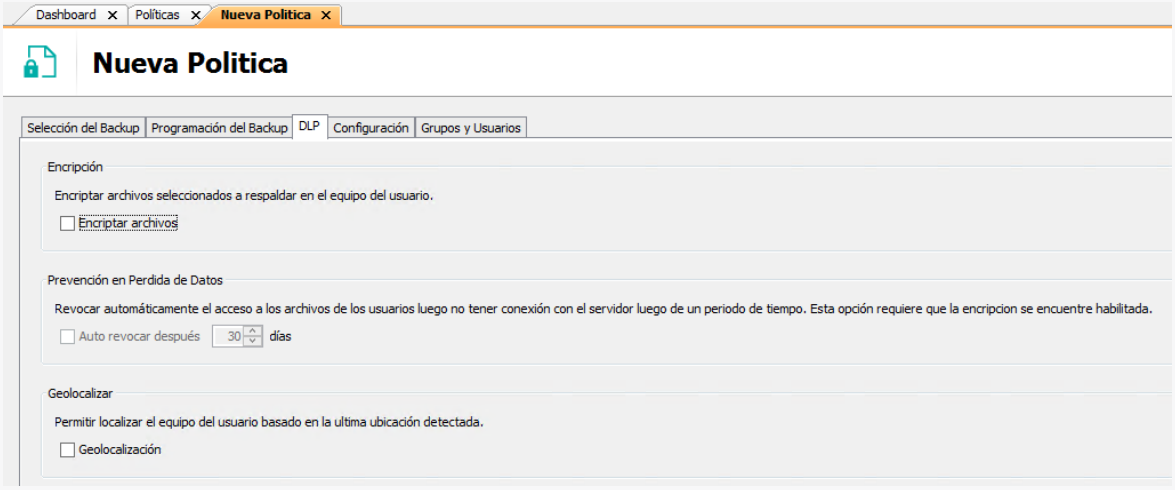
¿Qué necesita antes de activar el cifrado?

1. Cree un Certificado de autoridad que se emitirá a los usuarios de su red con un cifrado EFS certificado.
2. Modifique la plantilla de certificado EFS existente (o cree una plantilla personalizada) y asegúrese de que la clave privada es exportable.
3. Modifique la directiva de dominio predeterminada para deshabilitar los certificados auto firmados.
4. Asegúrese de que el certificado del agente de recuperación sea válido en la red. Http://support.microsoft.com/kb/937536.

Habilitar cifrado de datos

DLP comienza con la habilitación del cifrado de datos en la política de Aranda Data Safe. El cifrado de datos protege los documentos del negocio de accesos no autorizados cifrando los archivos en el equipo local del usuario.

Las configuraciones consisten en lo siguiente:



Encripción: Cifrar los archivos seleccionadas para realizar el backup en el equipo del usuario.

Prevención en Perdida de Datos: Revocar el acceso a los datos después de un periodo determinado de días sin conexión del agente al servidor principal.

Geolocalización: Permitir identificar la ubicación del equipo.

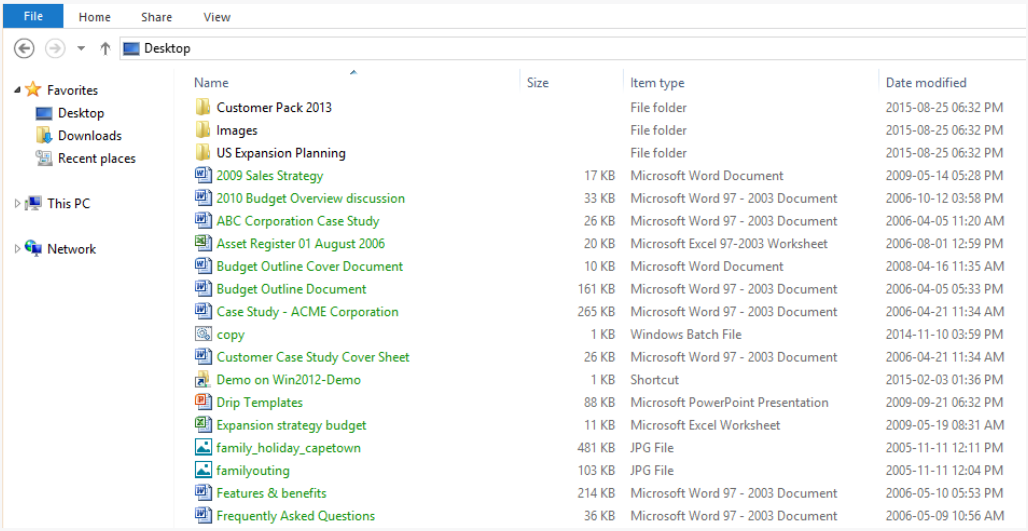
¿Qué sucede después de habilitar el cifrado?

Nueva máquina sin copias de seguridad

Aranda Data Safe tiene que realizar una copia de seguridad primero para adquirir las rutas de acceso a los archivos que se han incluido en la selección de copia de seguridad. Una vez completada la primera copia de seguridad, Aranda Data Safe comenzará a encriptar los archivos. El texto del archivo cifrado cambiará de negro a verde como se ve a continuación.

Máquina existente con copias de seguridad

Aranda Data Safe utilizará las rutas existentes de los archivos de copia de seguridad y comenzará a cifrar todos los archivos incluidos en la selección de copia de seguridad. El texto del archivo cifrado cambiará de negro a verde como se ve a continuación.



EFS hace uso de un certificado de cifrado que actúa como una clave para cifrar los archivos. Más información sobre encriptación EFS está disponible en el sitio web de Microsoft. Https://technet.microsoft.com/en-us/library/cc700811.aspx.

Aranda Data Safe realizará una copia de seguridad de los certificados de cifrado EFS del usuario antes de comenzar el proceso de encriptación. Siempre verificará si es necesario cargar nuevos certificados en el servidor. A continuación, puede ver los eventos de registro para el cifrado y descifrado:

Preguntas frecuentes

¿Cómo puedo transferir datos a otro equipo en un escenario de migración?
Utilice Aranda Data Safe para restaurar los datos de un usuario en un equipo nuevo. Esto lo restaurará en un formato sin cifrar. Los datos se cifrarán localmente con el certificado en el nuevo equipo.

¿Puedo usar una unidad externa para mover los datos de un usuario a otro ordenador en un escenario de migración?
Puede utilizar una unidad externa para mover los datos de un usuario a un nuevo computador. Deberá descifrar los datos antes de moverlos al nuevo equipo o puede que necesite importar el certificado de cifrado EFS desde el servidor de Aranda Data Safe utilizando el agente de Aranda Data Safe.

Tenga en cuenta que si no utiliza Aranda Data Safe para restaurar los datos de un usuario a la nueva máquina, se hará copia de seguridad de todos los datos como nuevos y tendrá una situación en la que tendrá datos duplicados en el servidor.

¿Cuándo no serán accesibles los datos a otros usuarios?
1. Extraer el disco duro y colocarlo en otro PC.
2. Acceso remoto a la parte C $ de la PC de otro usuario.
3. Iniciar sesión en el equipo con otro perfil.
4. Copiar datos en una unidad externa formateada con NTFS.
5. Compartir una carpeta en el equipo del usuario.

¿Cuándo serán accesibles los datos a otros usuarios?

1. Compartir archivos a través de Dropbox, OneDrive, unidad de Google.
2. Al copiar archivos a una ubicación de red.
3. Al copiar datos en una unidad extraíble formateada con FAT / FAT32

¿Cómo puedo eliminar el cifrado del computador de un usuario?

1. El cifrado se puede desactivar desde la política de Aranda Data Safe. El agente de Aranda comenzará a descifrar el archivo después de actualizar la nueva política en el inicio del agente o la próxima copia de seguridad.

Disabling Encryption process

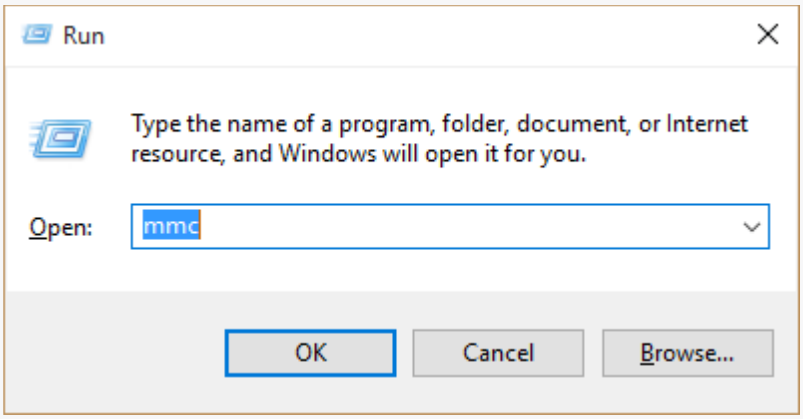
EncryptionRegistrar - The encryption process needs to be executed. The encryption flag was set to 'true' and is now set to 'false'.
EncryptionWatcherRegistrar - Deregistering encryption watcher.
EncryptionProcessTask - Running encryption process (because encryption was enabled/disabled).
EncryptionProcess - Starting encryption process
EncryptionProcess - [Pre-Encryption-Process Check] Check if EFS encryption keys need to be sent to server for safe keeping.
BackupEncryptionKeysTask - Determine if EFS encryption keys need to be sent to server for safe keeping.
BackupEncryptionKeysTask - EFS encryption keys have NOT changed, no need to send to server

¿Podemos activar de forma centralizada el cifrado para MAC?

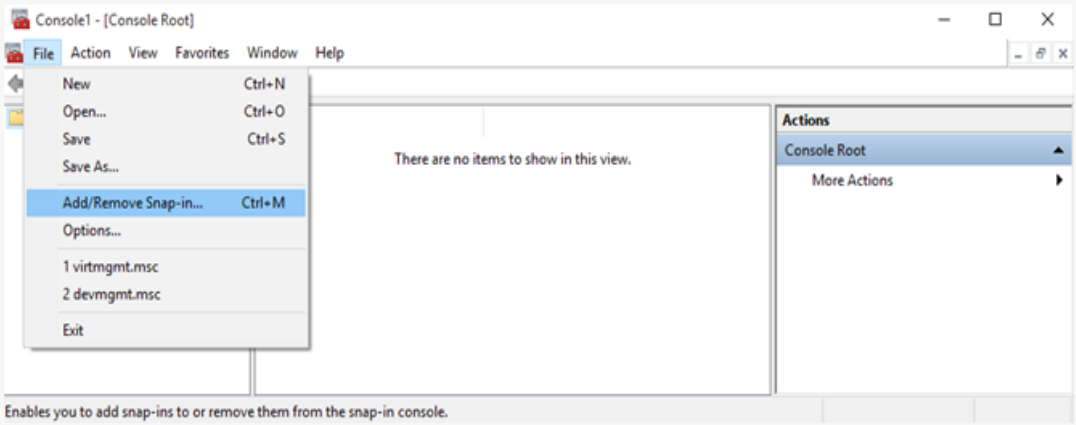
No, Aranda Data Safe usa Windows EFS, el cual no está disponible en máquinas Mac. El sistema operativo de Mac tiene cifrado de archivos incorporado y debe habilitarse desde las propiedades de archivo y carpeta.

¿Dónde encuentro el certificado de cifrado EFS del usuario en la máquina local?

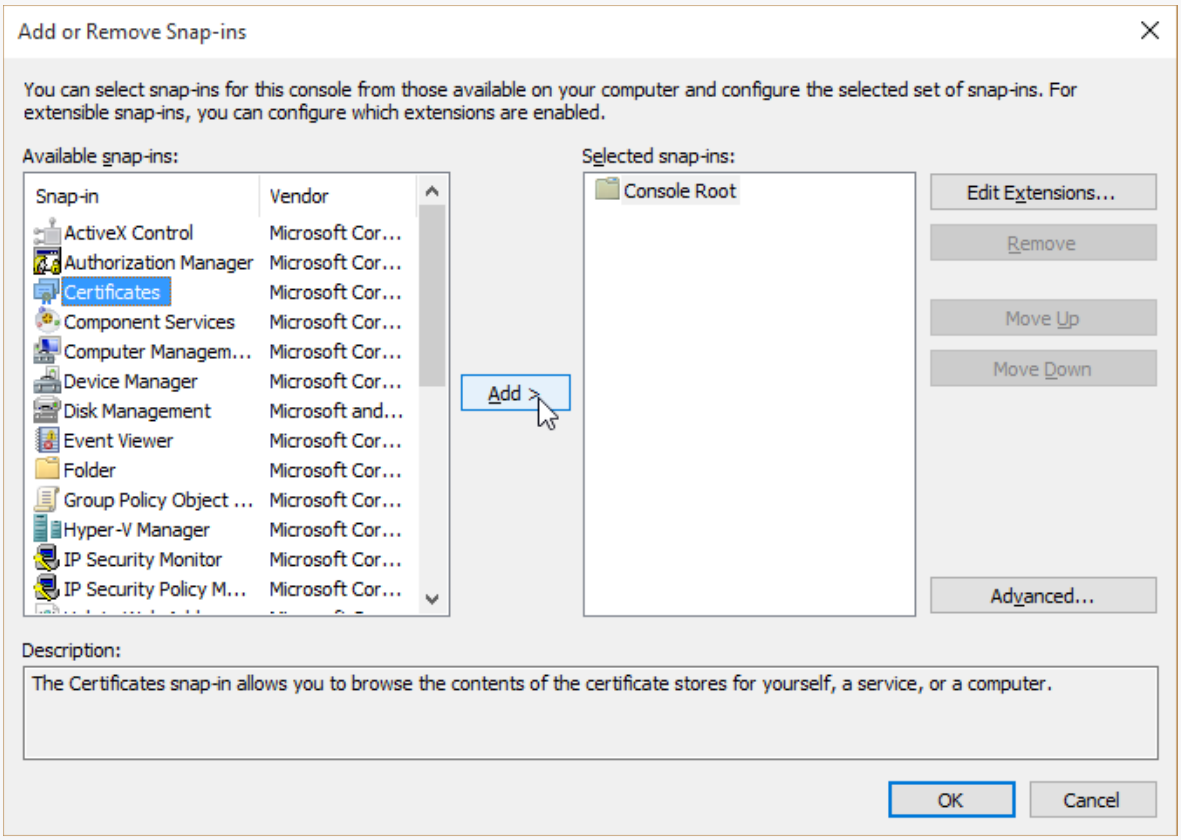
Deberá agregar certificados en la consola de administración de Microsoft
Inicio -> Ejecutar -> mmc



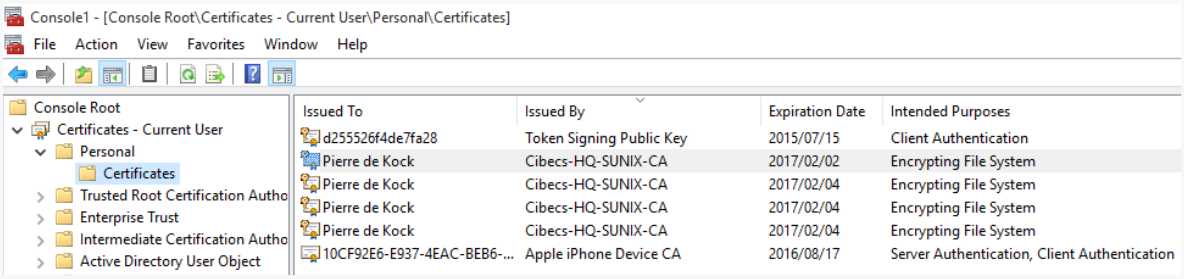
Agregar o quitar el complemento.



Agregar certificados y seleccionar valores predeterminados



Abra Certificados bajo Certificados -> Personal y busque los certificados EFS allí.



Problemas debidos al mal uso de EFS

Si, por ejemplo, los usuarios copian archivos cifrados a volúmenes FAT, los archivos serán descifrados y por lo tanto no estarán protegidos. Debido a que el usuario tiene derecho a descifrar los archivos que cifraron, el archivo se descifra y se almacena en texto plano en el volumen FAT. Windows 2000 no da ninguna advertencia cuando esto sucede, pero Windows XP y Windows Server 2003 proporcionan una advertencia.

Si los usuarios proporcionan a otros con sus contraseñas, estas personas pueden iniciar sesión utilizando estas credenciales y descifrar los archivos cifrados del usuario. (Una vez que un usuario ha iniciado sesión correctamente, puede descifrar cualquier archivo que la cuenta de usuario tenga el derecho de descifrar.)

Si la clave privada del agente de recuperación no se archiva y se elimina del perfil del agente de recuperación, cualquier usuario que conozca las credenciales del agente de recuperación puede iniciar sesión y descifrar de forma transparente todos los archivos cifrados.

Gestión del certificado de cifrado

La gestión de certificados de cifrado incorporada crea automáticamente copias de seguridad de los certificados de cifrado del usuario.

- El sistema realiza copias de seguridad automatizadas de los certificados de cifrado. Esta acción es realizada por el Agente de Usuario y almacenada en el servidor de Aranda Data Safe.
- Recomendamos encarecidamente que instale AD Certificate Services antes de implementar DLP en su red.
- Los certificados se pueden exportar en un formato cifrado, lo que permite un envío seguro al usuario.
- Los certificados sólo pueden importarse mediante un agente autenticado para garantizar la seguridad.

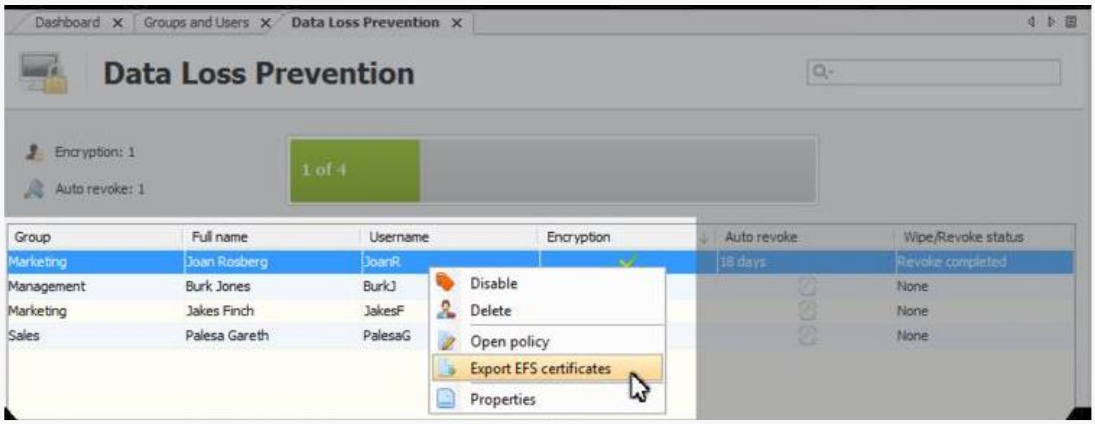
Pasos para exportar / importar certificados EFS

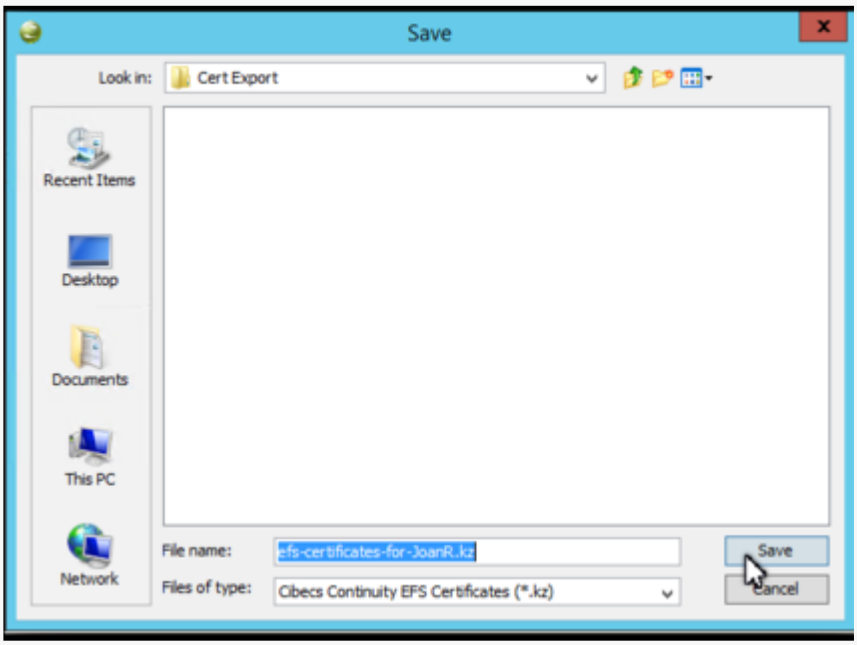
Si se ha revocado el acceso del usuario a sus archivos y desea restaurar el acceso a sus datos, puede utilizar los siguientes pasos para exportar / importar el certificado.

1. Haga clic con el botón derecho en la cuenta de usuario correspondiente en el Centro de control. Puede utilizar las vistas Grupos y usuarios, Estado de copia de seguridad o DLP para esta tarea.

2. Seleccione la opción Exportar certificados EFS y guarde el archivo en una ubicación de carpeta.

3. El certificado se exportará en un formato cifrado (efs-certificates-for-username.kz) para asegurar que sólo puede ser utilizado por el destinatario. El archivo puede ser enviado por correo electrónico al usuario.

