Manual Tareas Administrativas Active Directory – Intune

Contenido

[Unidades Organizativas 1](#_Toc129255749)

[Sincronización de objetos 2](#_Toc129255750)

[Proceso para crear un usuario 3](#_Toc129255751)

[Sincronizar el dominio 7](#_Toc129255752)

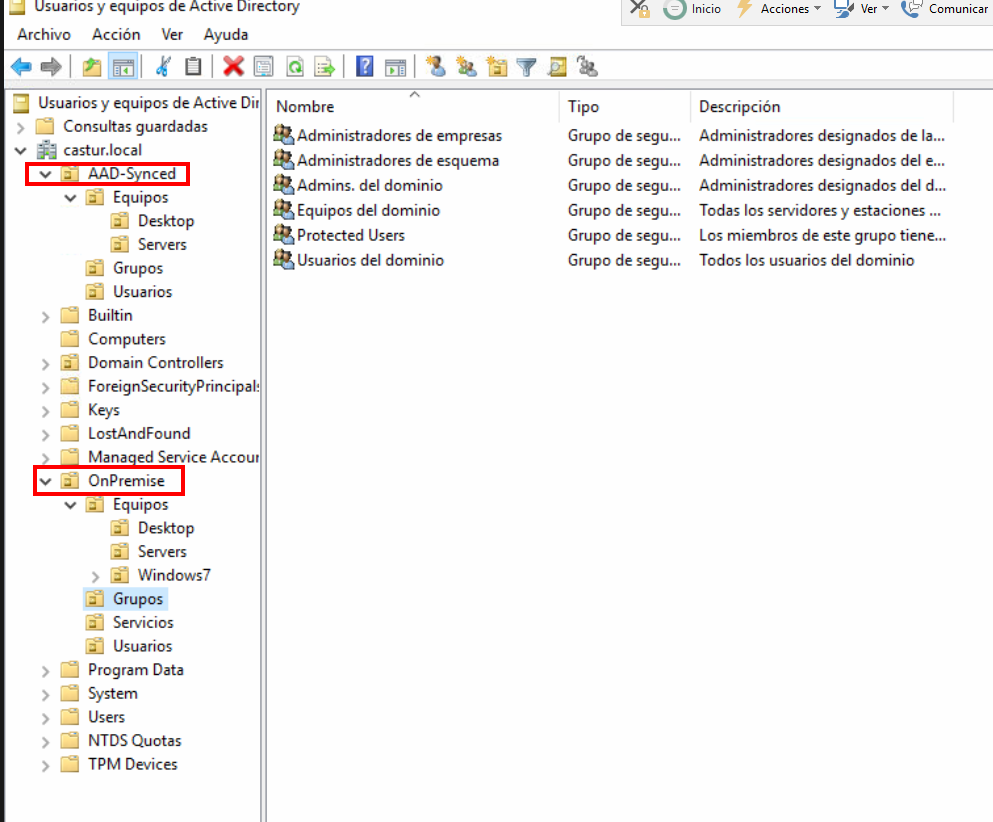
[Consola de AzureAD e Intune 8](#_Toc129255753)

[Establecer un dispositivo como de propiedad de la organización y establecer el usuario primario. 9](#_Toc129255754)

[Asignacion de licencias 11](#_Toc129255755)

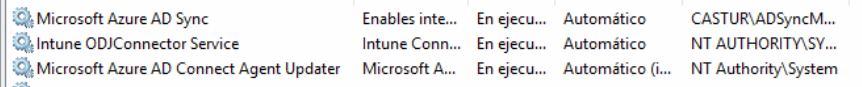
# Unidades Organizativas

En el Active Directory local organizamos los objetos (usuarios, computadoras, grupos) por unidades organizativas para poder aplicar política y configuraciones. En el primer nivel usamos dos UO principales para asegurarnos de separar los objetos que queremos sincronizar con el Azure AD en cloud de los que no. Esto es importante porque no queremos que los administradores locales y grupos privilegiados se sincronicen a la nube.