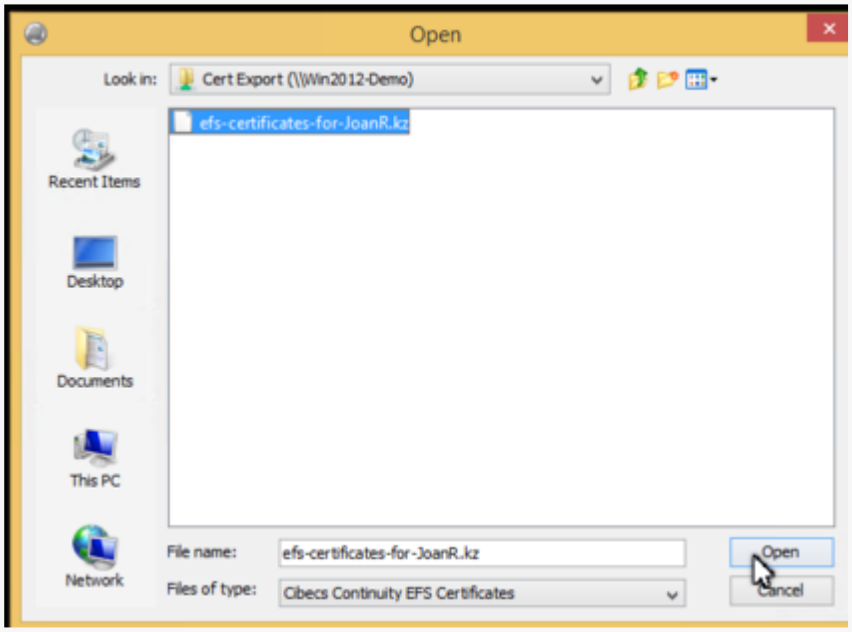




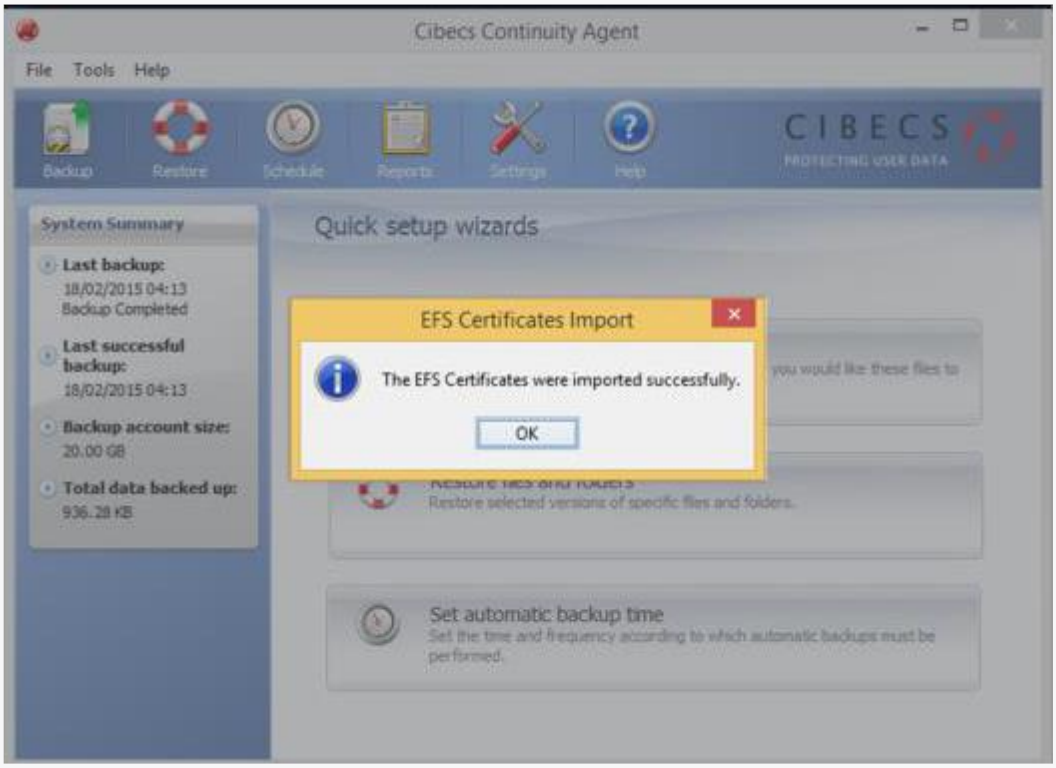
Agente de usuario

- Abra el Agente de usuario y seleccione el menú Herramientas.
- Seleccione Importar certificados EFS.

- Busque los efs-certificates-for-username.kz y suba.



- Se le notificará si la importación se ha realizado correctamente.
- El usuario tendrá acceso a sus archivos de nuevo.



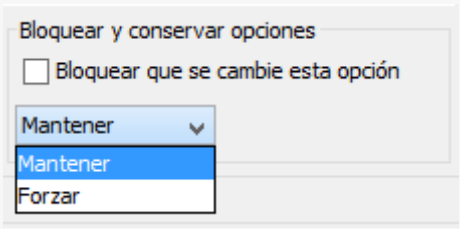
Configuración

Las opciones de configuraciones de los backups consisten en opciones generales, opciones de visualización del backup y de rendimiento. Estas ayudan a definir el comportamiento del agente del usuario durante un backup, la información que se mostrará al usuario y su rendimiento general.

Las configuraciones consisten en 3 grupos principales:

- Opciones de visualización generales
- Opciones de visualización del backup
- Opciones de rendimiento

Cada una de estas configuraciones contienen opciones para mantener o forzar



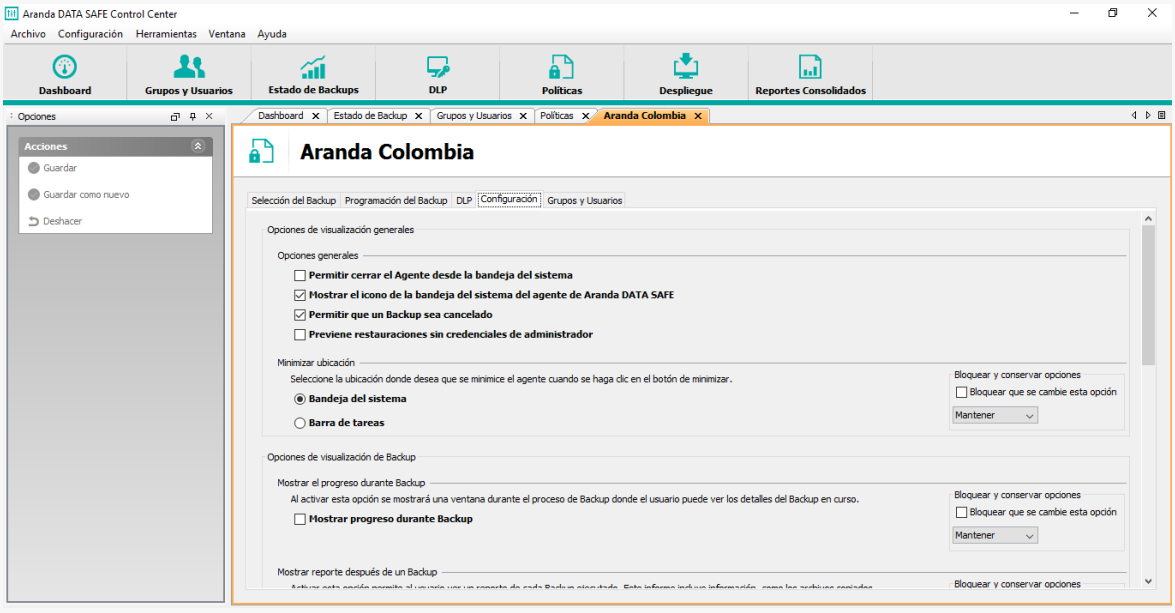
Seleccionar **Bloquear que se cambie esta opción** para prevenir que se realicen futuros cambios dentro de la consola del usuario final

Seleccionar **Mantener** de la lista desplegada para preservar las opciones configuradas en la consola del usuario final.

Seleccionar **Forzar** de la lista desplegada para sobrescribir la selección realizada en la consola del usuario final.

Opciones Generales

Para configurar las opciones generales de los backups, hacer clic en **Configuración** en la política y luego deslice hacia abajo o arriba para visualizar las diferentes opciones disponibles.



La siguiente lista de características describe cada una de las opciones del grupo disponibles al definir la configuración de los backups.

Opciones de visualización generales

Característica	Opción	Descripción
Permitir cerrar el Agente desde la bandeja del Sistema	Define si un usuario puede o no detener el agente desde la barra de tareas	
	Habilitado	Permite a un usuario detener el agente
	Deshabilitado	No permite al usuario detener el agente. Esta opción es recomendada.
Mostar el icono de la bandeja del sistema del agente de Aranda DATA SAFE	Define se muestra o no el icono del agente de usuario final en la barra de tareas del sistema	
	Habilitado	Se mostrara el icono del agente del usuario final
	Deshabilitado	No se mostrara el icono del agente en la barra de tareas
Permitir que un Backup sea cancelado	Define si los usuarios pueden o no cancelar un Backup que se encuentra en proceso	
	Habilitado	Permite a un usuario cancelar el Backup
	Deshabilitado	Prohíbe al usuario cancelar el Backup en curso. Esta opción es recomendada.
Previene restauraciones sin credenciales de administrador	Define si los usuarios pueden restaurar su información con o sin la intervención del administrador	
	Habilitado	Prohíbe a los usuarios restaurar su información si las credenciales del administrador. Las credenciales del administrador son solicitadas cuando se inicia una restauración.
	Deshabilitado	Permite al usuario realizar restauración de su información siempre y cuando el agente tenga conexión con el servidor de Data Safe.
Minimizar Ubicación	Determina el comportamiento del agente cuando se minimiza su ventana de control	
	Bandeja del sistema	El agente se minimizará en la bandeja del sistema. Recomendado
	Barra de tareas	El agente se minimizara en la barra de tareas.
Las opciones de la ubicación donde se minimizara el agente pueden ser forzadas, preservadas y bloqueadas		

Opciones de visualización del Backup

Característica	Opción	Descripción
Mostrar el progreso durante backup	Define si se visualiza o no en el agente el progreso del backup	
	Habilitado	Se visualizara el progreso del backup
	Deshabilitado	No se visualizara el progreso del backup
Mostrar reporte después de un Backup	Define si se visualiza un reporte con el resumen del backup	
	Habilitado	Se mostrara un reporte al finalizar el backup
	Deshabilitado	No se mostrara un reporte al finalizar el backup
Notificación de Backup	Define si se notifica de la actividad de Backup	
	Mostrar ventana de notificación antes de comenzar el Backup	Se visualizará una notificación antes de iniciar el backup. Se puede configurar para que el usuario pueda parar o saltar el próximo backup.
	Empezar sin notificar al usuario	Esta opción ejecuta el backup en el horario programado.
Las opciones de la ubicación donde se minimizara el agente pueden ser forzadas, preservadas y bloqueadas		

Opciones de rendimiento

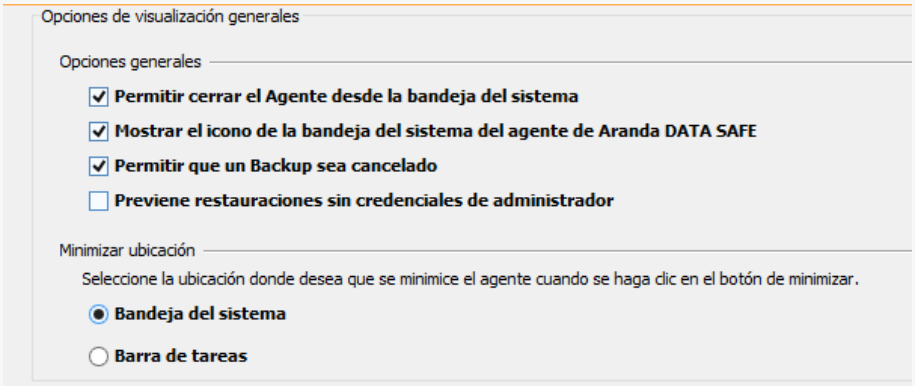
Característica	Opción	Descripción
Limitación de ancho de banda	Habilita la configuración y limitación del ancho de banda	
	Habilitado	Habilita la limitación del ancho de banda. Permite al administrador definir el ancho de banda en Kilobytes por segundo
	Deshabilitado	Deshabilita la limitación de ancho de banda. (Opción por defecto)

Impacto	Esta opción permite optimizar el rendimiento del agente	
	Menor Impacto	Configurar la barra en este estado utiliza menos recursos del equipo pero como resultado puede incrementar el tiempo del backup
	Opción por Defecto	Este estado es recomendado para PC, donde habilita una velocidad e impacto balanceado
	Backup más rápidos	Este estado usa los recursos disponibles para ejecutar el backup.
Procesamiento por lotes durante el Backup	Define si el procesamiento por lotes es habilitada o no	
	Habilitado	Permite el procesamiento por lotes. Cuando está activado, los datos del usuario se procesan por lotes en el disco duro local antes de ser trasladado al servidor de Aranda Data Safe. Esta opción se recomienda a los usuarios móviles ya que los Backups continuarán mientras el usuario se encuentra fuera de la oficina sin conexión al servidor de Aranda Data Safe. Cuando el usuario móvil vuelve a la oficina y está conectado de nuevo al servidor de Aranda, los datos del Backup se transferirán al servidor de Aranda Data Safe.
	Deshabilitado	Desactiva el procesamiento por lotes. Cuando la dosificación se desactiva se utiliza el método preferido de streaming. Los backups son enviados en tiempo real, la compresión y el

		cifrado a continuación, transfiriendo los datos a través de una conexión Segura al servidor de Aranda Data Safe.
Las opciones de la ubicación donde se minimizara el agente pueden ser forzadas, preservadas y bloqueadas		

Opciones Generales

Las opciones generales definen como se pueden controlar los backups desde el agente del usuario.



Seleccionar cada una de las opciones generales para activarlas.

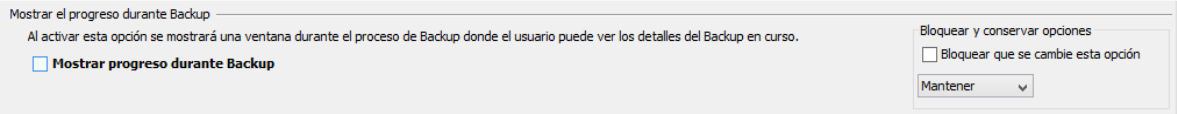
Permitir cerrar el Agente desde la bandeja del sistema permite que un usuario finalice el proceso del agente de Data Safe.
Mostrar el icono de la bandeja del sistema del agente de Aranda Data Safe mostrará el icono bandeja del sistema.
Permitir que un Backup sea cancelado permite a un usuario abortar un respaldo en curso
Previene restauraciones sin credenciales de administrador requiere que el usuario obtenga el permiso a los administradores para restaurar los datos.

Seleccionar la opción Minimizar ubicación para definir donde se minimizará la ventana del Agente, si a la bandeja del sistema o a la barra de tareas.

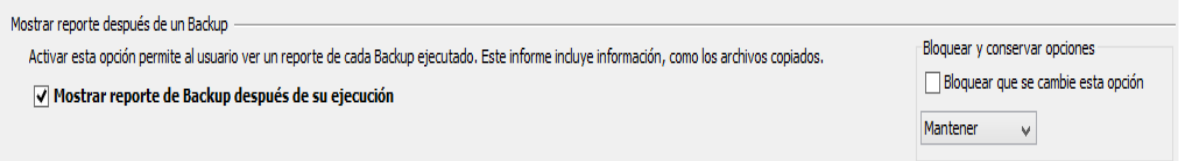
Opciones de Visualización de los Backups

Las opciones de visualización de los backups controlan cómo se muestra la información para el usuario durante un respaldo.

Seleccionar la casilla de verificación Mostrar el progreso durante Backup para visualizar el progreso d la restauración en curso.

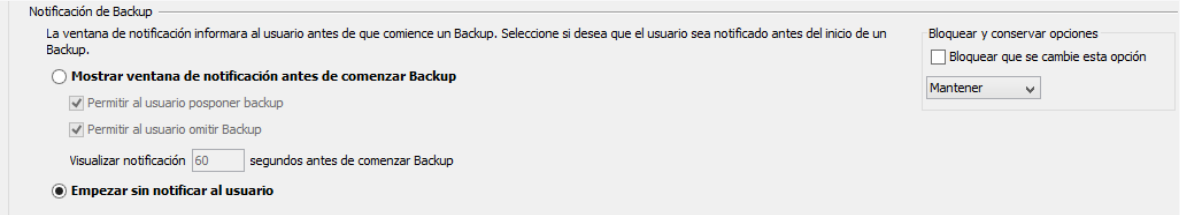


Seleccionar la casilla de verificación Mostrar el reporte después de un Backup para mostrar un informe resumen luego de cada respaldo.



Seleccionar la casilla de verificación Mostrar ventana de notificación antes de comenzar Backup o de Empezar sin notificar al usuario para indicar si el agente mostrará un mensaje de notificación antes del respaldo.

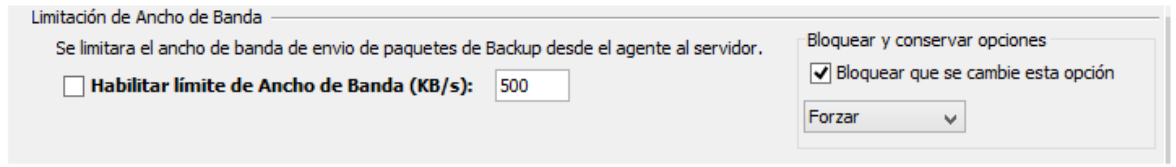
A la verificación Mostrar ventana de notificación antes de comenzar Backup incluye Permitir al usuario posponer el backup y Permitir al usuario omitir Backup, así como una notificación previa antes de comenzar a realizar el respaldo.



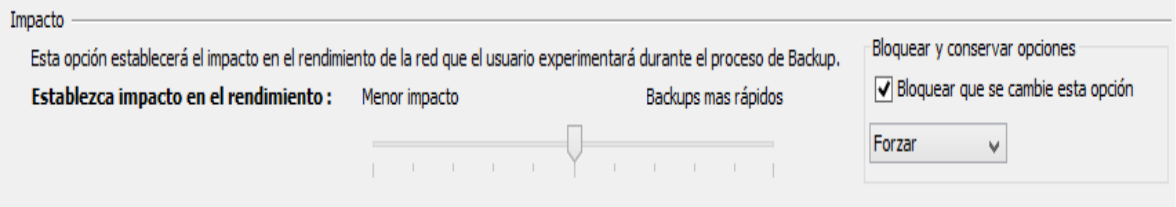
Opciones de Rendimiento

Las opciones de rendimiento se pueden configurar para gestionar el rendimiento de la red, de modo que los usuarios móviles puedan procesar los backups en el disco local, y poder configurar la cantidad de espacio disponible reservado en disco.

Seleccionar la opción de Habilitar límite de Ancho de Banda si quiere limitar el tráfico que se generara en la red. Ingrese el ancho de banda deseado en kilobytes por segundo. Este valor puede estar entre 1 y 10240 kilobytes por segundo (1KB – 10MB).



Ajustar la barra de deslizamiento del Impacto para definir el rendimiento en el procesamiento de los archivos de los equipos finales traducido en el porcentaje de la velocidad de la CPU.

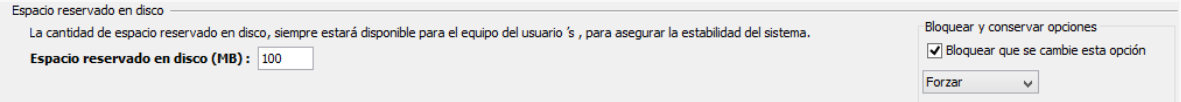


Menor Impacto: En este estado, el agente de Data Safe tiene el menor impacto en el sistema lo cual puede incrementar la duración de los respaldos.

Por defecto: En este estado, el agente de Data Safe realiza respaldo balanceando la velocidad de la CPU y el rendimiento.

Backups más rápidos: Se realizarán los respaldos de más rápido ya que no se tiene un límite para el procesamiento de los backups.

Configurar un valor entero en Megabytes para la opción del Espacio reservado en disco

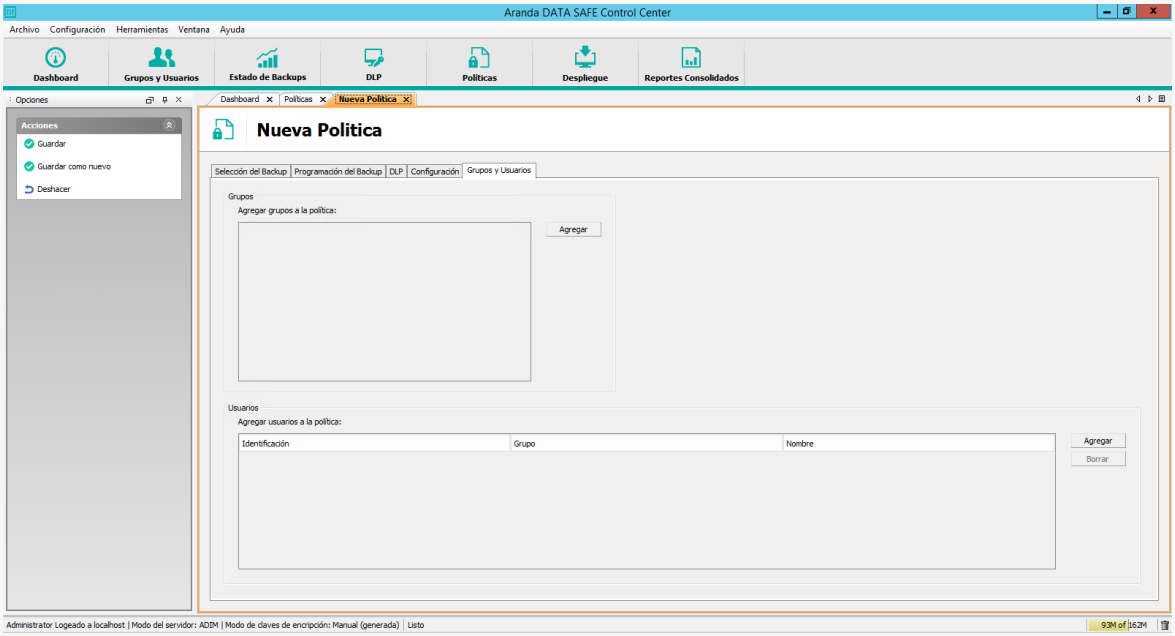


4.3 Grupos y usuarios

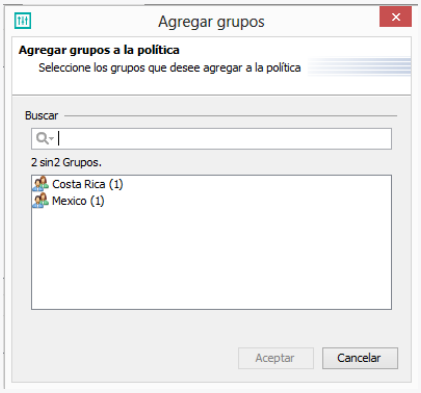
Esta pestaña permite asignar políticas de backup a los diferentes grupos y usuarios.

Adicionar grupos y usuarios

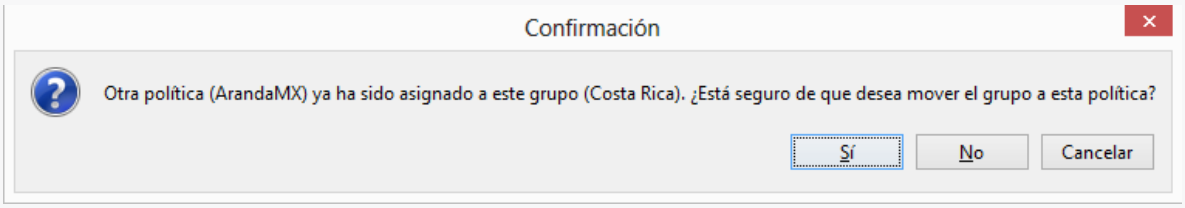
Para asignar grupos a una política de backup, seleccione la pestaña de Grupos y Usuarios



Seleccionar la opción Agregar en la parte de grupos en la política de Backup. Puede buscar o seleccionar el grupo deseado para agregar a la política. Y luego hacer clic en Aceptar para agregar el grupo.

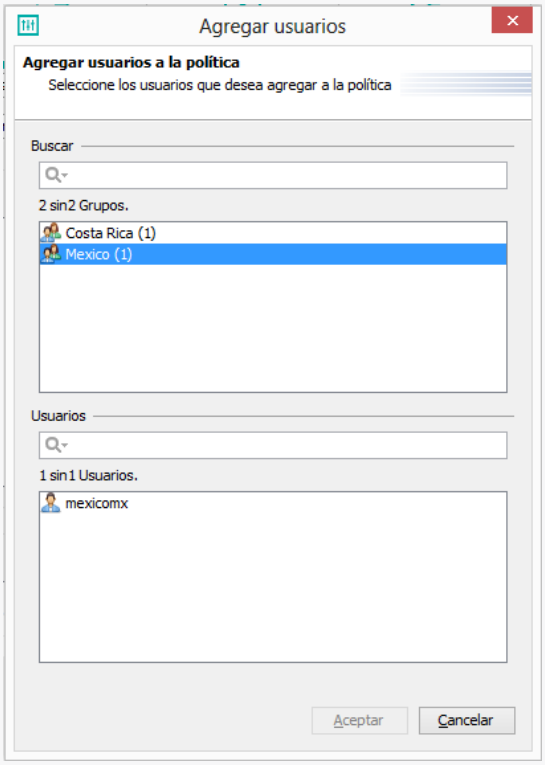


En caso que el grupo este habilitado en otra política, se desplegara un mensaje informando la política en la cual está asociado, hacer clic en **SI** para asignar el grupo a la nueva política, o **NO** para no asignar la política a este grupo



Si se desea agregar usuarios a la política de backup:

Seleccionar la opción Agregar dentro del panel de usuarios de la política de Backup.

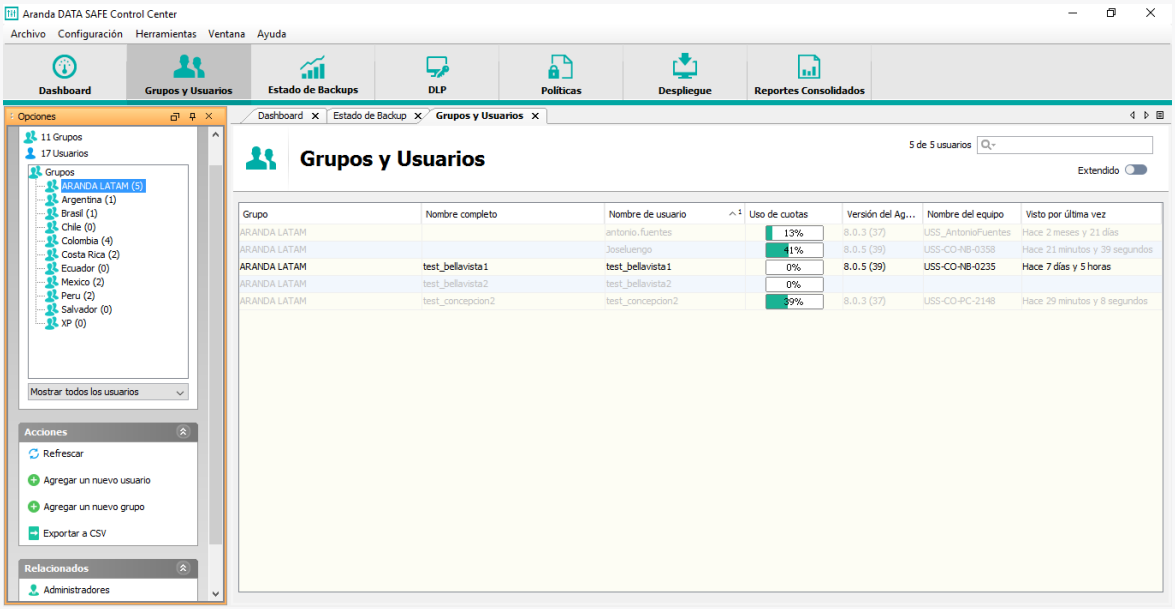


Es posible buscar o seleccionar el grupo que contiene al usuario que le será asignado la política.

A continuación, buscar o seleccionar el usuario(s) que desea asignar a la política. Hacer clic en Aceptar para agregar el usuario.

Importar grupos de backup desde el directorio activo

Cuando el servidor de Aranda Data Safe se encuentra en modo integración con el directorio activo, se pueden importar unidades organizacionales (OUs) y grupos de seguridad como grupos de usuarios.



Cuando los grupos y usuarios son creados y mantenidos, estos pueden ser importados a la consola de administración.

Para importar grupos desde el directorio activo:

Seleccionar la pestaña de grupos y usuarios y luego hacer clic en Importar grupos desde el directorio activo.

La consola de administración se conectará con el directorio activo y traerá la estructura organizacional. Puede seleccionar diferentes directorios activos si tiene configurado más de un dominio en el servidor de Aranda Data Safe.

Seleccionar las unidades organizacionales o grupos de seguridad a importar.

Es posible definir la Cuota de Backup y seleccionar la política de respaldo a ser usadas por los grupos. A cada usuario se le asignará la cuota y política del grupo.

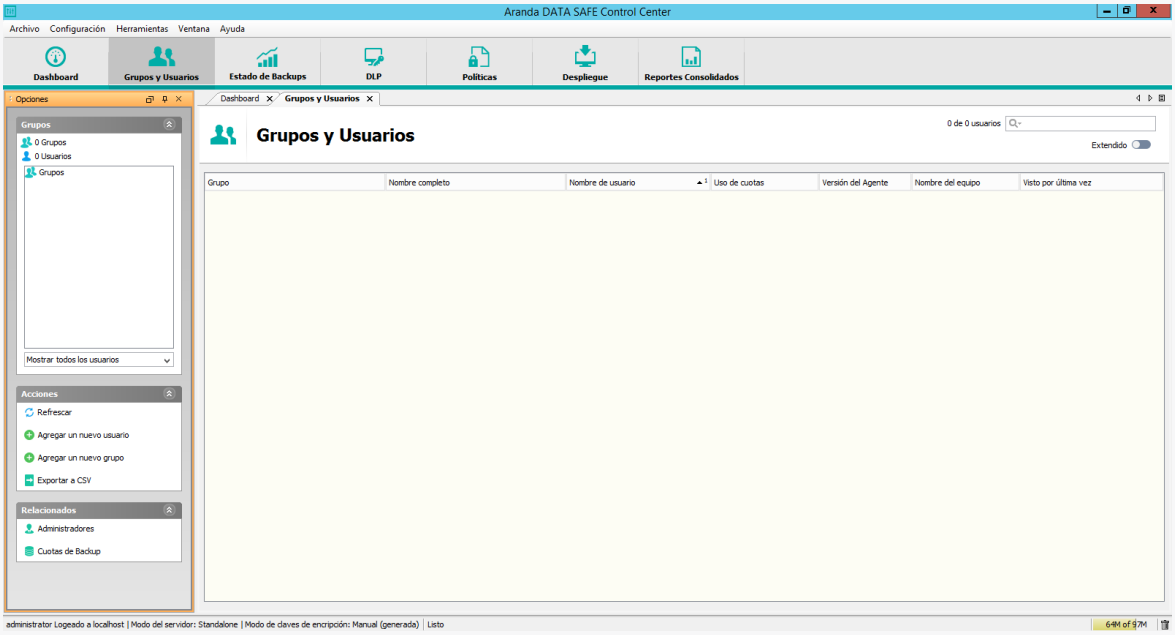
Hacer clic en Importar para comenzar el proceso.

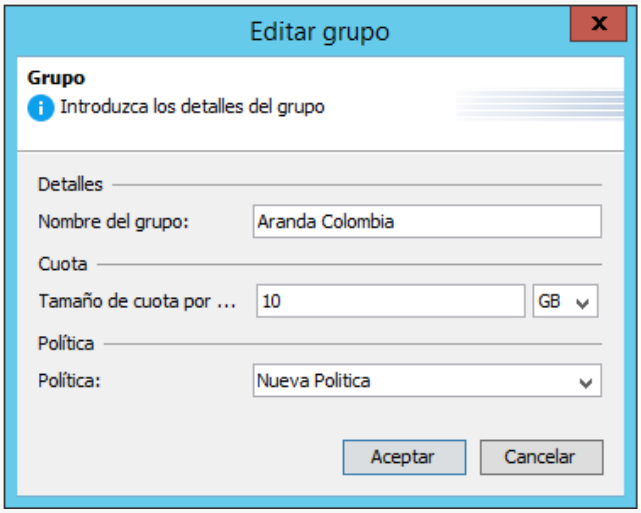
En este modo no es necesario agregar usuario, ya que este será agregado automáticamente luego del despliegue del agente a cada equipo de los usuarios finales.

Agregar grupos y usuarios en modo Independiente (StandAlone)

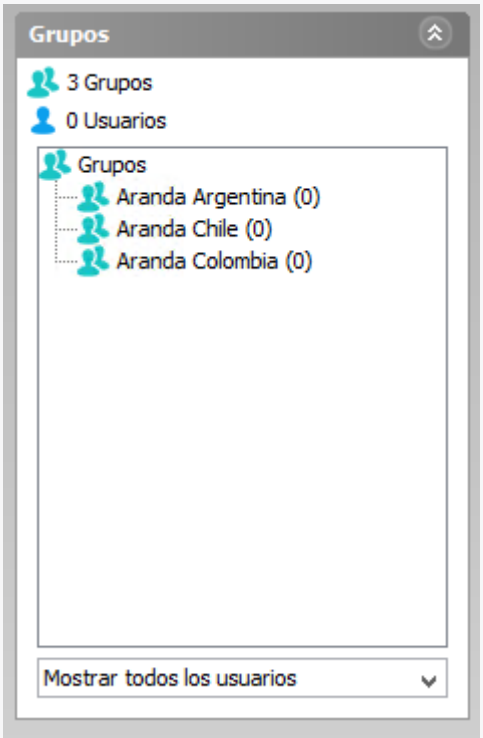
Cuando los servidores de Aranda Data Safe son configurados en modo independiente, se deben agregar manualmente los grupos y usuarios.

Para agregar un nuevo grupo de usuarios, hacer clic sobre la opción Agregar un nuevo grupo en el panel de Acciones.



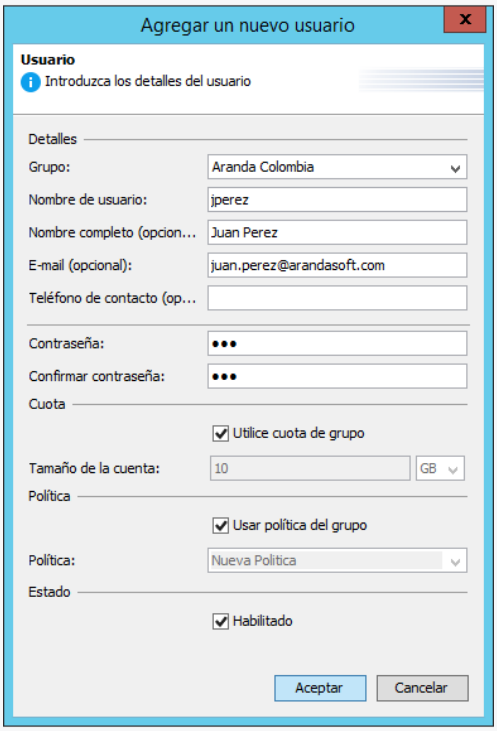


Ingresar el nuevo nombre del grupo > Ingresar la cuota (Espacio) para todos los usuarios en el grupo > Seleccionar la política de backup usada por el grupo > Hacer clic en Aceptar para agregar el grupo >El nuevo grupo será mostrado en el panel de grupos.



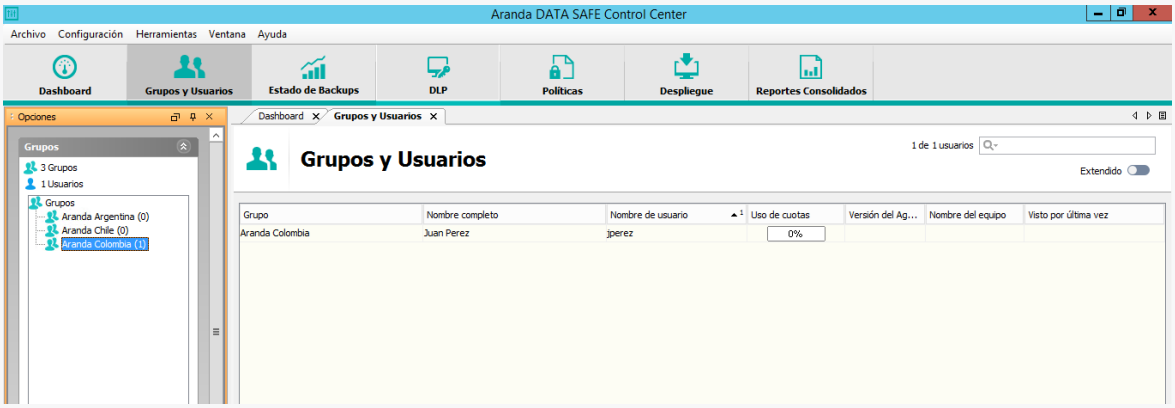
Agregar un nuevo usuario:

Hacer clic sobre la opción Agregar un Nuevo Usuario desde el panel de Acciones.



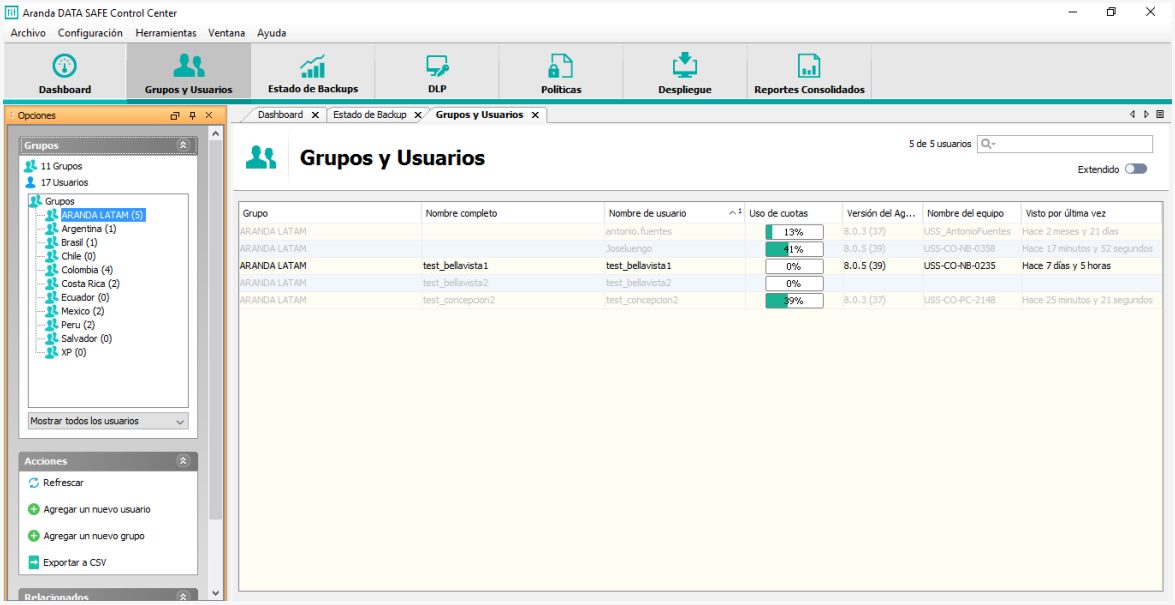
Seleccionar el grupo al cual el usuario pertenecerá. Ingresar los detalles del usuario. La cuota (espacio) y la política son las predefinidas en el grupo.

Hacer clic en Aceptar para agregar el usuario.



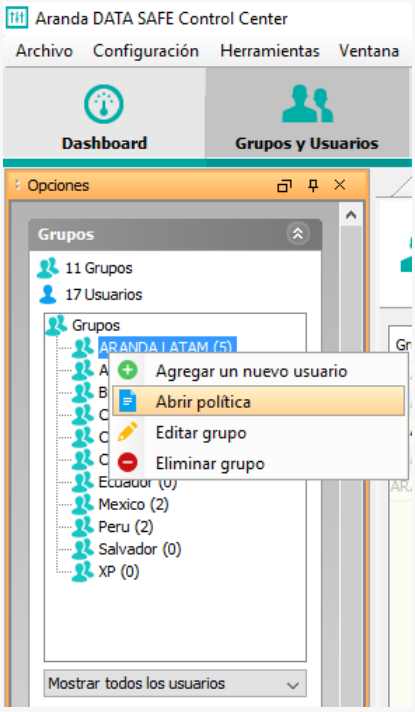
Asignar políticas de backup a grupos y usuarios

Las políticas de backup pueden ser asignadas a grupo o a usuarios individuales. Por defecto los usuarios heredan la configuración definida en los grupos donde se encuentran.

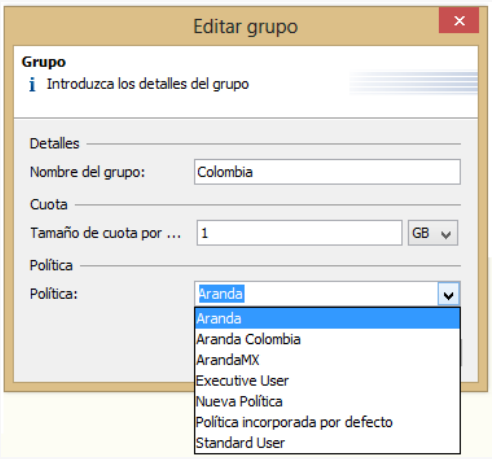


Asignar política a un grupo

Para asignar una política a un grupo: Hacer clic derecho sobre el grupo a asignar la política de Backup.



Hacer clic en “Editar grupo”

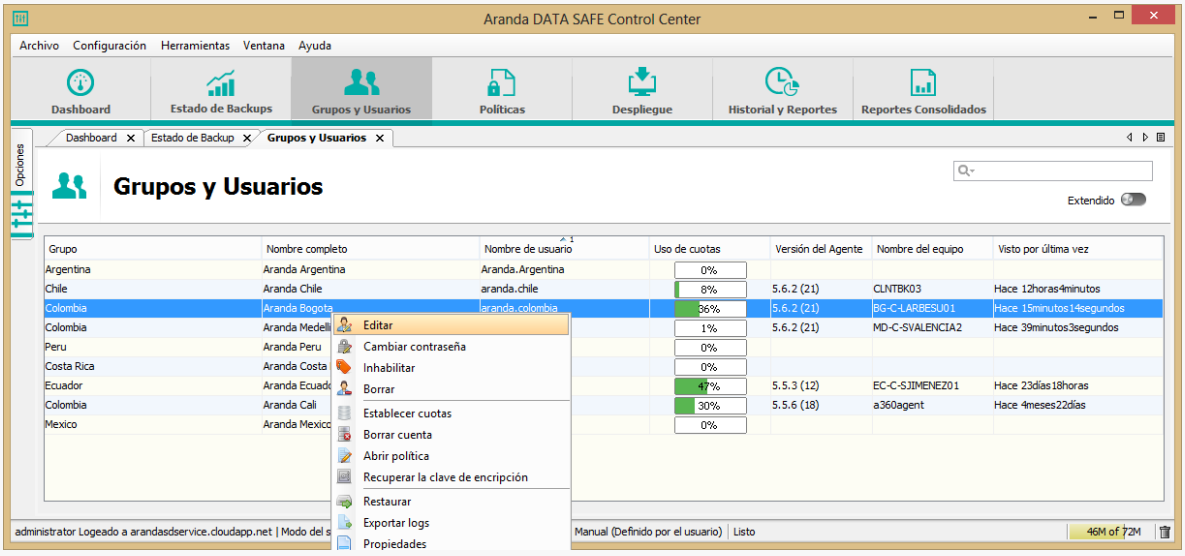


Seleccionar la política de backup a asignar desde la lista desplegable.

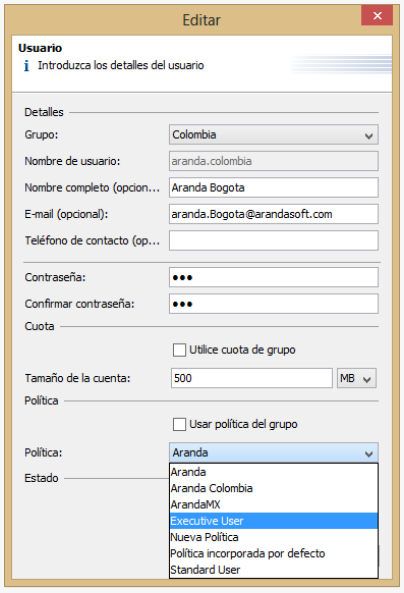
Dar en Aceptar para guardar los cambios realizados.