# Sincronización de objetos

Hay tres servicios que se encarga de hacer la sincronización de objetos y monitorizar que ambos dominios estén funcionando como se espera:

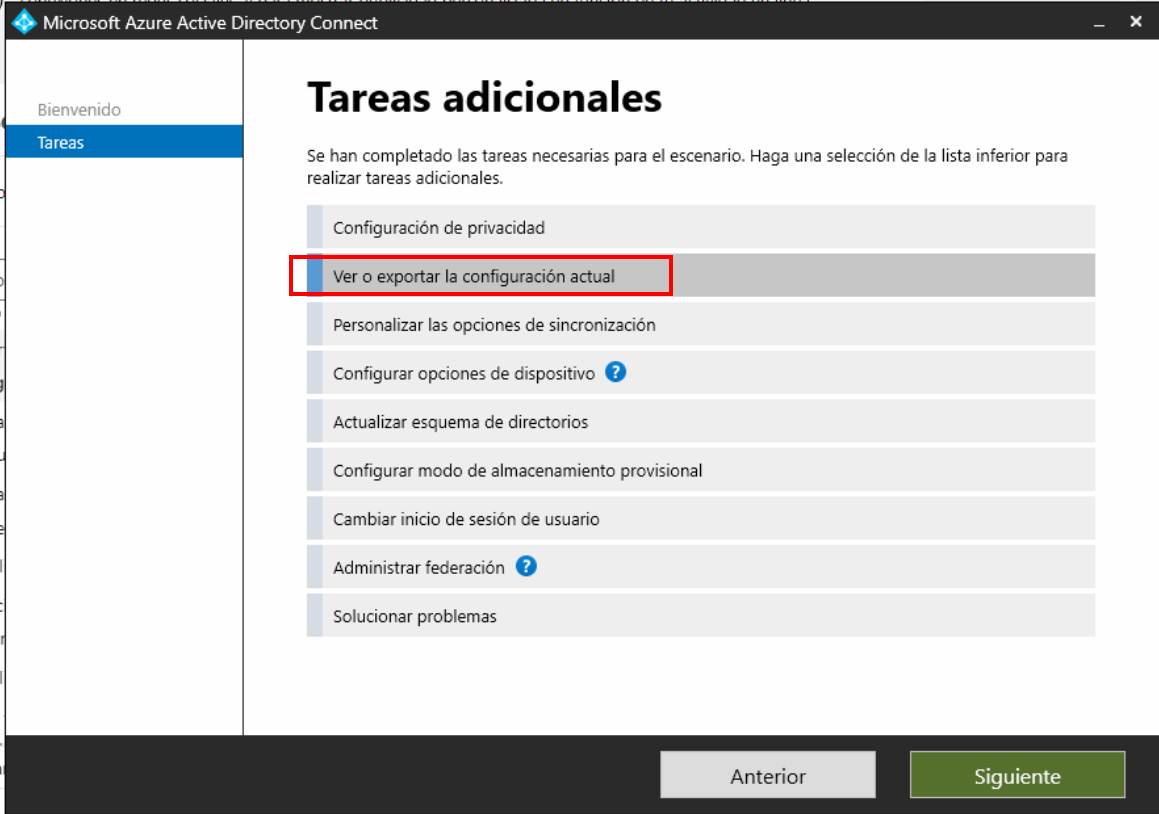


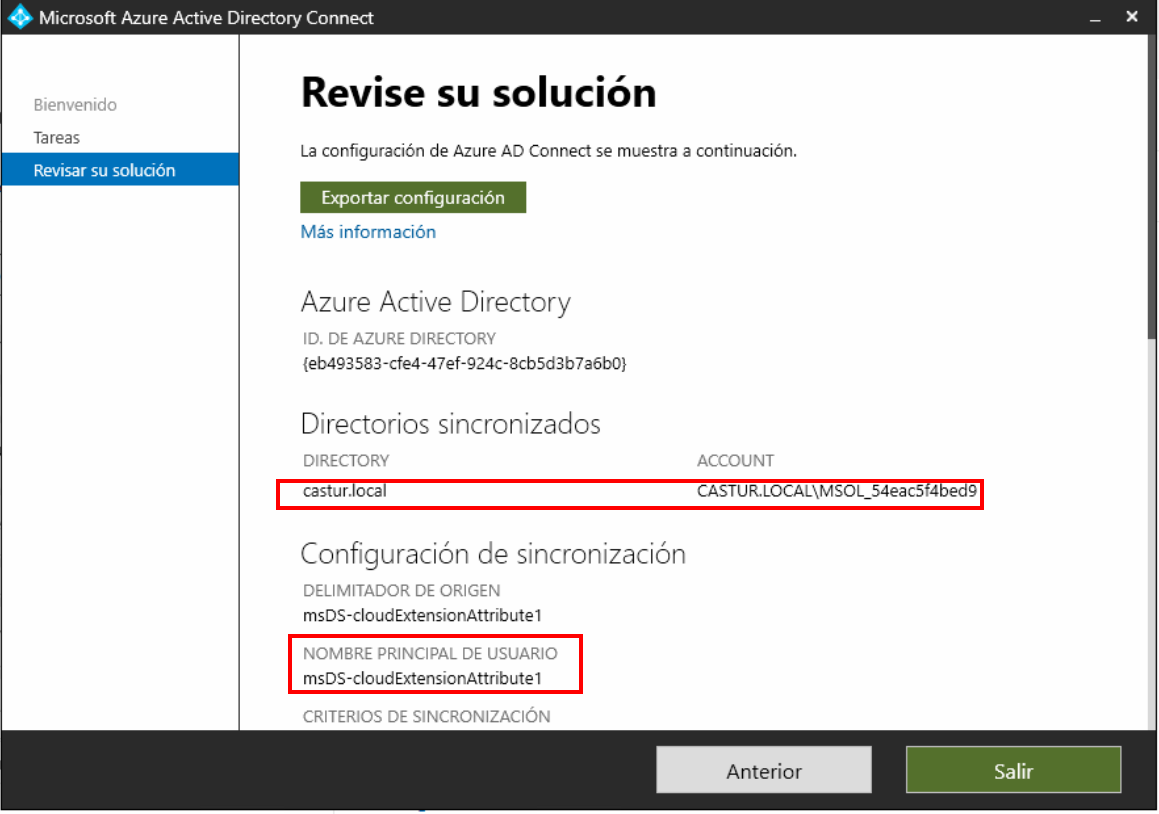
Intune OJD Connector y Azure AD Connect Agent no tienen más mantenimiento que asegurarse que estén levantados.

El Azure AD Connect es el que se encarga de filtrar y sincronizar objetos.



Es importante revisar que el servicio se levanta tras los reinicios del servidor porque a veces no termina de levantar solo.



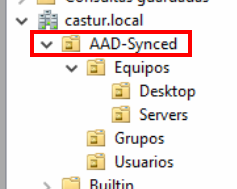