Asignar política a usuarios

Para asignar una política a un usuario: Seleccionar el usuario a editar dentro del panel de Grupos y usuarios.



Hacer clic derecho sobre el usuario a editar.



Deseleccionar la opción de Usar política del grupo.

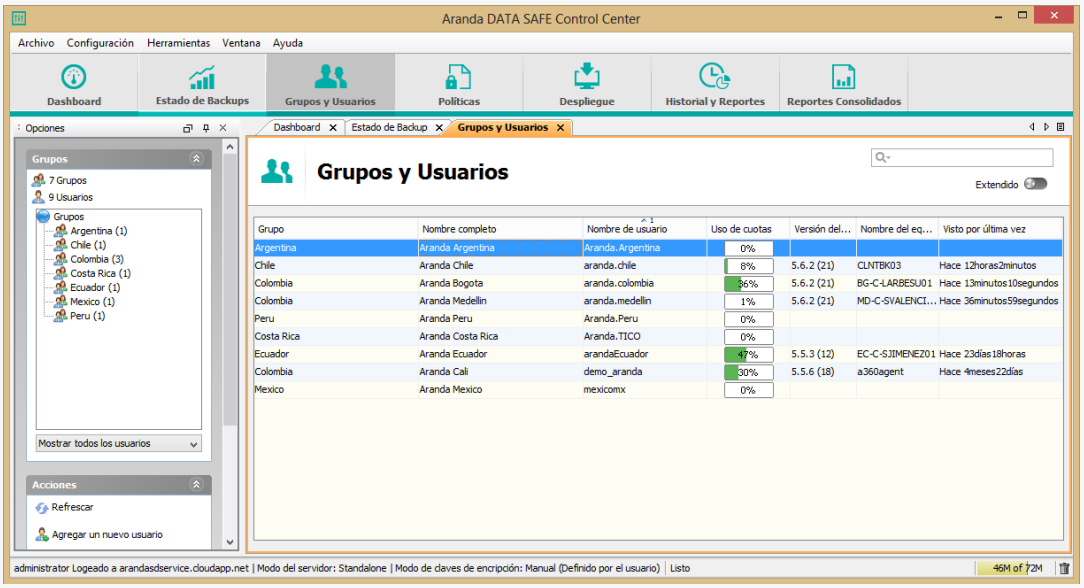
Seleccionar la política a asignar al usuario desde la lista desplegable.

Dar Aceptar para guardar los cambios realizados.

Manejo de las cuentas de backups

Las cuentas de backup son mostradas en el panel de Grupos y usuarios, donde puede gestionar el estado del grupo y usuarios.

Seleccione el panel de Grupos y usuarios.



Se muestra información crítica para cada uno de los usuarios creados en el servidor de Aranda Data Safe.

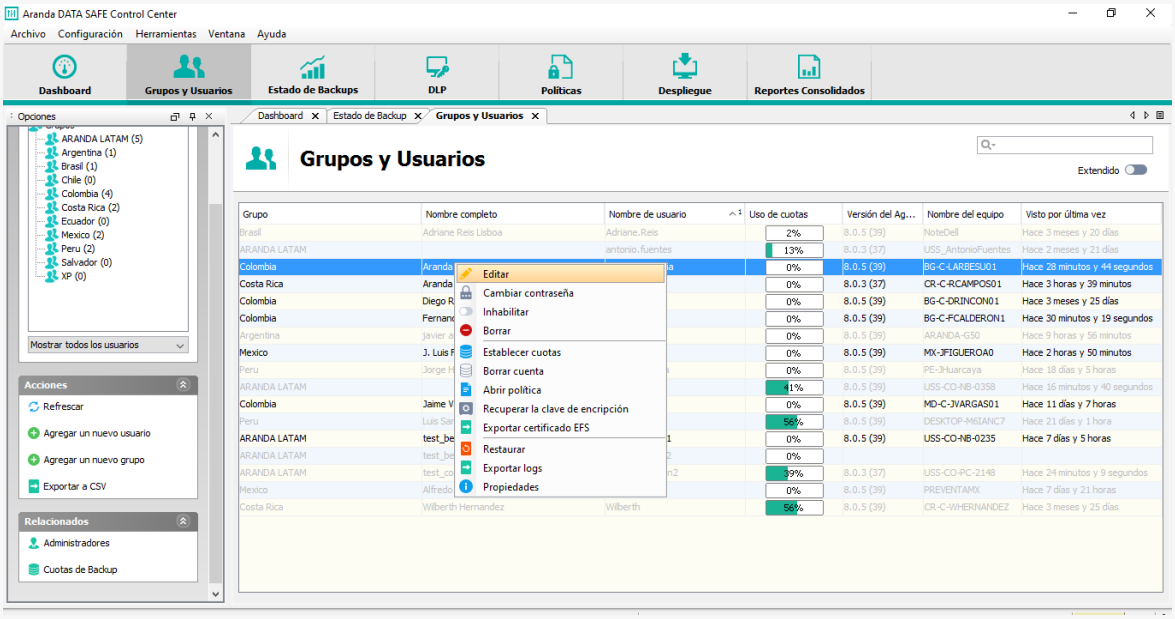
- El grupo al cual el usuario se encuentra asignado.
- El nombre de usuario.
- El porcentaje de cuota (espacio) usado por cada usuario.
- La versión del agente.
- El nombre del computador para cada usuario.
- El tiempo de la última conexión efectuada entre el agente y el servidor.

Extendido: Hacer clic sobre este botón para mostrar más información

Cuota usada: cantidad de espacio usado en Bytes, MB y Gb

- Cuota asignada: Espacio asignado para el usuario en Bytes, MB y GB.
- ID: el ID asignado al usuario durante la activación
- Fecha de activación: Fecha de última activación del agente.

Adicional a esto existen otras opciones de gestión de los usuarios



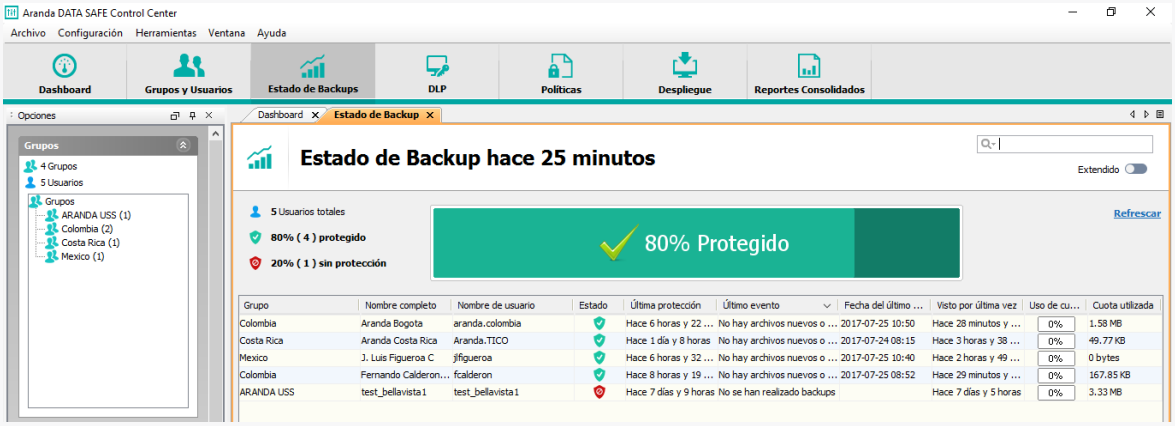
- **Editar:** Opción para editar la información del usuario, así como la asignación de cuotas y políticas de backup.
- **Cambiar contraseña:** permite cambiar la contraseña de autenticación del atente. Esta debe ser modificada tanto en la consola de administración como en el agente.
- **Inhabilitar cuentas de usuarios:** Puede inhabilitar cuentas de usuarios y eliminarla del servicio. Si ya se encuentra deshabilitada, puede usar la opción para volver a activar al usuario.
- **Borrar usuario:** Esta opción permite borrar por completo la una cuenta de usuario del sistema. Esta opción también elimina los datos respaldados en el servidor.
- **Establecer cuotas del usuario:** Esta opción permite incrementar o disminuir el espacio asignado por usuario.
- **Borrar cuenta del usuario:** Esta opción eliminar los datos respaldados en el servidor de Data Safe.
- **Abrir política:** Esta opción permite ver y editar la política asociada al usuario. La modificación de la política es también aplicada a los grupos y usuario que usen esta política.
- **Recuperar la clave de encriptación:** Use esta opción para recuperar la contraseña de cifrado de los backups para el usuario seleccionado.

- **Restaurar backup localmente:** Esta opción permite restaurar el backup del usuario seleccionado de manera local.
- **Exportar logs:** Esta opción permite exportar los logs del agente con fines de verificación.
- **Propiedades:** Se muestra información adicional de los equipos de los usuarios.

Estado de los Backups

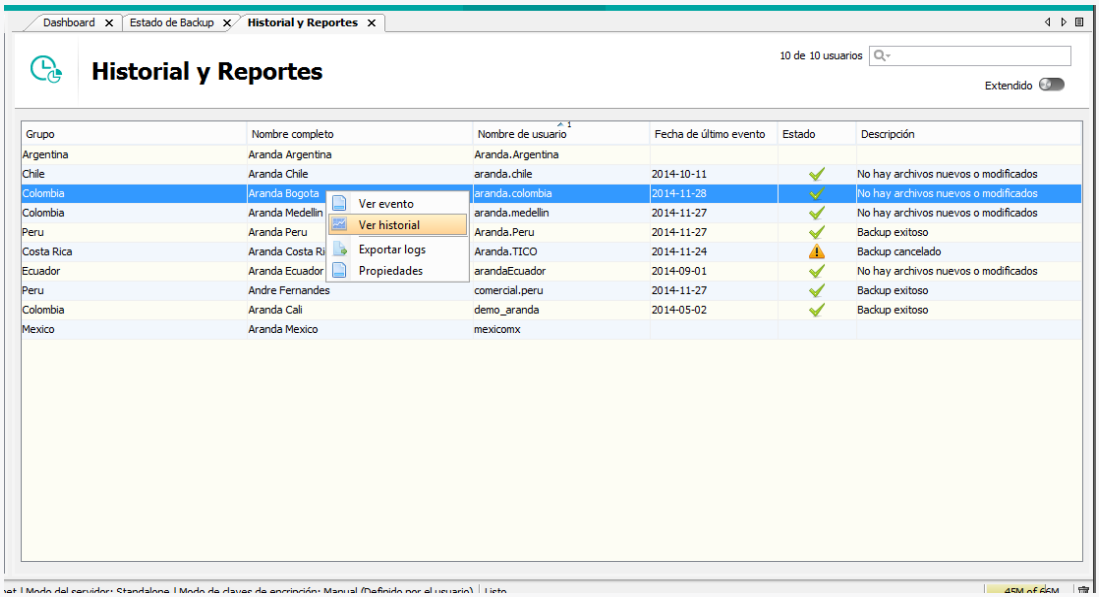
Centro de control

La notificación de eventos de backups está disponible para todos los usuarios en la consola de administración. Esta característica permite a los administradores ver informes que muestran el estado de los respaldos de un usuario, tamaño, la duración, el resumen de datos e información variada otra cuenta, incluyendo algunas de las funciones de gestión.



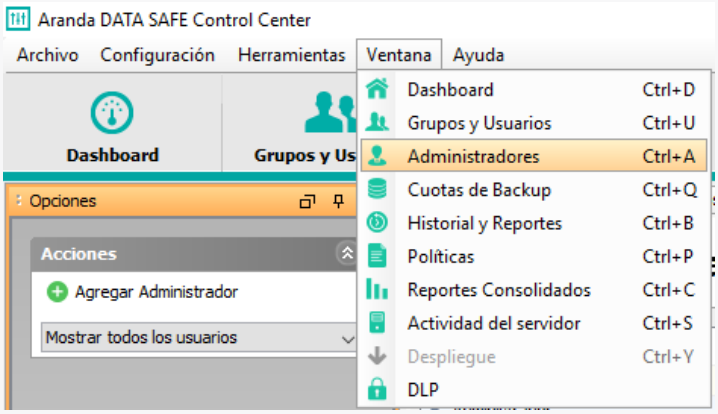
Para ver el historial y eventos de los backups por los usuarios, nos ubicamos en las opciones de la barra superior, “Ventana” y seleccionamos “Historial y Reportes”, donde se podrá ver los eventos por usuarios de respaldos y restauraciones realizadas. Además de esto se mostrarán reportes por cada uno de los eventos generados en la consola los cales pueden ser exportados a diferentes formatos.

Para ver el historial de un usuario, se debe seleccionar uno de estos y hacer clic derecho.

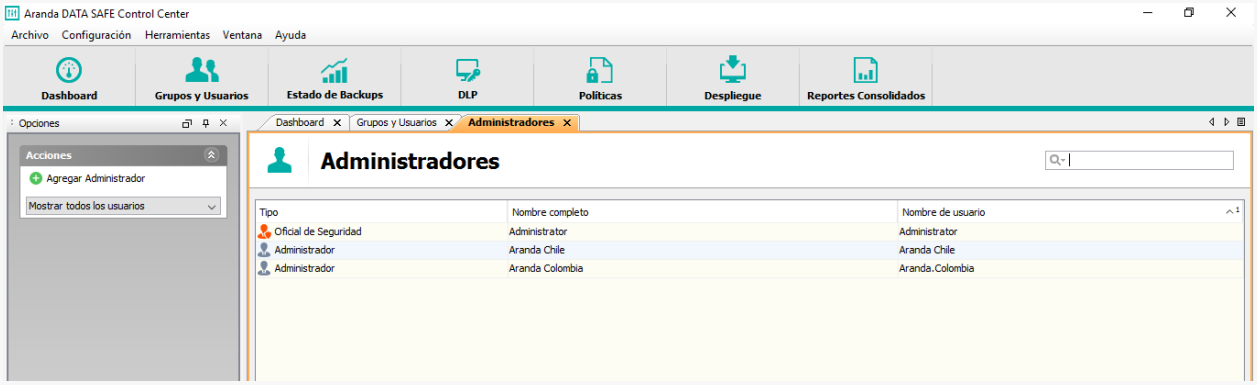


4.4 Manejo de usuarios administradores

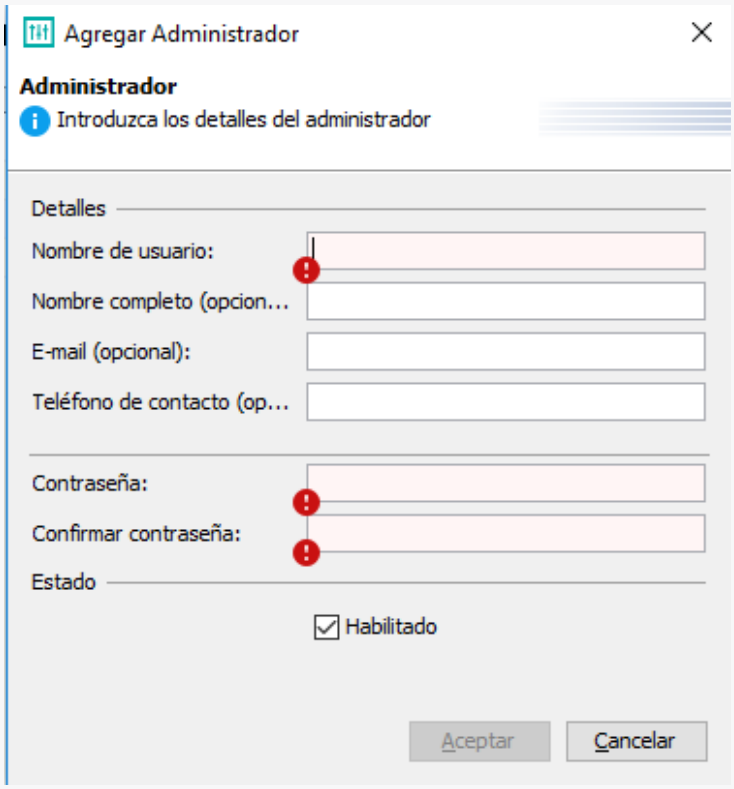
Cada persona responsable de administrar y mantener los servidores de Aranda Data Safe requiere una cuenta administradora, la cual puede ser creada en la pestaña de administradores de la consola de administración. Para abrir esta ventana, seleccione la opción administradores en la lista desplegable del menú Ventana.



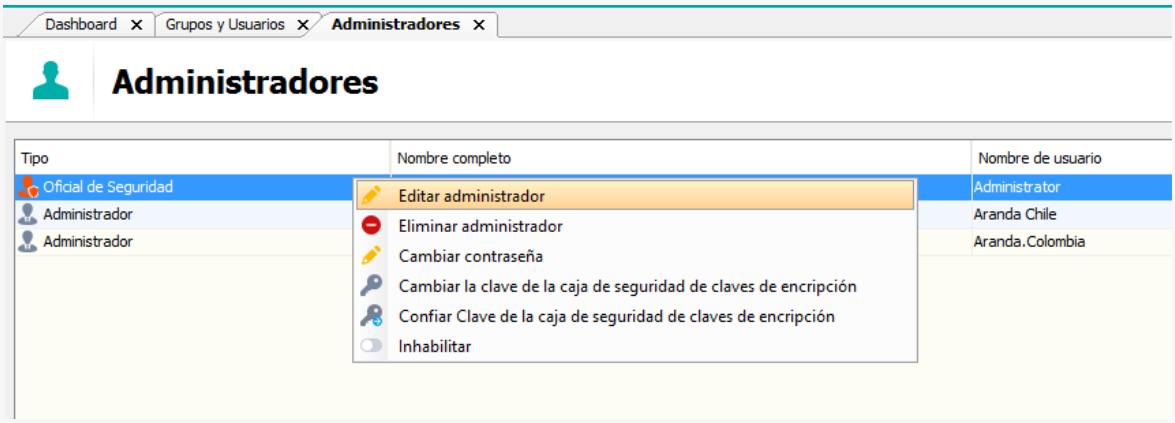
Gestión de Administradores



Para crear un usuario administrador, hacer clic en el botón **Agregar administrador** y a continuación definir los datos del mismo.



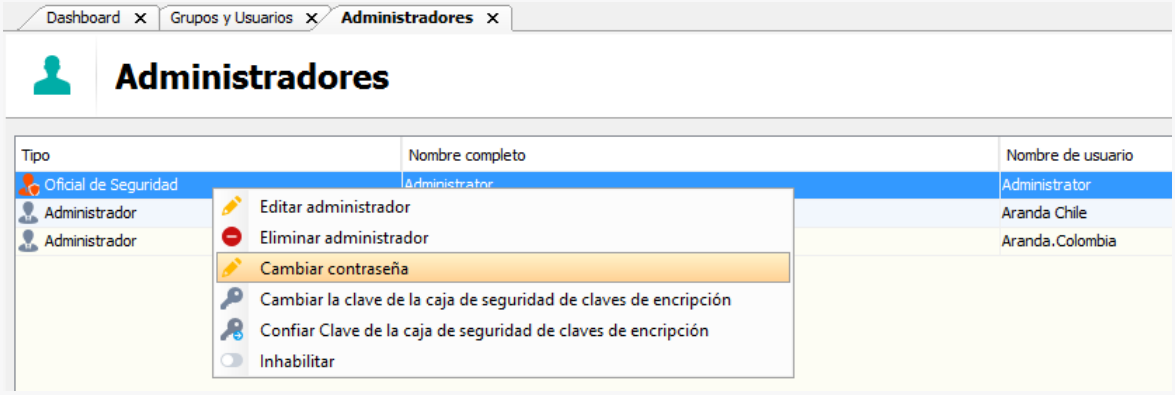
Cuando el usuario se encuentre creado podremos editarlo dando clic derecho sobre este.



Se presentan las siguientes opciones configurables sobre el administrador:

- **Editar administrador**: Se usa para modificar los parámetros de este, como lo son el nombre, correo, teléfono y contraseña.
- **Eliminar administrador:** Eliminar el administrador seleccionado para que no pueda volver a ingresar a la consola de administración

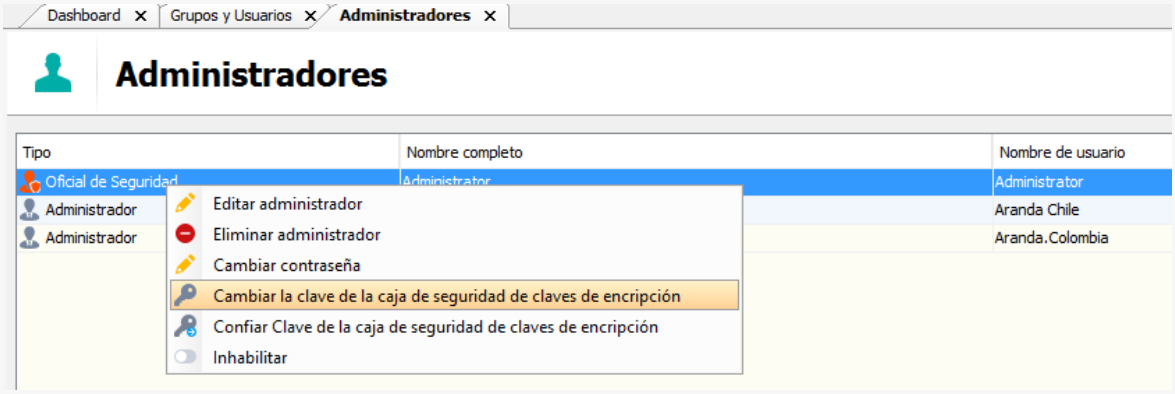
- **Cambiar contraseña:** Definido para cambiar la clave del usuario administrador
- **Inhabilitar:** Inhabilita el usuario administrador para el ingreso a la consola.



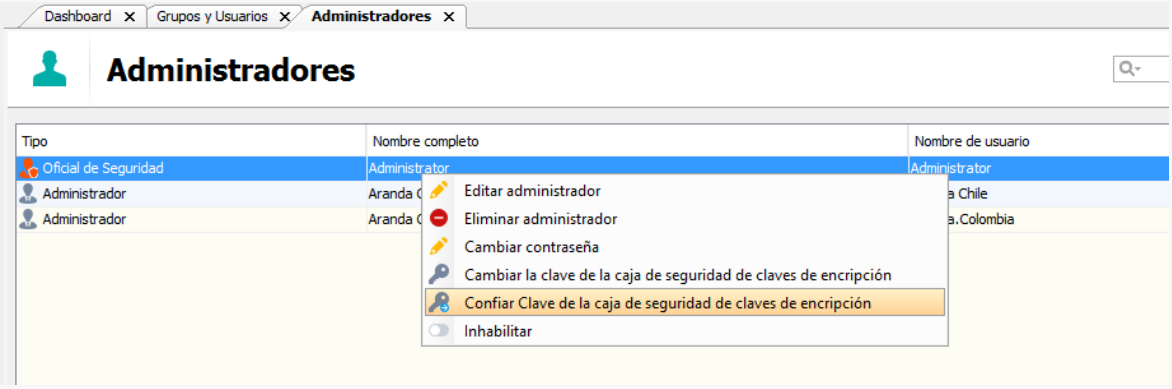
Oficiales de Seguridad
Los oficiales de seguridad son administradores de la herramienta con las siguientes funcionalidades adicionales:

- Recuperar backups de usuario finales de forma local,
- Recuperar la contraseña de cifrado de los backup de los usuarios en caso de pérdida.

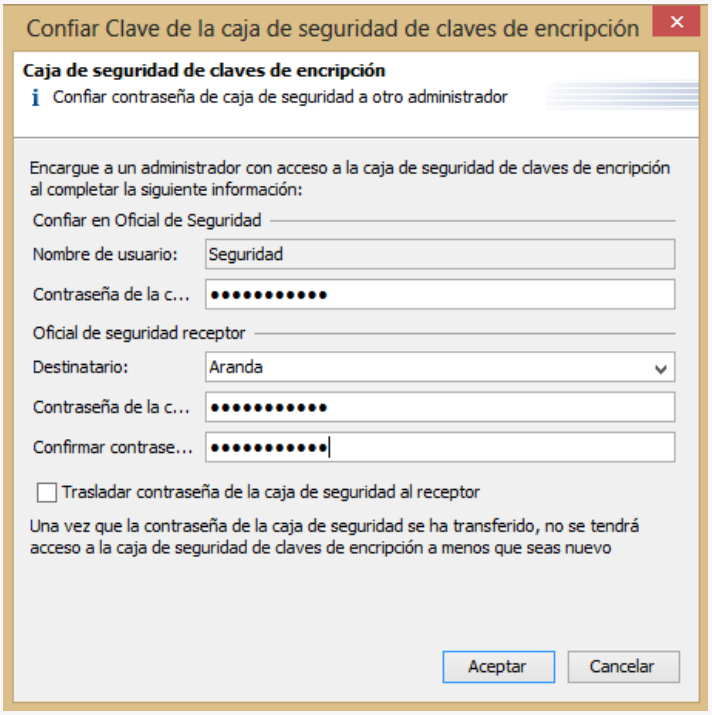
Para cambiar la contraseña de la caja de seguridad de claves de encriptación, seleccione el administrador oficial de seguridad y hacer clic derecho. Tener presente que esta contraseña es la usada para poder recuperar backups de manera local y poder recuperar las contraseñas de cifrado de los usuarios en caso de pérdida.



Para configurar la clave de la caja de seguridad de claves de encriptación, hacer clic derecho y seleccionar la opción. Esta opción permite crear nuevos oficiales de seguridad.



Se mostrará una ventana donde se debe definir la contraseña del oficial de seguridad y seleccionar en la casilla destinatario a que administrador se le dará permisos de oficial de seguridad. Luego de seleccionar el administrador, introduzca la contraseña de ese usuario.



4.4 Historial y Reportes

Aranda Data Safe ofrece opciones integrales de información para grupos y usuarios individuales de backup en formato de tabla y lista. Los informes le proporcionan las herramientas para monitorear todos los eventos de respaldo para garantizar que todos los datos se respalden con eficiencia y eficacia.

Hay cuatro opciones de fuente para la generación de informes:

- La Estado de los Backup proporciona informes para usuarios individuales dentro de los grupos asignados. Una sola vista muestra los eventos de backup para todos

- los usuarios dentro de una sola o dentro de varios grupos con opciones de desglose para mostrar los registros y los informes detallados. Ver la ficha Estado del backup.

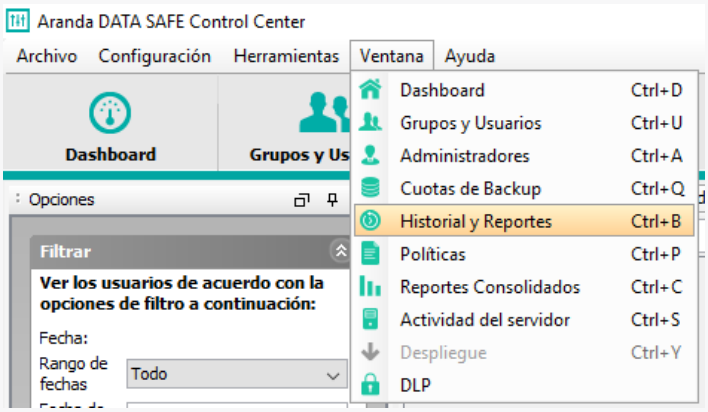
- El Historial y reportes ofrece información completa que muestra los datos específicos de eventos y filtrado para Grupos. Este punto de vista se muestra de acuerdo con los grupos con filtrado extendida para este tipo de eventos. Los datos del grupo pueden entonces también profundizar hasta Usuario historial de eventos como se discutió en Grupos y usuarios.

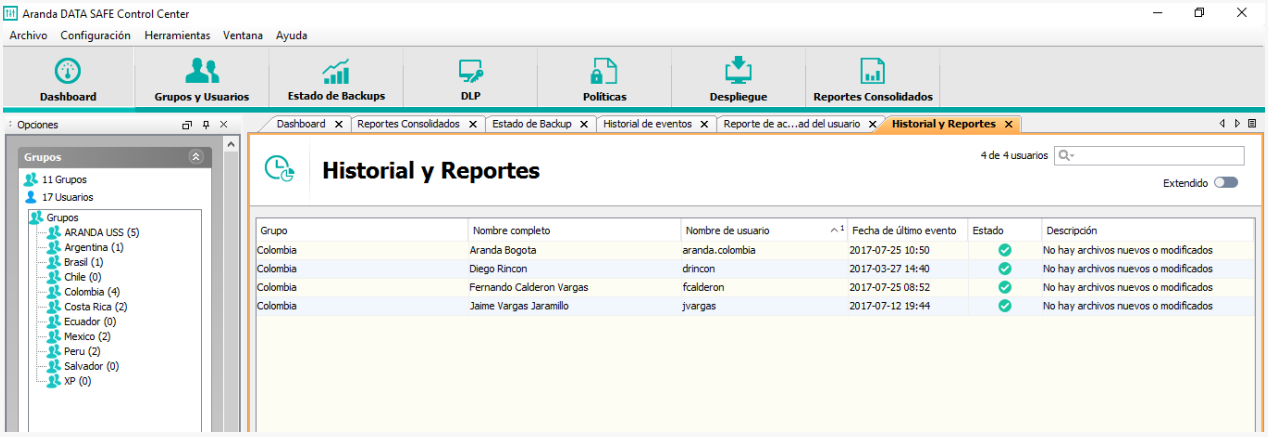
- Los reportes consolidados, proporcionan informes consolidados para todos o para los servidores seleccionados de Aranda Data Safe, dentro de la organización y de las implementaciones del directorio activo.

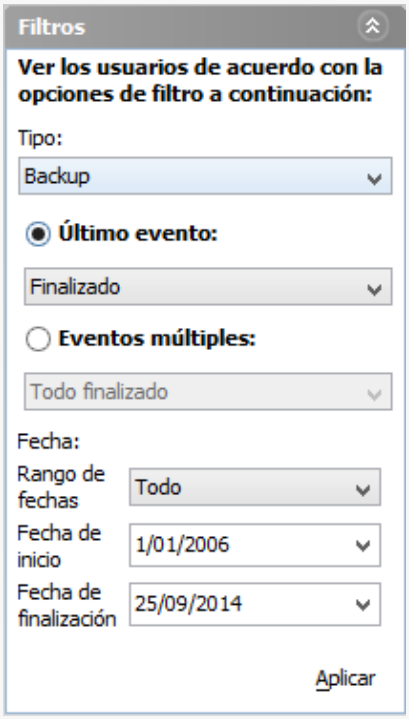
- El Dashboard, proporciona una visión general de cómo se encuentra la organización en cuanto a la protección mediante backups de la información.

Historial y reportes

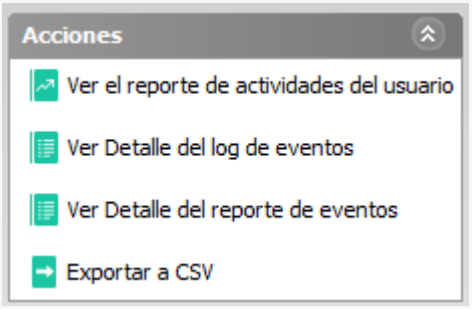
Cuando las cuentas de backup han estado activas por periodos largos de tiempo, el número de entradas en el historial de eventos será numerosa, por lo tanto, posiblemente poco manejable. La funcionalidad de filtros está disponible para ayudarle en la visualización única de la información de manera sencilla.

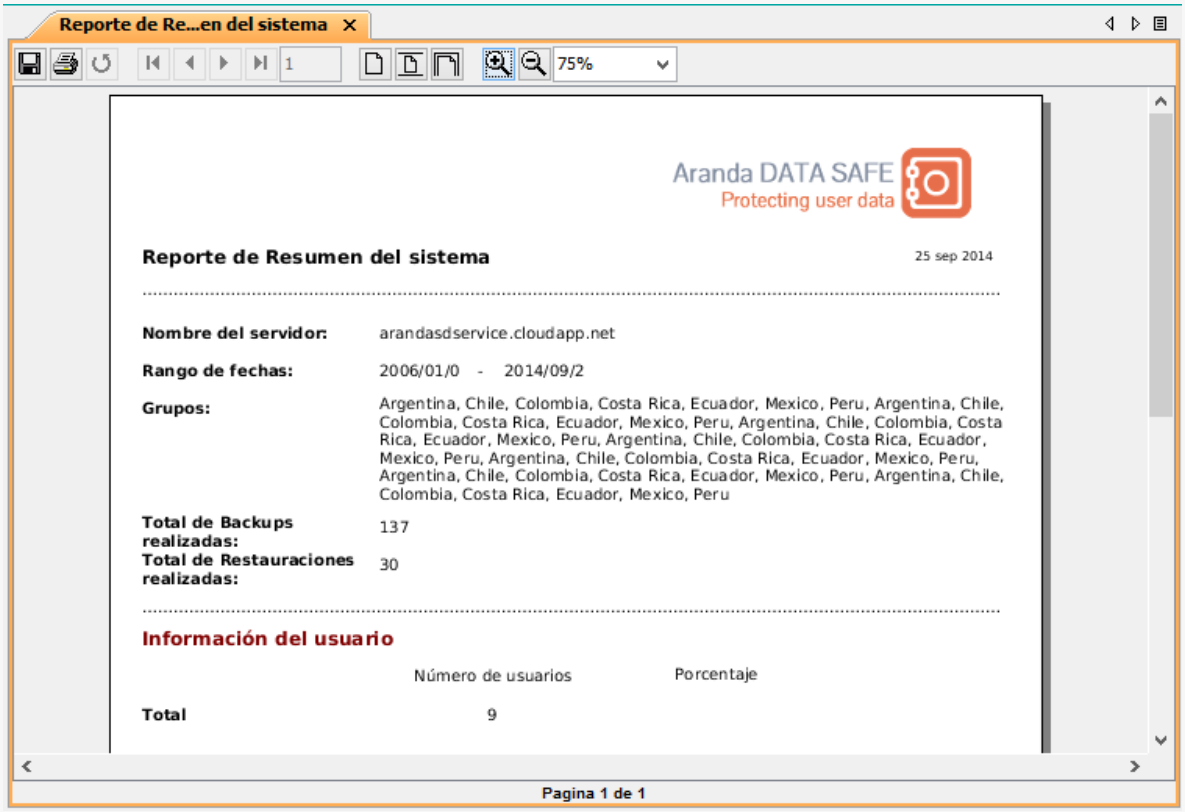






Se pueden visualizar reportes por cada evento registrado en el panel de historial y reportes mediante el panel de acciones.





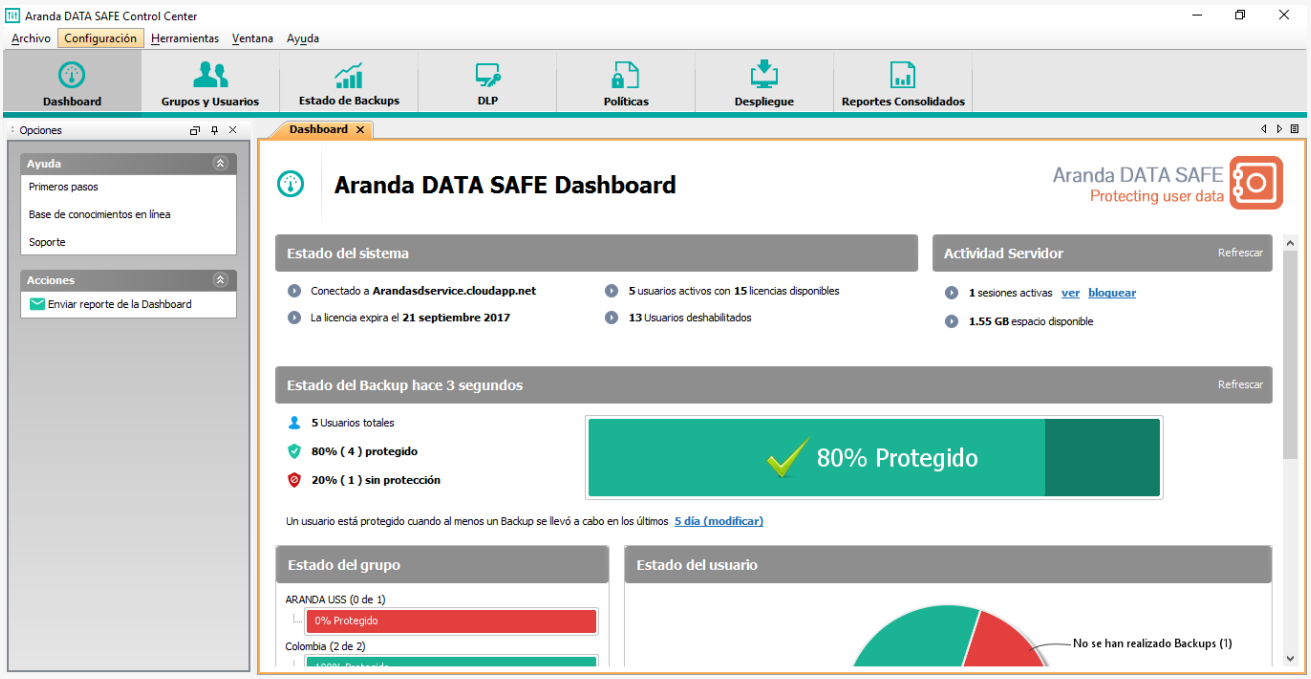
Dashboard de Aranda Data Safe

El Dashboard de la consola de Aranda Data Safe en un portal de información que le proporciona una visión general el estado de protección obtenido en el servidor de Aranda Data Safe.

Estadísticas del Dashboard

Se muestran una variedad de estadísticas e informes de estado con respecto a la concesión de licencias del Servidor de Aranda Data Safe, los usuarios activos, los grupos y el estado de protección del usuario.

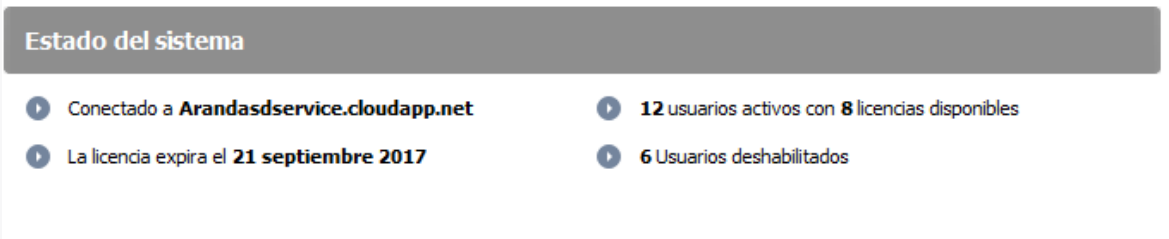
El Dashboard siempre se muestra cada vez que inicie sesión en la consola de administración y se conecte a un Servidor de Aranda Data Safe configurado.



Panel de estado del sistema

El panel de estado del sistema muestra:

- El nombre servidor de Aranda Data Safe actualmente conectado.
- La fecha de caducidad de la licencia actual.
- El número de licencias utilizadas y disponibles para el servidor conectado.
- El número de cuentas de usuario deshabilitadas en el servidor conectado.

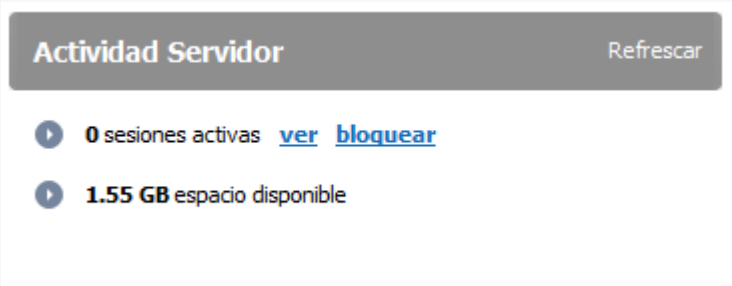


Actividad del servidor
El panel de Actividad del servidor proporciona las siguientes opciones

- **Ver** - Esta opción se utiliza para ver una lista de backups/Restauraciones en curso desde el servidor.

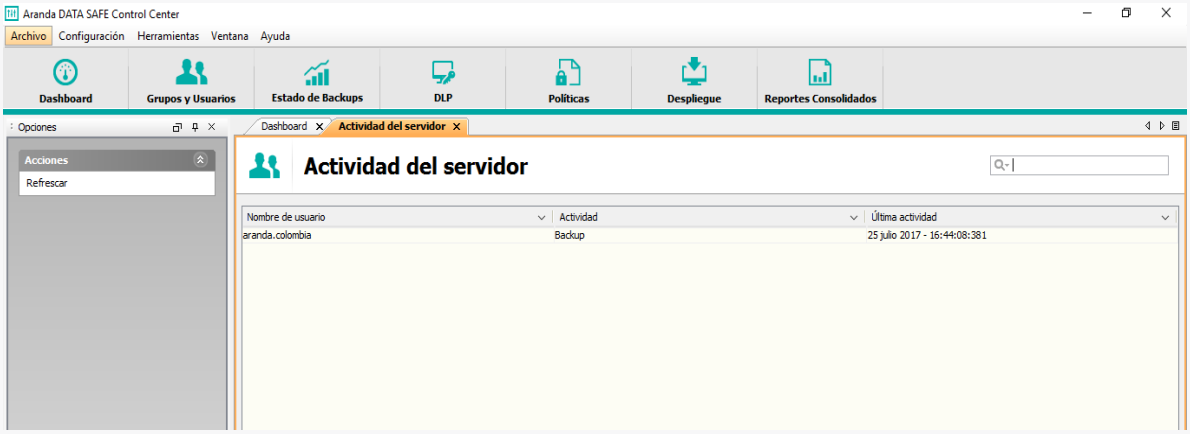
- **Bloquear** - Esta opción se utiliza para bloquear todas las nuevas conexiones al servidor.
- **Almacenamiento disponible** - Esta opción muestra la disponibilidad de almacenamiento para los datos.

El almacenamiento disponible mostrará dos valores si la ubicación de la instalación y de la ubicación de los datos se ha dividido. Durante la instalación del software de servidor de Aranda Data Safe usted tiene la opción de especificar una ubicación de almacenamiento distinta de la ubicación de la instalación.



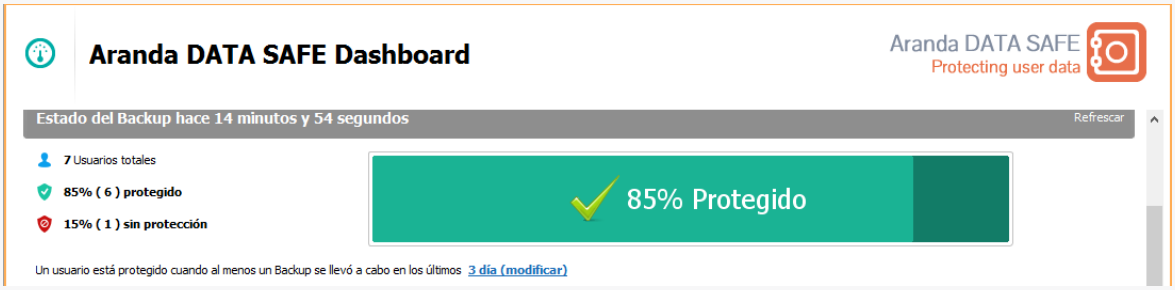
Ver actividad del servidor

Para ver la actividad del servidor, hacer clic en el botón **ver.** A continuación, se mostrarán los backup o restauraciones en curso que se realizan desde o hacia el servidor de Aranda.