En la configuración personalizada para Campoastur tenemos una cuenta local MSOL\_54eac5f4bed9 que ejecuta el servicio y hemos puesto como propiedad local para sincronizar con Azure AD a la propiedad ms-DS-cloudExtensionAttribute1.

Lo hemos elegido porque:

* El dominio de correo campoastur.es no está administrado por nosotros
* El ms-DS-cloudExtensionAttribute1 una propiedad que no se usa de forma local
* El atributo userPrincipalName referencia al dominio local castur.local que queremos que siga siendo usable para logarse porque hay usuarios que no se van a sincronizar

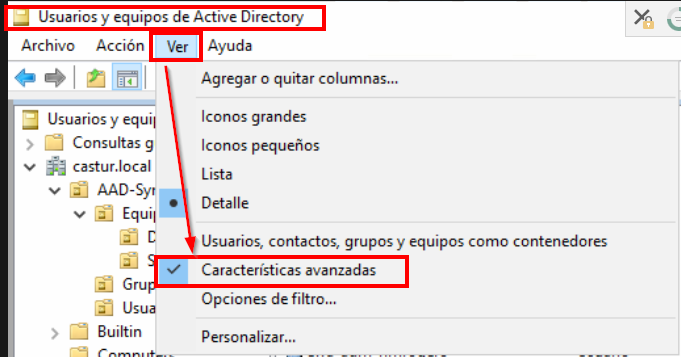
Aunque no se ve en la exportación de la configuración la sincronización esta filtrada y solo se sincronizan objetos que estén contenidos en la OU=AAD-Synced



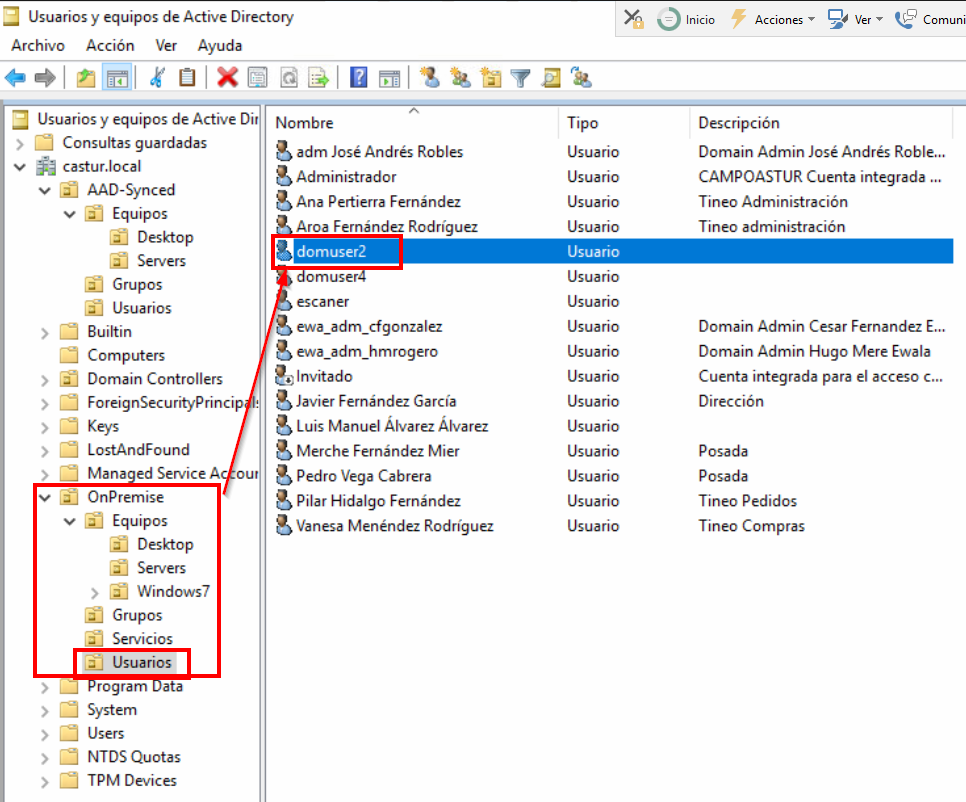
# Proceso para crear un usuario

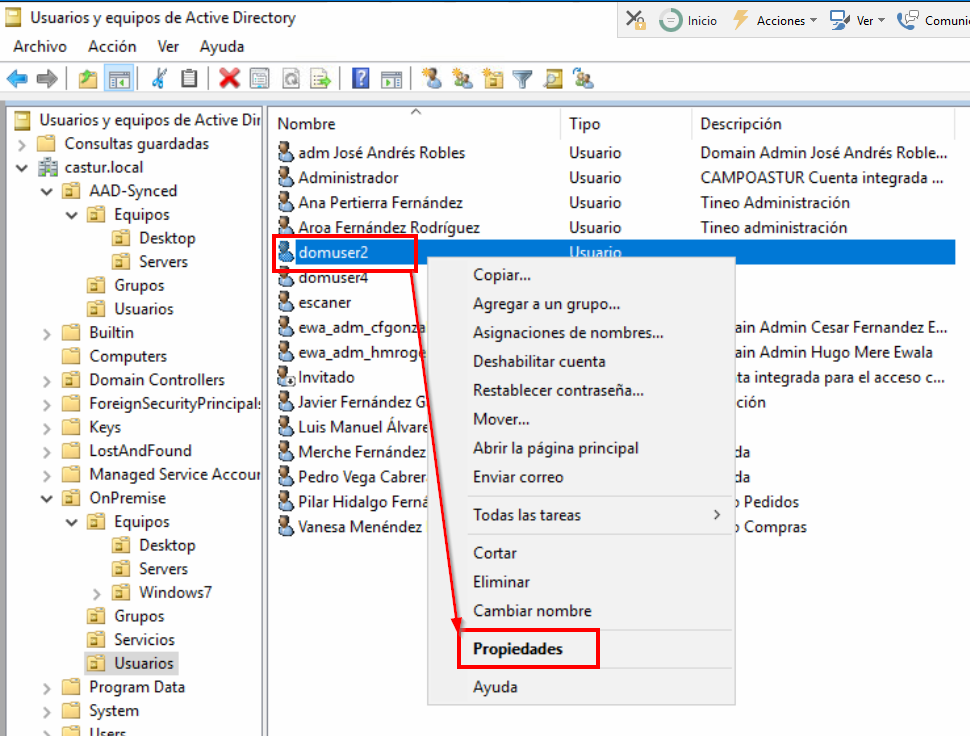
Comenzamos por crear un usuario del dominio tal como lo habíamos hecho hasta ahora y a continuación le añadimos el nombre de usuario con el dominio cloud en el parámetro ms-DS-cloudExtensionAttribute1