Estado del Backup

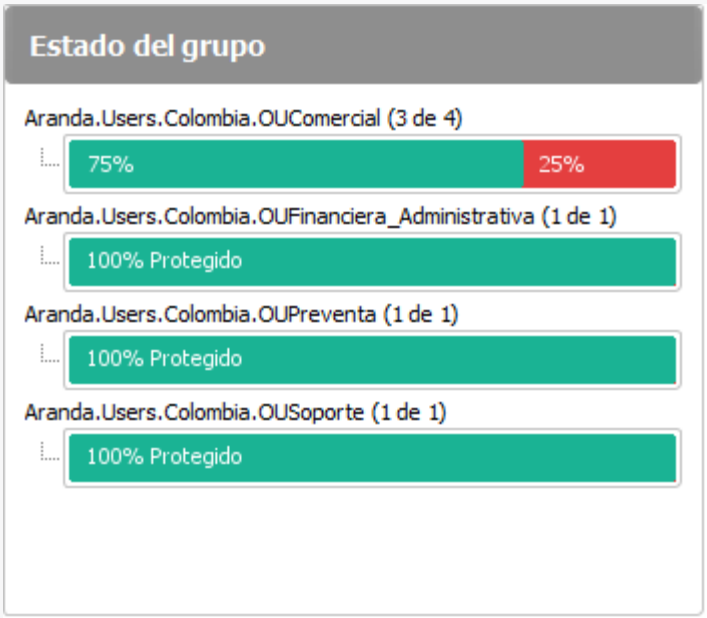
El panel Estado del backup muestra un gráfico de barras de la situación general de todas las cuentas de backup en el servidor conectado, y también muestra la relación entre el porcentaje de usuarios protegidos y no protegidos. (Haga clic en Actualizar para actualizar los datos y asegurarse de que se muestra la última información de estado.)



Los datos de estado también se pueden configurar para mostrar al menos un backup para un número determinado de días hábiles. Seleccione la opción de **x día (Modificar)**, establezca el número de días y luego haga clic en la opción Actualizar para actualizar los datos de estado. Haga clic en el Gráfico de barras para mostrar la lista de estado de backup detallado que, por defecto, mostrara usuarios desprotegidos.

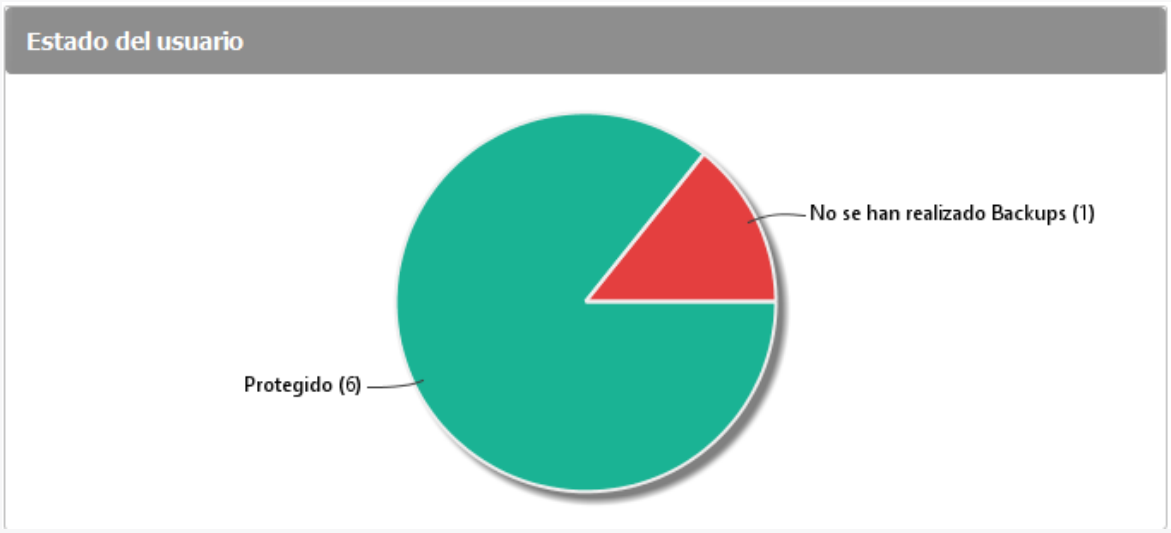
Estado de los grupos

El panel Estado de grupo muestra una lista de los gráficos de barras en el Dashboard para cada grupo de backup creados en el servidor, donde se muestra el porcentaje de todos los usuarios protegidos y no protegidos dentro de cada grupo de backup.



Estado de los usuarios

El panel Estado de usuarios muestra un gráfico circular en el Dashboard que muestra el porcentaje de todas las categorías.



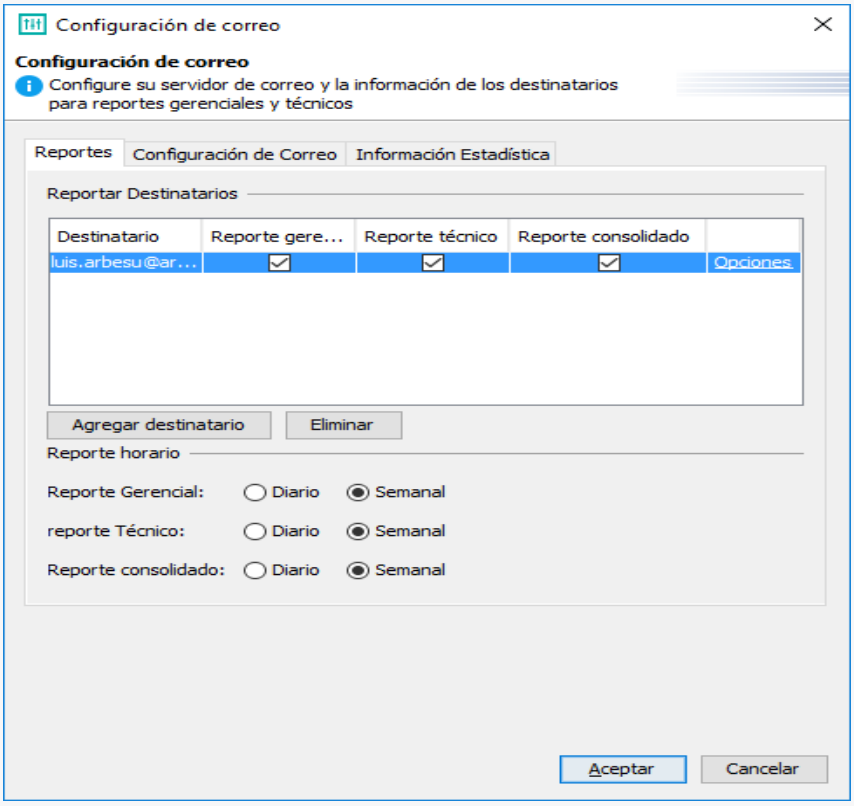
Envío de reportes por correo

Un Reporte de Dashboard con información comercial y técnica puede ser configurado para envío por correo electrónico a destinatarios seleccionados y en intervalos de tiempo especificaos como diario o semanal. Los destinatarios de los informes también se pueden configurar para recibir el grado de protección y los datos estadísticos de todos o de determinados grupos de Backup.

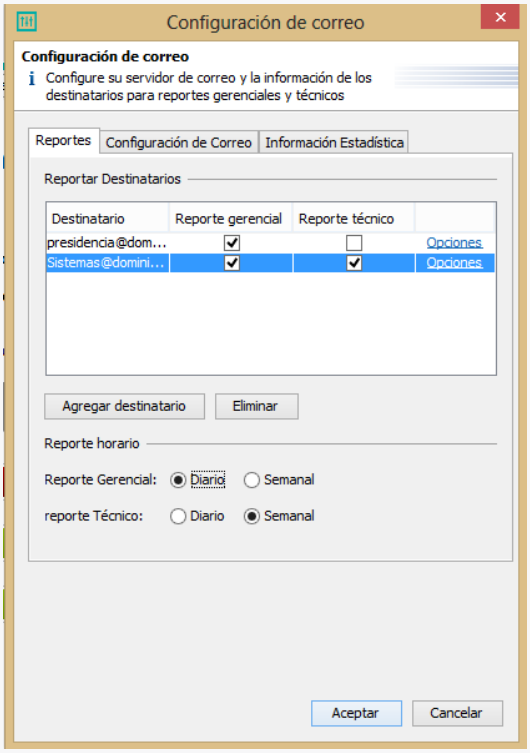
4.5 Configuración del correo

Seleccionar la opción de configuración de correo en el menú de configuración. La ventana de diálogo consiste en tres fichas: Configuración de correo, reportes y datos estadísticos.

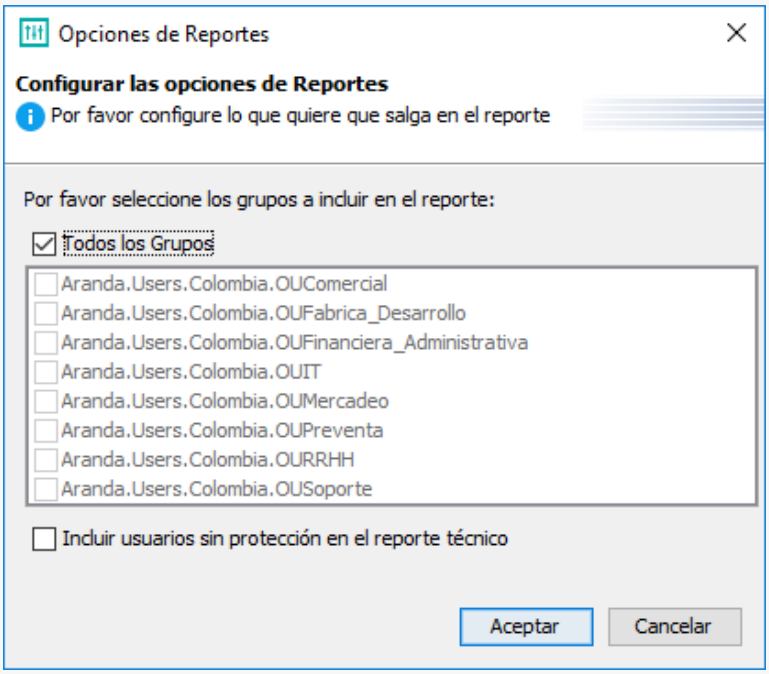
Defina el host del correo electrónico SMTP y proporcione las credenciales validas de conexión para el envío de correos electrónicos.



Definir los destinatarios a enviar los reportes, la periodicidad de envío y el tipo de reporte (Técnico o gerencial)



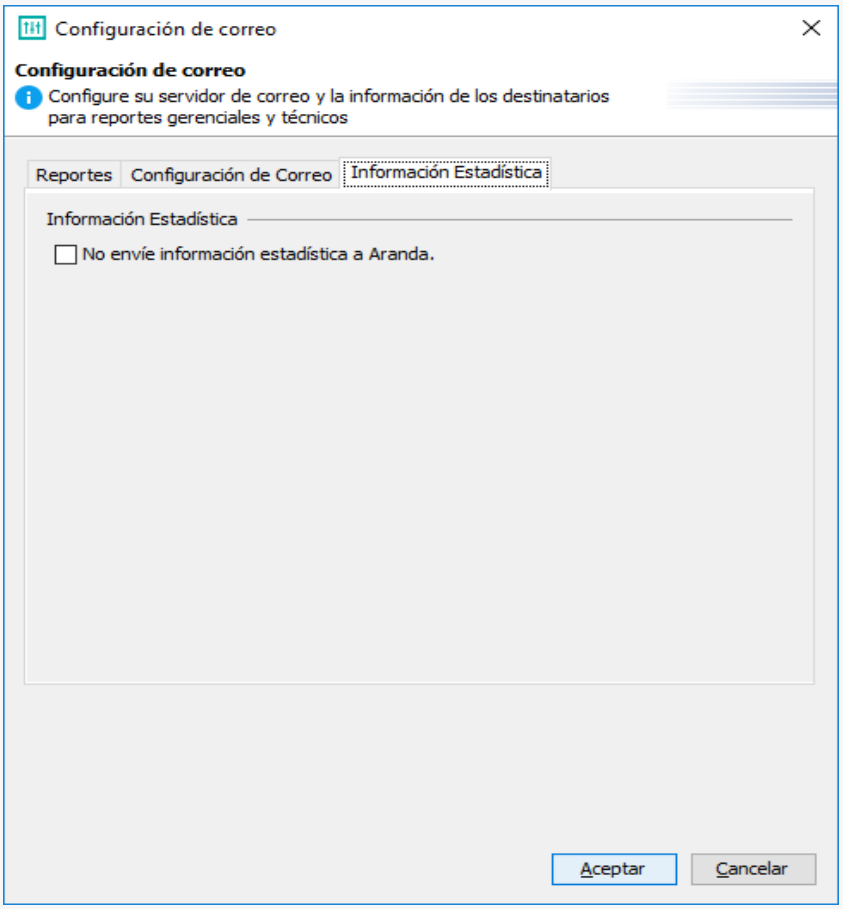
Dentro de las opciones puede definir el grupo de usuarios del quiere recibir información general de los backups.



Una característica de información estadística está disponible y activada por defecto. Esto enviará los datos estadísticos del sistema de manera anónima a Aranda.

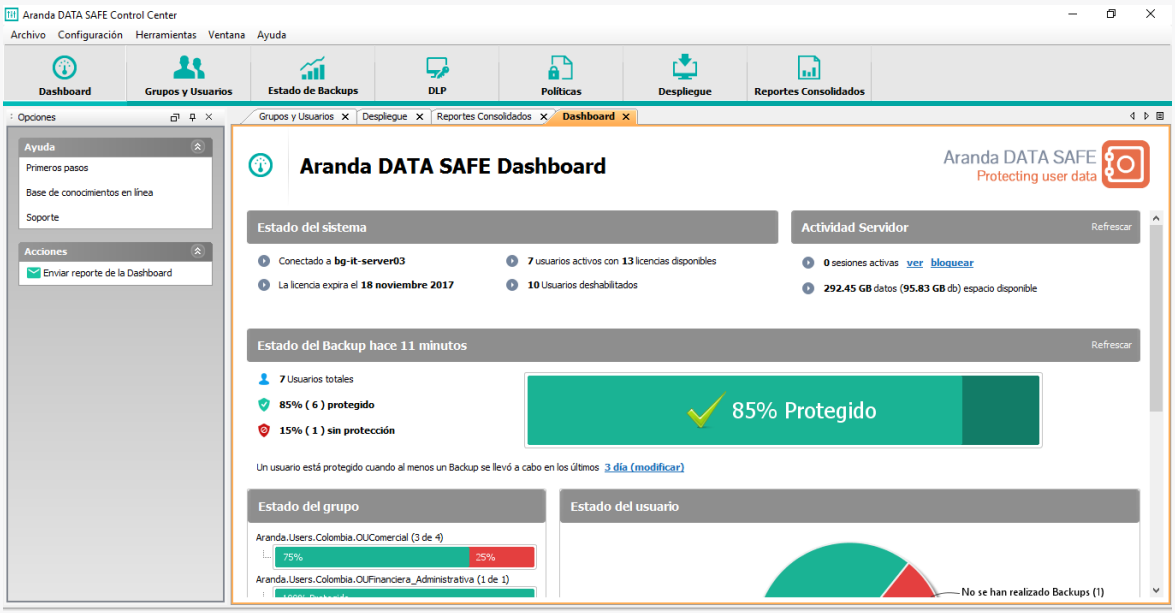
Se recomienda dejar habilitada esta opción de modo que la información vital del sistema pueda ayudar a mejorar el producto y también ayudar a la solución de problemas.

Si no desea que se envíen datos estadísticos a Aranda puede deseleccionar esta casilla.



Envío de correos electrónicos del Dashboard

El Informe Email Dashboard se puede enviar por correo electrónico de forma manual a la lista de destinatarios en la configuración de reportes por correo electrónico. Ver Configuración de correo electrónico.



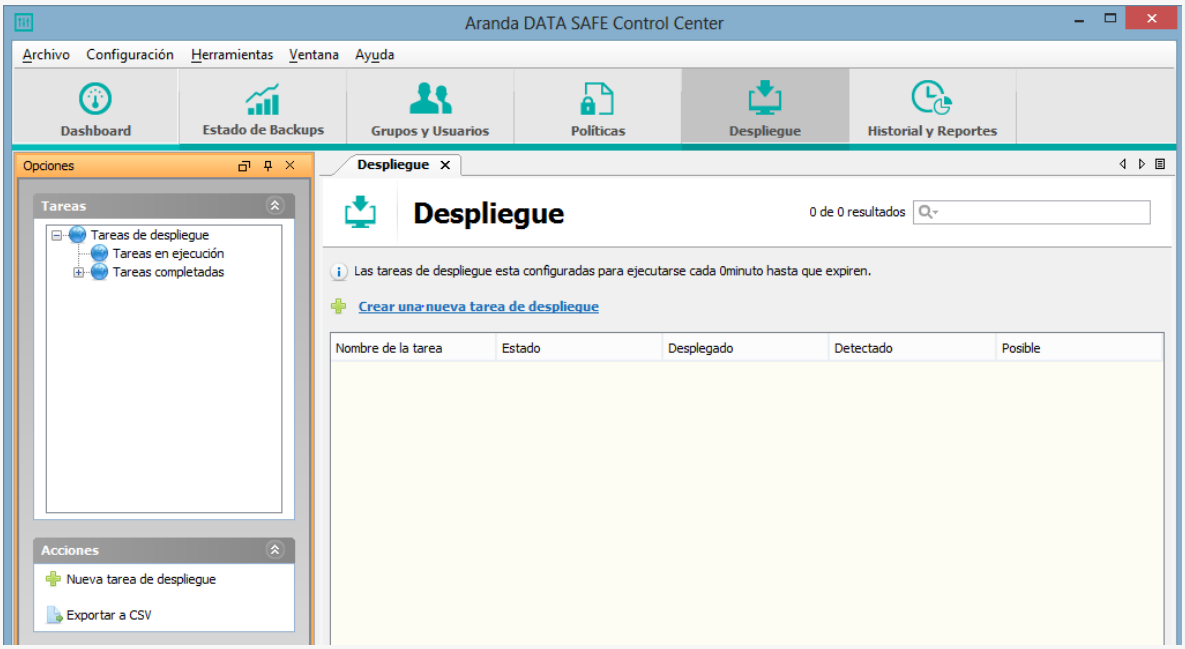
Despliegue

Los agentes de usuario de Aranda Data Safe pueden ser desplegados directamente desde el Consola de administración a un rango de direcciones IP, múltiples rangos de direcciones IP, nombres de equipos o que pertenecen a un archivo CSV. Para configurar las tareas de despliegue, seleccione la pestaña Despliegue.

Al abrir la pestaña de despliegue, una lista de tareas de despliegue se muestra por defecto. La siguiente información de resumen se proporciona para tareas en ejecución o finalizadas:

- Nombre de la tarea: Nombre descriptivo de la tarea de distribución dado por el administrador.
- Estado: Muestra si la tarea está en un estado de pausa, En ejecución o finalizado.
- Desplegado: Muestra el número total de equipos a los que el agente ha sido desplegados.
- Detectado: Muestra el número de equipos detectados dentro del rango de posibles equipos.
- Posible: Muestra el número total de posibles equipos de acuerdo con el rango de direcciones IP o un archivo CSV definido al crear una tarea de distribución.

Hacer clic en la opción Crear una nueva tarea de despliegue para crear una tarea de distribución de agentes.



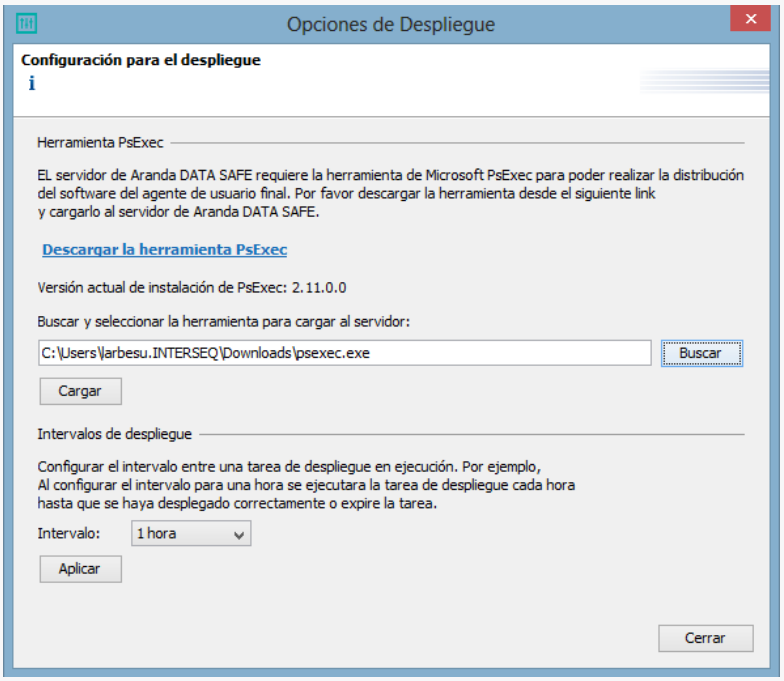
Al crear una tarea de distribución por primera vez se le pedirá descargar el aplicativo PsExec de Microsoft PSTools suite a una ubicación en el servidor. Se requiere de la herramienta PsExec para llevar a cabo el despliegue centralizado del agente final del usuario en varios equipos de la red.

Hacer clic en Configurar para iniciar el proceso.