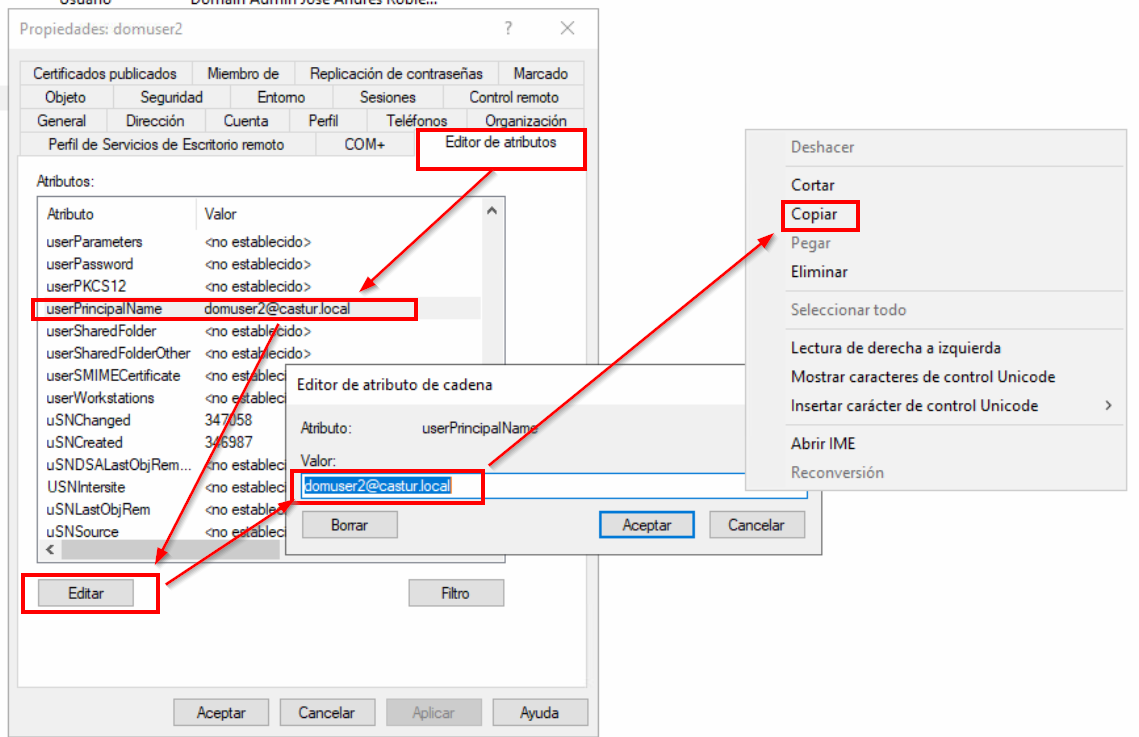
Nota: para poder ver el editor de atributos debemos tener activada la vista de “Características Avanzadas”

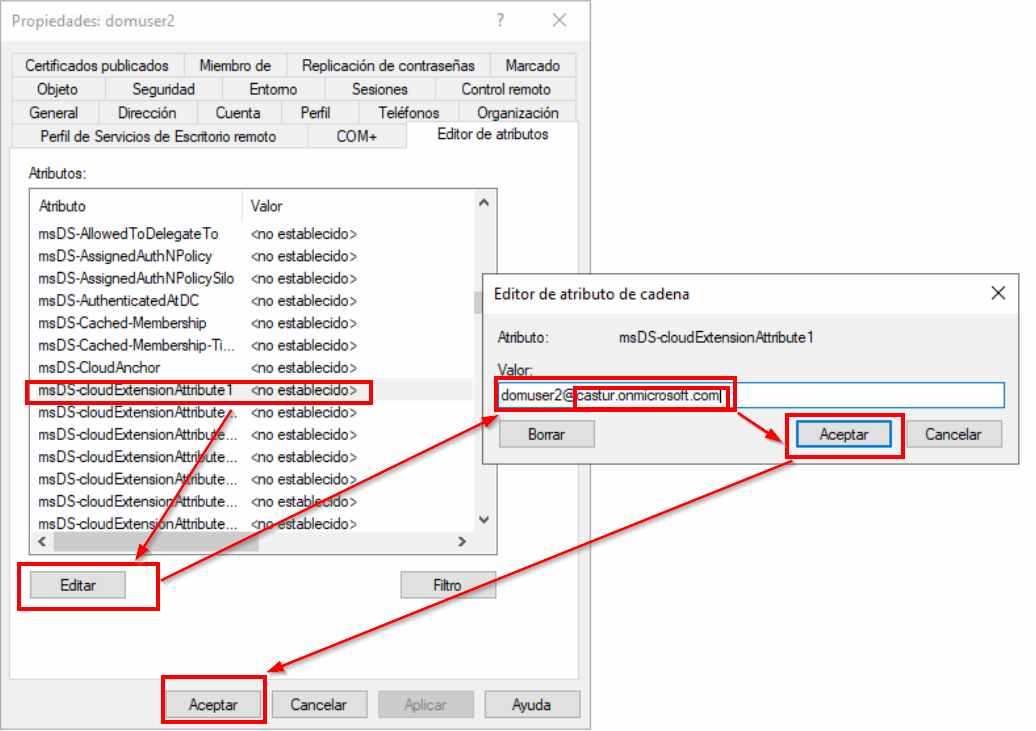


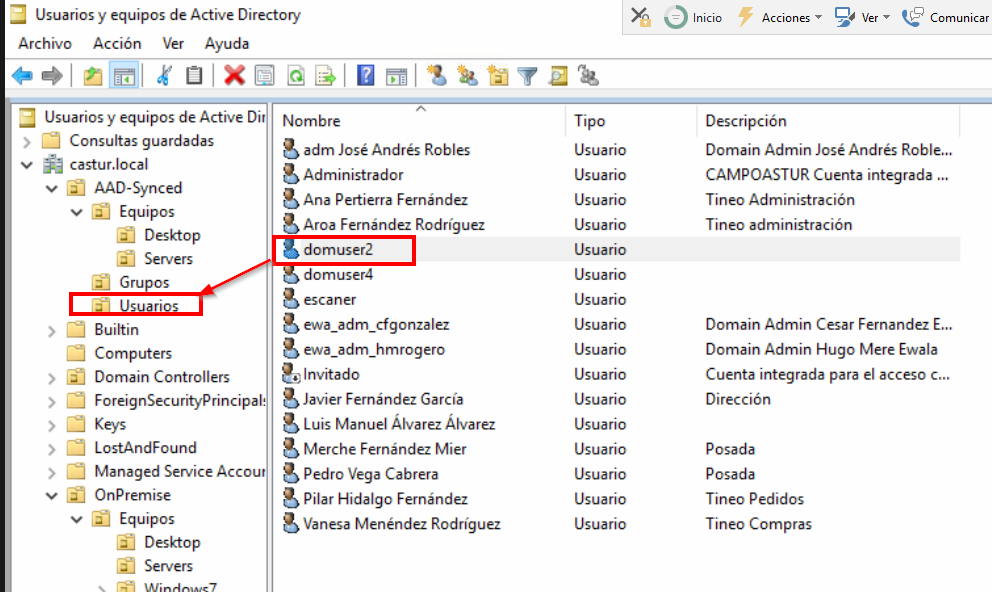
Partimos del usuario ya creado “domuser2” que está en la estructura de OU de OnPremise