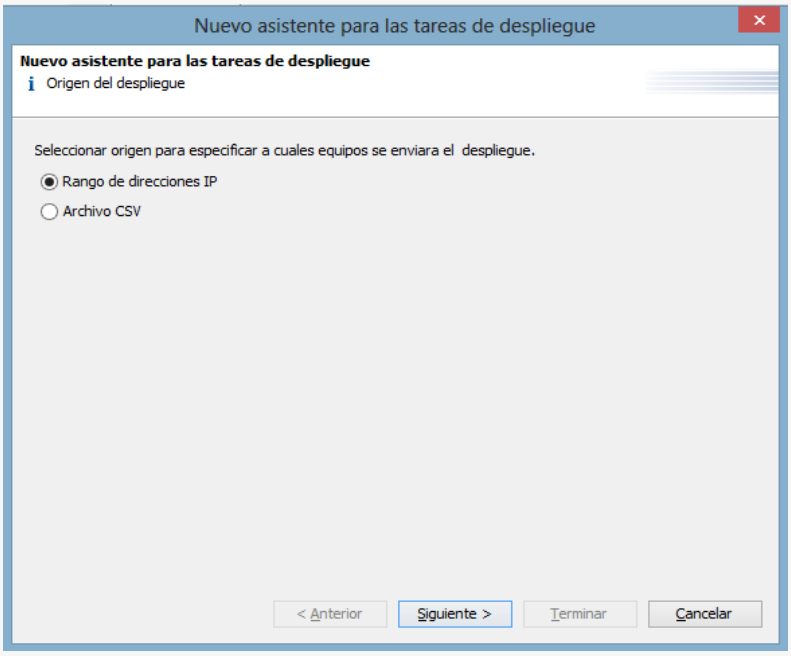
El cuadro de diálogo Configuración del despliegue será mostrado y le permite descargar la herramienta 'PsExec', para luego subirlo desde la ubicación extraída al servidor correspondiente.

Hacer clic en el enlace de descarga herramienta PsExec.

Buscar el archivo PsExec y cargarlo a la herramienta.



Luego de cargar el archivo PsExec se lanzará el Asistente para las tareas de despliegue.

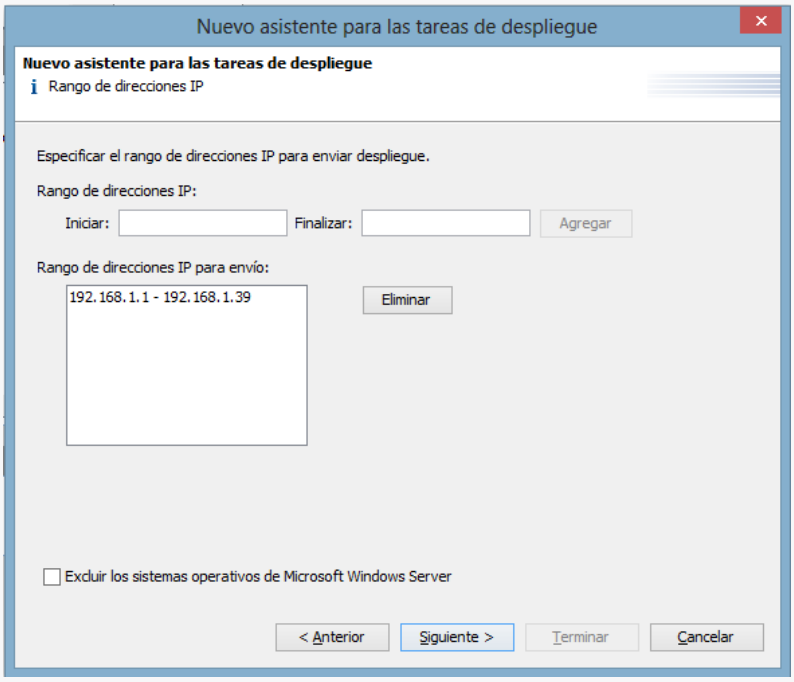


Se requiere una fuente para especificar a qué equipos se realizará el despliegue. Las siguientes opciones de fuente están disponibles:

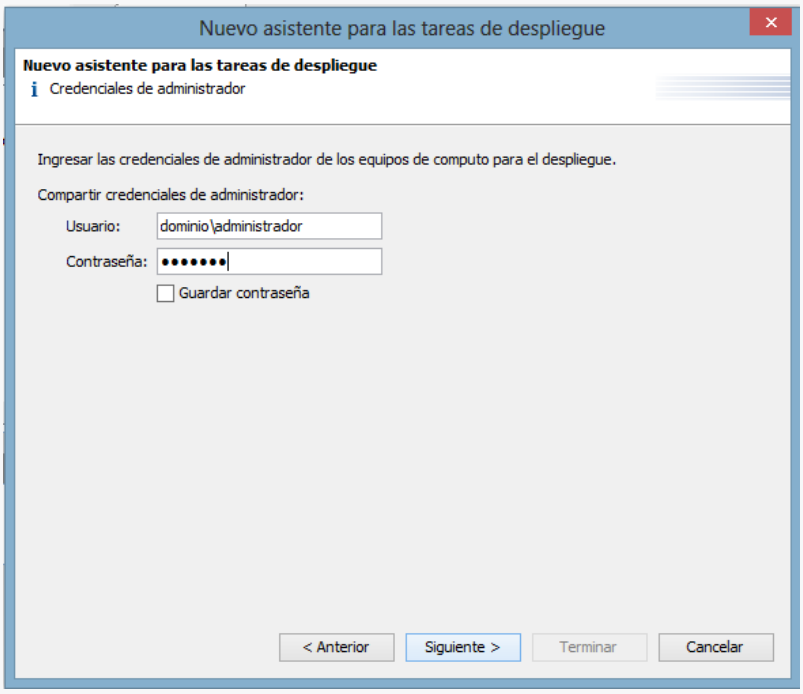
- Rangos de direcciones IP: Esta opción permite al administrador especificar un inicio y final del rango de IP dentro de su red. La tarea de distribución intentará implementar en todas las direcciones IP dentro de este rango.
- Archivos CSV: Esta opción permite al administrador especificar direcciones IP y / o nombres de host de computadora dentro de un archivo de valores separados por comas (CSV). La tarea de distribución intentará implementar en todas las direcciones IP y nombres de host informáticos especificados en el archivo CSV.

Nota: Al crear un archivo CSV asegúrese que se introduzca cada nombre de host o la dirección IP en una nueva línea dentro del archivo.

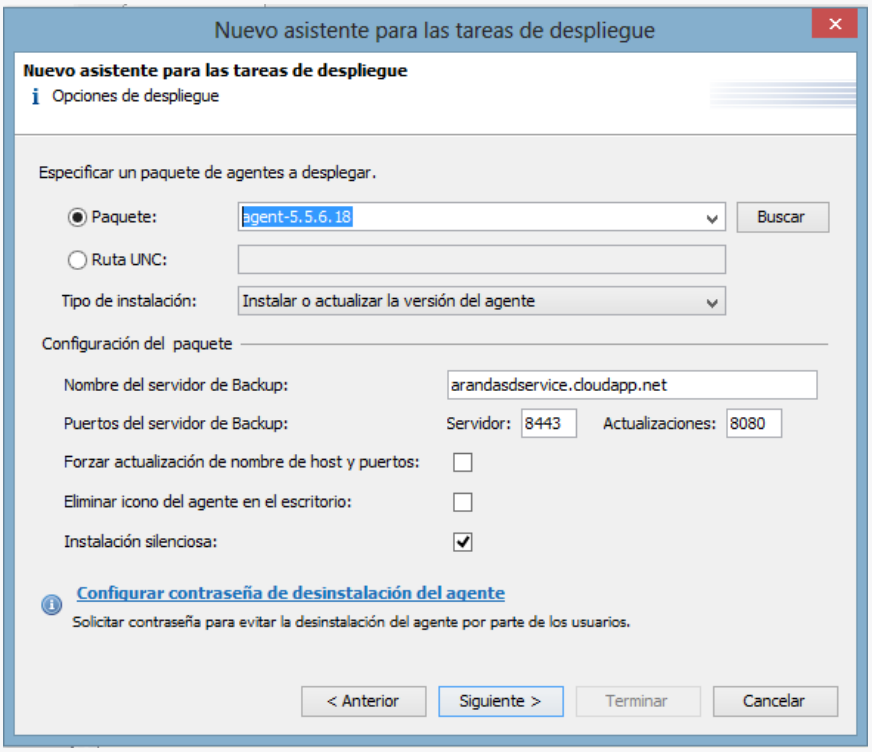
Dar siguiente para continuar.



Ingresar el usuario administrador con privilegios de instalación en las maquinas.



Hacer clic en siguiente para continuar.



4.5.1 Especifique un paquete de agente a desplegar

- **Paquete:** Introduzca el archivo MSI del agente de usuario correspondiente para subir al servidor de implementación. Este archivo de instalación del agente se instalará en cada equipo de destino en el despliegue.
- **Ruta UNC**: Se recomienda utilizar un archivo de instalación del agente que está disponible en una ruta UNC para desplegar a los equipos en un sitio diferente al servidor de implementación. Esto se realiza copiando el archivo de instalación del agente dentro de una carpeta compartida en un servidor local para los equipos que desea implementar. Es importante que la cuenta de despliegue tenga acceso a esta ubicación compartida para realizar el despliegue con éxito.

4.5.2 Tipo de instalación

- **Instalar o actualizar la versión del agente**: Seleccione esta opción si desea implementar una nueva versión del agente de usuario a los equipos destino. Para las nuevas instalaciones y actualización de los agentes de usuarios ya instalados previamente.
- **Repara la configuración actual o cambiar la configuración:** Seleccione esta opción para reparar la versión instalada del agente de usuario o volver a configurar el nombre del servidor o los puertos de Backup del servidor.

Al reconfigurar estos valores tendrá que seleccionar la opción "Forzar actualización de nombre de host y puertos".

4.5.3 Configuración del Paquete

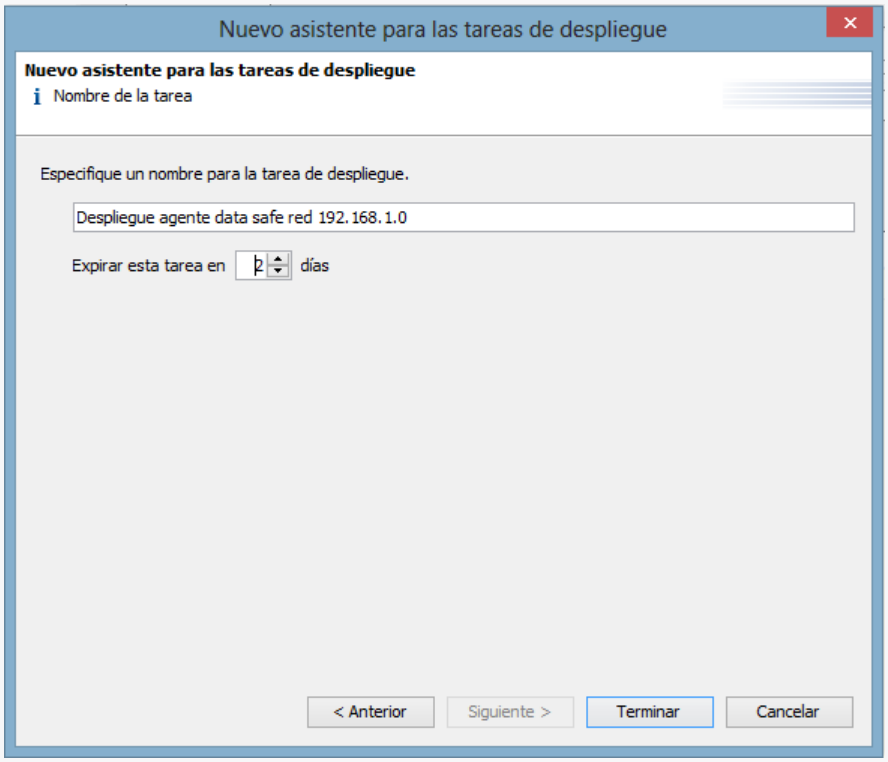
- Nombre del servidor de backup: El agente de usuario puede ser direccionado a cualquier host con el nombre del servidor Aranda Data Safe aquí definido.
- **Puertos del servidor de Backup**: El agente de usuario puede ser configurado para utilizar puertos específicos para comunicarse con el servidor de Aranda. Es importante que los agentes de usuario estén configurados para comunicarse en los mismos puertos que el servidor de Aranda.
- **Forzar actualización de nombre de host y puertos:** Seleccione esta opción si desea actualizar el nombre de host del servidor o los puertos del servidor de backup.

- **Eliminar icono del agente en el escritorio:** Seleccione esta opción si no desea que el usuario tenga un icono del agente en el escritorio del equipo.

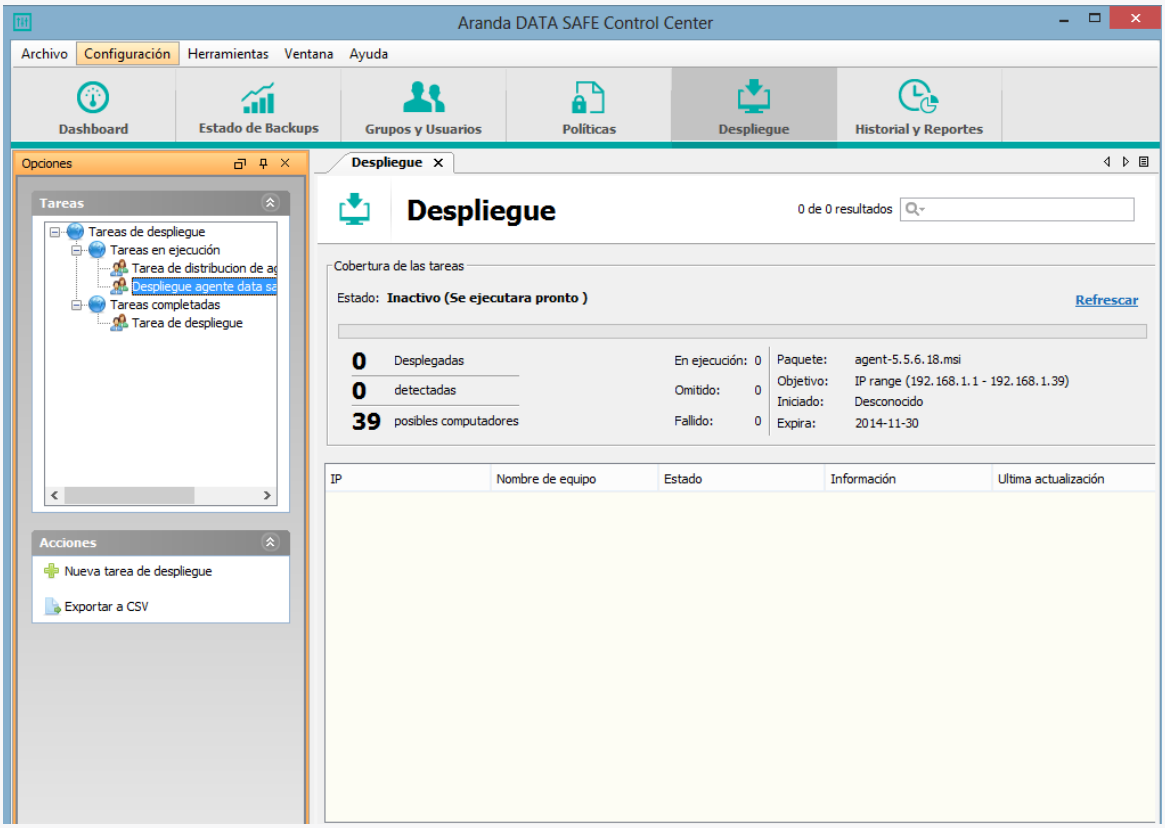
4.5.4 **Instalación silenciosa:** Seleccione esta opción si no desea que el usuario pueda ver la ventana de activación del agente de usuario en la primera puesta en marcha y activación de la cuenta.

- **Configurar contraseña de desinstalación del Agente:** Seleccione esta opción si desea configurar una contraseña que prohíbe a los usuarios desinstalar el agente de usuario desde sus computadoras. Esto también se puede configurar en el menú Herramientas de la consola de administración.

Dar en siguiente para continuar con el proceso y definir un nombre para la tarea de despliegue.



Hacer clic en Terminar para culminar la configuración de la tarea de despliegue y dar inicio a esta.



Agente usuario final

El agente de usuario es el software de Backup de Aranda que se instala en el equipo de cada usuario final de Backup. Actúa en nombre del usuario y se encarga de realizar los procesos de respaldo y recuperación.

i) Introducción al agente del usuario

- El agente de usuario comprende las siguientes características:
- Cuando se encuentra conectado al servidor de Data Safe, los datos del backup del usuario están disponibles en todo momento para su restauración.
- Los procesos de respaldo son impuestos por una política de backup asegurando que todos los datos críticos se encuentren respaldados de forma segura.
- La política de backup verifica que el agente del usuario herede los criterios predefinidos, como la selección de los datos, horarios y configuraciones.

- La política de Backup también puede bloquear la configuración, no permitiendo realizar cualquier cambio en la política guardada en el agente de usuario.
- Aranda Data Safe emplea NTFS *Journal Scanning* y requiere que los datos residan en volúmenes NTFS. Sin embargo, el agente de usuario automáticamente realizará un análisis del sistema de archivos en los volúmenes que no son NTFS.

  ii) **NTFS Journal Scanning** proporciona un registro persistente de los cambios realizados en los archivos en un volumen. NTFS mantiene los cambios diarios mediante el seguimiento de la información sobre los archivos agregados, eliminados y modificados para cada volumen.

Una solución de backup automática, como Aranda Data Safe verifica los cambios en el estado de un volumen para llevar a cabo su tarea.

Alternativamente, el método de escaneo de un volumen completo, no es aceptable debido a la disminución en el rendimiento del sistema que causaría. Además, si un gran número de directorios y archivos necesitan ser respaldados, la cantidad de procesamiento y memoria necesaria para tal aplicación podría generar que el rendimiento del sistema operativo se vea afectado.

Para evitar estos inconvenientes, el sistema de archivos NTFS mantiene un diario de cambios. Cuando se realiza algún cambio en un archivo o directorio en un volumen, se actualizan los cambios realizados con una descripción del cambio y el nombre del archivo o directorio.

- Data Safe utiliza tecnología de parches, con lo que únicamente se realiza backup a los cambios realizados sobre los archivos y no a el archivo completo.

La tecnología de parches binarios (Binary Patching Technology) compara un archivo modificado contra su versión original y extrae las diferencias entre los dos archivos en un tercer archivo, que se llama un "archivo delta". Este "archivo delta" se comprime en lo que se conoce como un "parche", el cual a menudo es del 85% a 99,9% más pequeño que el archivo original. Como tal, Binary Patching reduce significativamente el tiempo y ancho de banda requerido para completar un Backup.

- Con las características avanzadas de Aranda Data Safe, como *Patching Technology* y *NTFS Journal Scanning* siendo utilizados, el agente de usuario logra realizar backups diarios de manera más rápidas.
- Aranda Data Safe emplea VSS (Microsoft Volume Shadow Copy) para realizar backups de archivos mientras están en un estado abierto.

Microsoft Volume Shadow Copy crea una imagen de los datos de backup después de haber sido activado por el servicio del agente de Data Safe.

Data Safe realiza un backup de esta imagen para asegurar que los archivos no están bloqueados mientras que esta es respaldada. Si el servicio Volume Shadow Copy se encuentra fallando o el servicio del Agente de Data Safe Cibecs no es ejecutado, el backup puede encontrar archivos bloqueados.

Dentro del alcance de este manual no se discutirá como se realizan los cambios de políticas de Backup dentro de la consola del usuario final. Para más información para definir una política de Backup por favor ir a **Definiendo Políticas de backup**.

Opciones de instalación del Agente de Usuario

Para poder usar o desplegar un agente de usuario, es necesario someterse a una cierta configuración, en términos de dirección. Esta dirección significa que el agente sabe con qué servidor se debe asociar y que política de Backup utilizará.

La solución de Aranda Data Safe contiene el paquete de implementación del Agente de Usuario. Este archivo es un paquete de instalación y no contiene ninguna información dirigida servidor.

IMPORTANTE: Todos los agentes de usuario deben ser direccionados a un servidor de Aranda Data Safe antes del despliegue.

Existen 3 métodos distintos para crear un paquete para la instalación del agente del usuario final. Usando las Opciones de despliegue definidas en la consola de administración durante la configuración inicial del servidor de Aranda Data Safe.

Usando las opciones del agente dentro de las opciones de herramientas en la consola de administración. Mediante el archivo MSI se puede realizar la instalación, el cual acepta parámetros en la línea de comando que le permite aplicar el nombre correcto del servidor de Aranda Data Safe.

Definiendo la configuración del agente

Existen 3 métodos que pueden ser usados para definir la configuración inicial del agente. Defina cuál es el método que mejor se acopla a su organización para realizar los despliegues de los agentes.

Opciones de instalación del agente desde el menú de la consola de administración

- La opción de instalación del agente le proporciona opciones para crear paquetes de instalación Básico y Avanzado.
- Al crear un paquete de instalación, se incluye toda la información necesaria del servidor de Aranda Data Safe y no se necesitan parámetros de instalación.
- Si tiene varios servidores Aranda Data Safe dentro de su organización, debe generar un paquete de instalación para cada servidor.
- La opción avanzada (Automatizada) de instalación construye un paquete para la instalación basada en directorio activo.
- La opción Básica (Manual) de instalación crea un paquete de instalación desatendida que se recomienda para entornos donde no se tiene un Directorio Activo configurado.
- Consulte las opciones de instalación del agente.

Creación de un paquete de instalación del agente desde las opciones del menú de la consola de administración

- Esta opción es una alternativa a la opción de instalación básica.
- Cuando la construcción de un paquete de despliegue, un nuevo paquete de instalación del agente es creado, el cual incluye toda la información necesaria del servidor de Aranda Data Safe.
- Esta opción crea un paquete de instalación desatendida que se recomienda para ambientes donde no se tiene un directorio activo.
- Ver Crear paquete de instalación del agente.

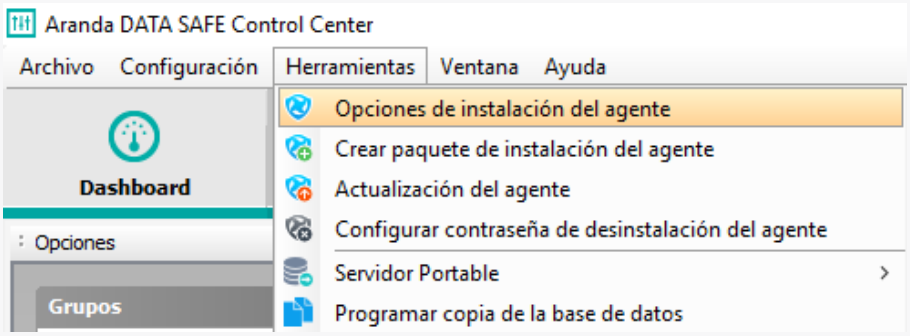
Usando parámetros de instalación

- Los paquetes de instalación agent.msi aceptan una serie de parámetros para su instalación. Estos parámetros le permiten definir el nombre del servidor de Aranda Data Safe dentro del agente del usuario final. Esta opción puede ser la preferida para soluciones automatizadas de despliegue de software.
- Ver Instalación del agente usando parámetros.