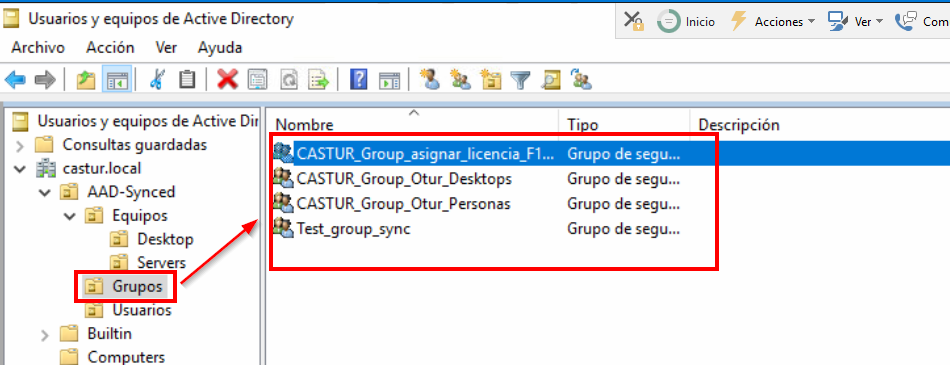


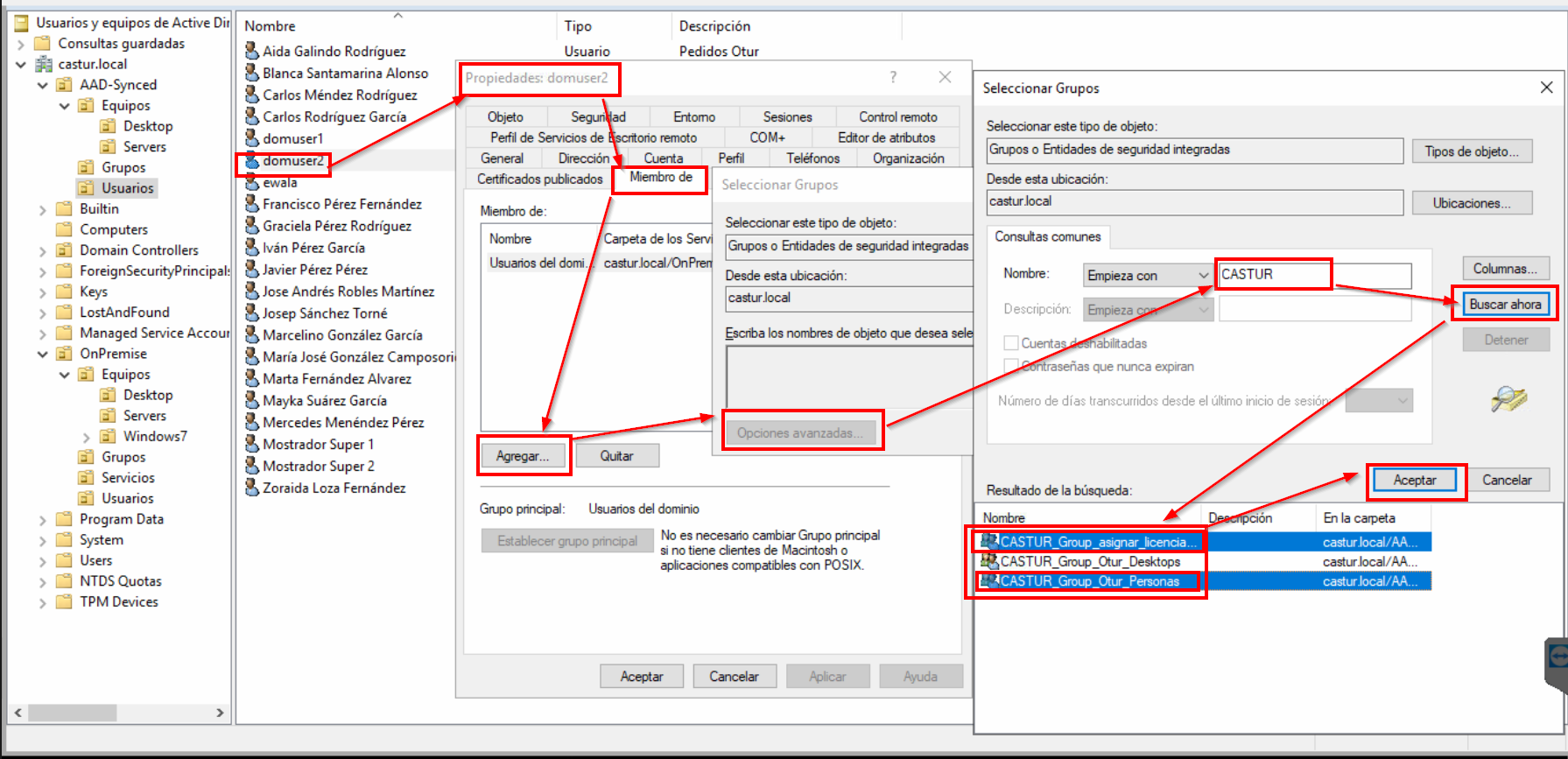
En el editor de atributos copiamos el valor de usePrincipalName 