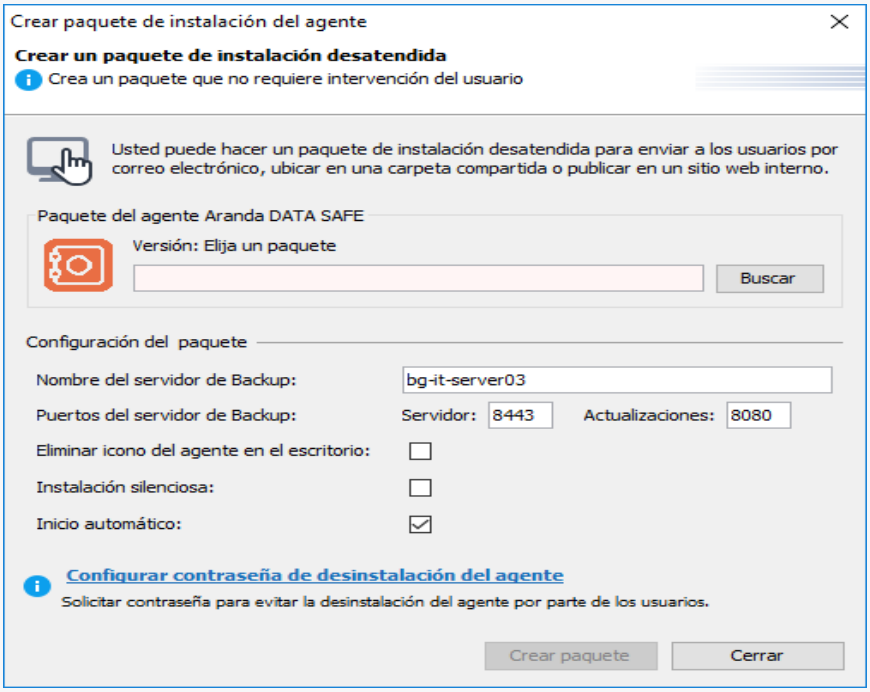
Creación del paquete de instalación del agente del usuario

Para crear un paquete de instalación de una instalación basada en GPO del Directorio Activo, se puede usar la consola de administración por el administrador para crear un agente con una configuración específica "agente-<Servidor>.msi", el cual puede ser utilizado para el despliegue manual o automatizado.

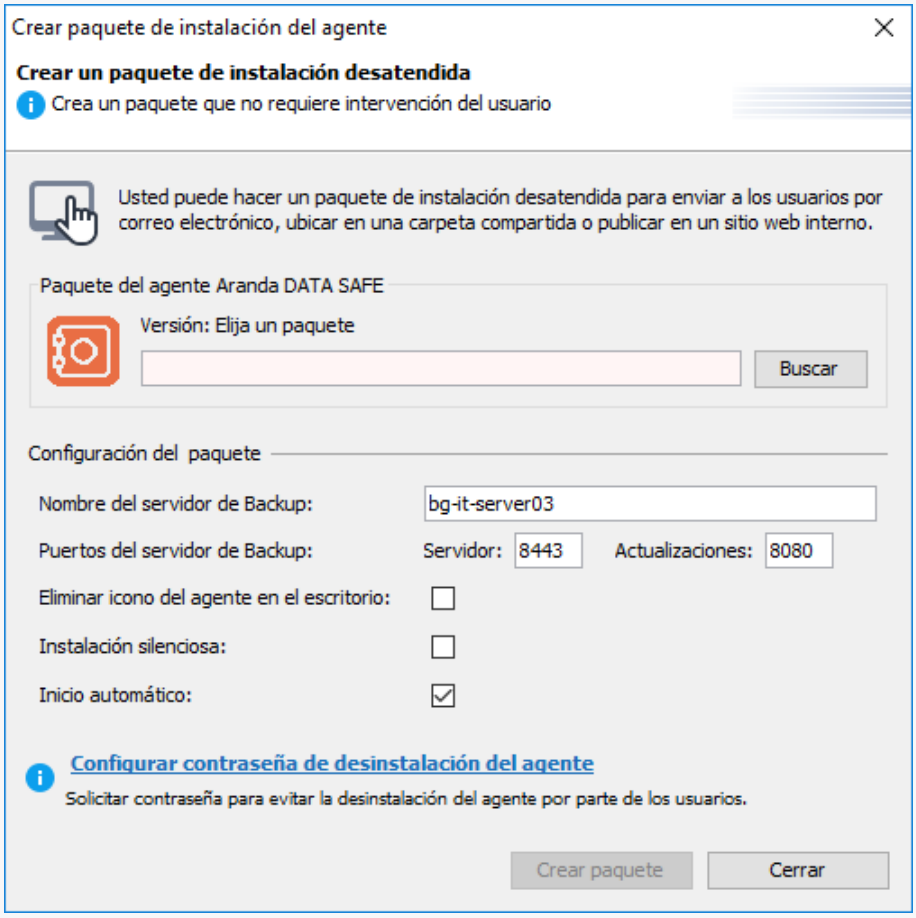
Abrir las **Herramientas** del menú



Seleccionar la opción **Opciones de instalación del agente.**



Debajo de la opción **instalación automática** para la instalación basada en el directorio activo por política de GPO, hacer clic en **Crear paquete de Instalación.**



La dirección IP o el nombre del servidor de Aranda Data Safe al que está conectado se introduce como el nombre de host del servidor de Backup. Este es el nombre de host del servidor al que se asocia el archivo del agente de usuario de final.

- Si el nombre de host no es la del servidor que desea asociar al agente de usuario, puede introducir el nombre de host o IP del servidor alternativo de Data Safe requerido.

- Haga clic en el botón **Buscar** ubicado junto al campo paquete del Agente Aranda DATA SAFE y busque el archivo de instalación de agente.

Por defecto, el agente de usuario se comunicará con el servidor de Aranda Data Safe por los puertos 8443 y 8080. Se pueden usar puertos diferentes a los usados por defecto.

Seleccione **Eliminar icono del agente en el Escritorio** si no desea que se visualice el agente del usuario en el escritorio del equipo del usuario final.
Seleccione la opción **Instalación silenciosa** para crear un paquete de Data Safe que será instalado sin la intervención del usuario.
Seleccione **Inicio Automático** si desea que el agente se inicie luego de la instalación. Esto no es recomendado cuando se utiliza la opción de despliegue automático para instalar el agente del usuario.

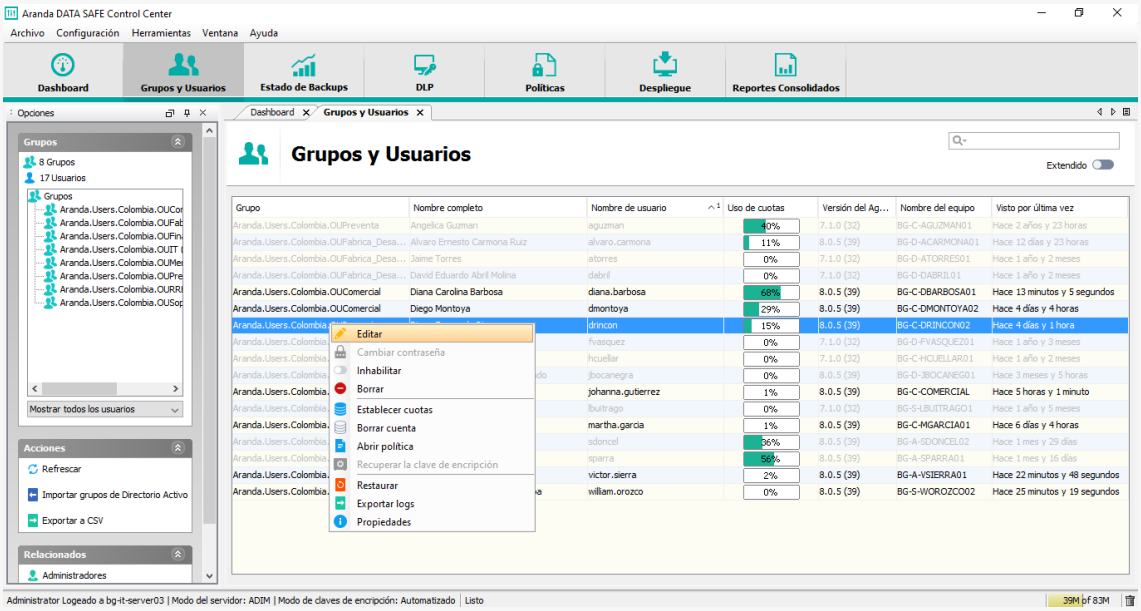
Hacer clic en **Crear Paquete** para iniciar y crear el paquete del agente del usuario final.

Deshabilitando cuentas de backup

Propósito:	Deshabilitar las cuentas de backup inactivas y liberar la licencia del Agente de un usuario. Los datos de la cuenta del backup de seguridad se conservan en caso de que se requieran recuperar información.

Se pueden deshabilitar varios usuarios simultáneamente utilizando las funciones de edición múltiple.

Procedimiento:
Para deshabilitar una cuenta de backup: Seleccione la pestaña Grupos y usuarios en el Centro de control.



Hacer Clic derecho en el usuario a deshabilitar y hacer clic en deshabilitar.

Los datos de la cuenta de backup se conservan. La cuenta no se mostrará y no se incluirá en los informes de copia de seguridad.

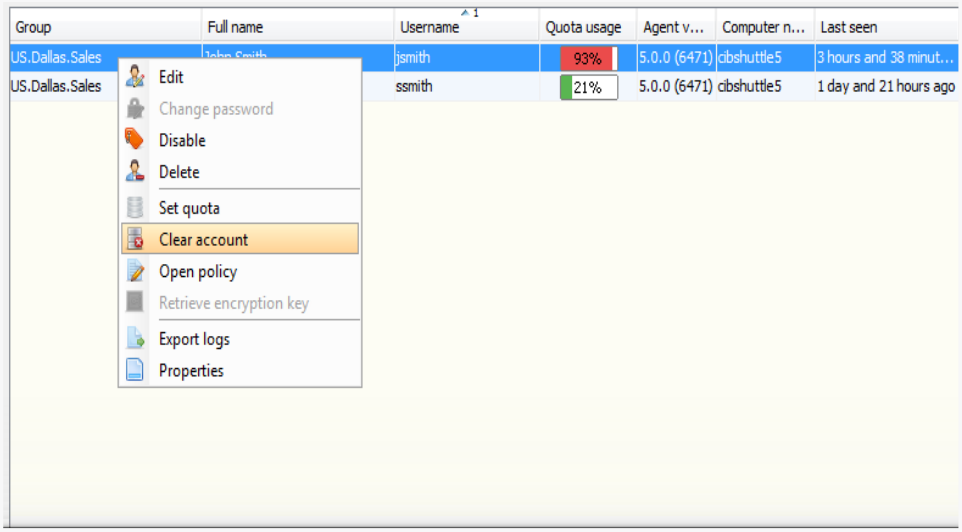
Eliminación de la cuenta de respaldo

Propósito:	El borrado de la cuenta de backup suele tener lugar cuando una cuenta de usuario se ha desactivado durante un tiempo de acuerdo con la política de la empresa y todos los datos deben ser eliminados.

Se pueden borrar varios usuarios simultáneamente usando las funciones de edición múltiple.

Procedimiento

Para borrar una cuenta de backup: Seleccione la pestaña Grupos y usuarios en el Centro de control.



Haga clic con el botón derecho del ratón en la cuenta backup del usuario y seleccione la opción Borrar cuenta de usuario. Los datos de usuario se eliminan inmediatamente.

Recuperación de datos

Frecuencia:	Cuando se requiera.
Propósito:	Recuperar datos críticos del negocio de una cuenta de backup inactiva.
Procedimiento:	La recuperación de datos de una cuenta de backup inactiva se realiza de la misma manera que la de una cuenta de respaldo activa.
Nivel:	Oficial de seguridad de Data Safe.
Propósito:	Realizar recuperación de los datos seleccionados o de cualquier dato que se haya borrado, perdido o dañado, a la estación de trabajo original del usuario.

Procedimiento:	Un usuario puede recuperar los datos en la ubicación original o en una ubicación especificada mediante el asistente de restauración simple. Para realizar una recuperación a la estación de trabajo original:

Iniciar el agente de usuario.

Seleccionar el botón **Restaurar** en la barra de herramientas.

Hacer clic en **Siguiente** en cada paso para seguir el proceso de recuperación impulsado por el asistente.

Paso 1: Seleccionar la fecha de copia de seguridad que desea restaurar. De forma predeterminada, se selecciona el último conjunto de copias de seguridad.
Paso 2: Seleccionar las carpetas y archivos que desea restaurar. Esto podría ser todos o sólo archivos especificados.

Paso 3: Seleccionar la ubicación en la que desea restaurar. De forma predeterminada, se selecciona la ubicación original.

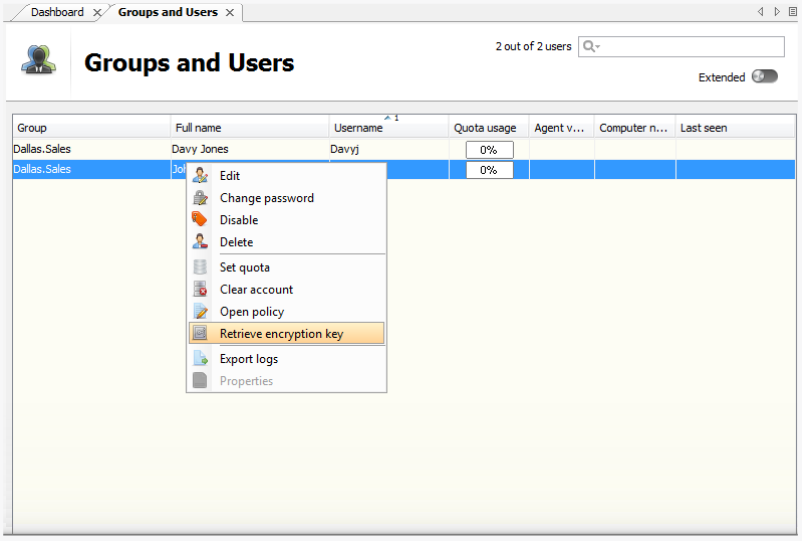
Hacer clic en **Finalizar** para iniciar la recuperación.

Recuperación a una nueva estación de trabajo

Propósito:	Realizar una recuperación de los datos seleccionados o de todos los datos en una nueva estación de trabajo. Esto puede ser necesario, si la estación de trabajo original fue dañada o robada.
Procedimiento:	Para restaurar a una nueva estación de trabajo, la clave de cifrado del usuario es necesaria antes de que se puedan restaurar los datos. Sólo los ofíciales de seguridad asignados pueden proporcionar claves de cifrado.

Esto es válido únicamente cuando se ha seleccionado la función de seguridad de cifrado independiente. Para recuperar la clave de cifrado de un usuario en el Centro de control:

Seleccionar la pestaña Usuarios y grupos.



Hacer clic con el botón derecho en la cuenta del backup del usuario y seleccione la opción Recuperar clave de cifrado.

El oficial de seguridad debe ingresar una contraseña segura válida para mostrar la clave de cifrado del usuario. La clave de cifrado debe mantenerse a salvo en todo momento y debe descartarse inmediatamente después de haber sido utilizada durante el proceso de activación de la cuenta.

Para realizar una recuperación en la nueva estación de trabajo: Instalar e inicie el software de User Agent. Ingresar la clave de cifrado para activar el agente de usuario recién instalado.

Seleccionar el botón Restaurar en la barra de herramientas.

Hacer clic en Siguiente en cada paso para seguir el proceso de recuperación controlado por el asistente.

Paso 1: Seleccionar la fecha de copia de seguridad que desea restaurar. De forma predeterminada, se selecciona el último conjunto de copias de seguridad.
Paso 2: Seleccionar las carpetas y archivos que desea restaurar. Esto podría ser todos o sólo archivos especificados.

Paso 2: Seleccionar la ubicación en la que desea restaurar. De forma predeterminada, se selecciona la ubicación original. Hacer clic en Finalizar para iniciar la recuperación.

5. Troubleshooting

Troubleshooting en copias de seguridad y recuperación.

Frecuencia:	Cuando se requiera.
Propósito:	Reúna toda la información que pueda ayudarle a resolver el problema que está experimentando.
Procedimiento:	Determinar la causa raíz posible de un problema se hace mucho más simple cuando hay suficiente información disponible y por lo tanto la resolución sería mucho más rápida en la mayoría de las situaciones. En algunos casos, el problema puede quedar inmediatamente claro después de comunicarse con el usuario. Los problemas conocidos, como Unable to connect to server, debido a problemas de conectividad pueden ser resueltos por el Administrador. Los errores nuevos o inesperados deben escalarse al soporte de Cibecs junto con la siguiente información: • Proporcione una visión general del escenario. Los usuarios pueden a menudo destacar un área que vale la pena investigar como la causa posible. • Proporcione la información de su estación de trabajo:

	O Sistema operativo: Service packs, Platform 32 / 64bit. O Información del sistema de archivos NTFS o FAT32. • Díganos qué aplicación predeterminada de correo electrónico está utilizando, como Outlook, Thunderbird, etc. • Adjuntar la aplicación de Windows y los registros de sucesos del sistema. • Adjunte las capturas de pantalla que pueda tener con respecto al error recibido. • Adjunte los archivos de registro del agente de usuario. • Adjunte los archivos de registro del servidor de Cibecs.

5.1 Códigos de error de despliegue

Pasos para la solución de problemas de implementación que debe seguir siempre:

Hacer clic al nombre de host de la estación de trabajo para asegurarse de que está activo en la red.

- Si la máquina no está disponible en la red utilizando el nombre de host, intente hacer clic a la dirección IP.

- Si no puede hacer clic a la estación de trabajo mediante cualquiera de los métodos, visite la estación de trabajo y asegúrese de que está conectada a la red.

- Desactivar el firewall si está en un estado habilitado.

- Habilitar la detección de red y compartir archivos e impresoras en la configuración de red.

Acceda a la estación de trabajo a través de la red mediante Admin$share

Escriba el siguiente dominio en la barra de direcciones del explorador de Windows: ***\\workstationhostname\admin$***

Una vez que se puede conectar correctamente al recurso compartido de Admin $, puede continuar con la tabla de solución de problemas de código de salida siguiente.

Código de Salida	Descripción	Troubleshooting
n/a	No se detectó ningún equipo	Si espera que las máquinas estén en las IP estipuladas, compruebe los firewalls del punto final y la configuración de descubrimiento de red.
2	Paquete de agentes de Aranda no encontrado	Si está utilizando un recurso compartido UNC, asegúrese de que el paquete de agente se encuentra en la ubicación compartida.
6	No se puede instalar el agente en el equipo cliente	Credenciales incorrectas ingresadas en la tarea de despliegue, asegúrese de que las credenciales tengan suficientes privilegios y que las haya ingresado correctamente.
		Asegúrese de que los puertos 135 y 445 están abiertos y disponibles en el equipo cliente, ya que estos puertos son necesarios para el acceso de PsExec.
		Si está utilizando un recurso compartido UNC, asegúrese de que el paquete de agente se encuentra en el recurso compartido.

		Esto puede ocurrir en situaciones en las que un equipo del cliente tiene dos direcciones IP y la instalación se está intentando en ambas direcciones. Esto puede resultar en la implementación en una de las direcciones IP que falla con código de error 6.
801	Se ha producido un problema al descargar el paquete del agente.	Error en la verificación de la firma Md5 para el paquete descargado. Permita que la tarea de implementación realice otra ejecución. Si el problema persiste, cancele y cree una nueva tarea de implementación para los equipos cliente con error.
1326	Las credenciales de inicio de sesión proporcionadas eran incorrectas. Asegúrese de haber introducido credenciales válidas para la tarea de implementación	Compruebe las credenciales configuradas al crear la tarea de implementación.
1618	Ya se está realizando otra instalación en el equipo cliente	Permitir que la tarea de implementación realice otra ejecución para el equipo del cliente. Si el problema persiste, confirme si se está implementando otro software en el equipo cliente y si es necesario reinícielo.
		Esto puede ocurrir en situaciones en las que un equipo cliente tiene dos direcciones IP y la instalación se está intentando en ambas direcciones IP. Esto puede resultar en la falla de una de las instalaciones, ya que no puede continuar debido a la instalación que ya se está realizando.
1619	No se puede acceder al recurso compartido de UNC	Se han introducido credenciales incorrectas en la tarea de implementación; asegúrese de que

		introduce las credenciales con los privilegios suficientes para acceder al recurso compartido UNC y que los ha introducido correctamente.
1620	El recurso compartido UNC no está disponible	Asegúrese que el recursos compartido UNC está en línea y es accesible.
2250	No se puede conectar al equipo cliente	Las máquinas con Windows 7/8 que tienen sus firewalls deshabilitados requieren que el servidor funcione como un administrador de dominio.
		La conexión del servidor puede estar inactiva. Si la implementación falla en todos los puntos finales, compruebe la tarjeta de interfaz de red en el servidor.
		Si el despliegue falla en algunos puntos finales, compruebe las tarjetas de interfaz de red de los puntos finales, así como si el recurso Admin $ está habilitado. Asegúrese de que el descubrimiento de red y el uso compartido de archivos e impresoras estén habilitados.
-1	Error inesperado durante la implementación. La tarea de despliegue puede haber sido cancelada por el administrador.	Contacte al equipo de soporte de Aranda.
-559038737	Error inesperado	Contacte al equipo de soporte de Aranda.