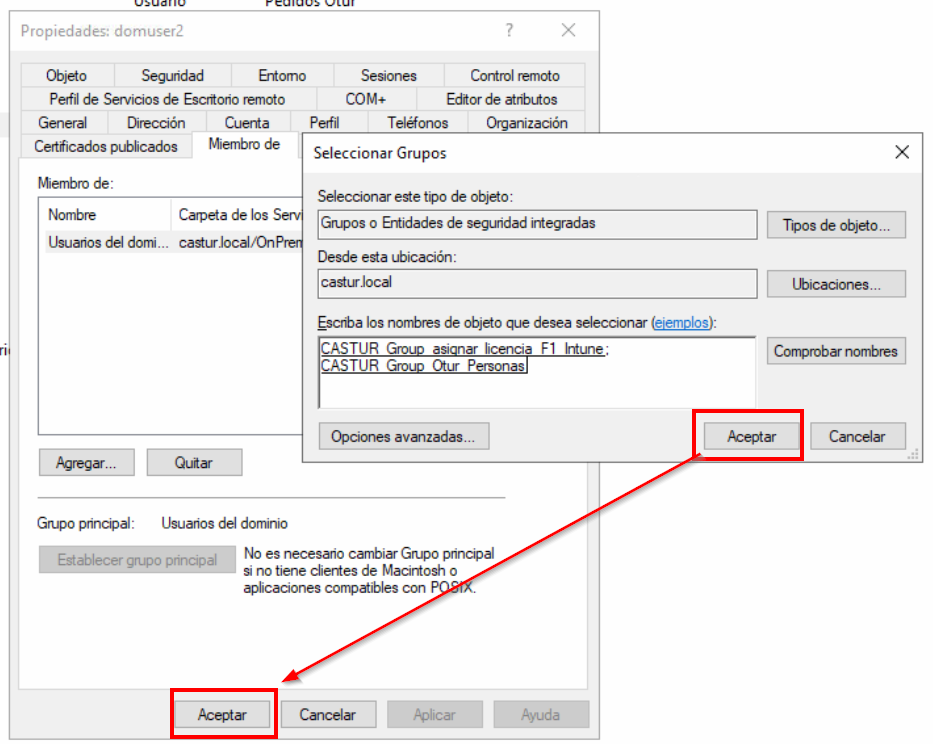
Vamos a la propiedad ms-DS-cloudExtensionAttribute1, pegamos el valor copiado y cambiamos el dominio por el dominio cloud de campoastur @castur.onmicrosoft.com

A continuación arrastramos el usuario a la OU=Usuarios,OU=AAD-Synced

Por último, nos queda introducir al usuario en los grupos correspondientes. De momento tenemos grupos para organizar a los usuarios y equipos por su asignación a una sede y tenemos un grupo para asignar licencias de Intune de forma dinámica

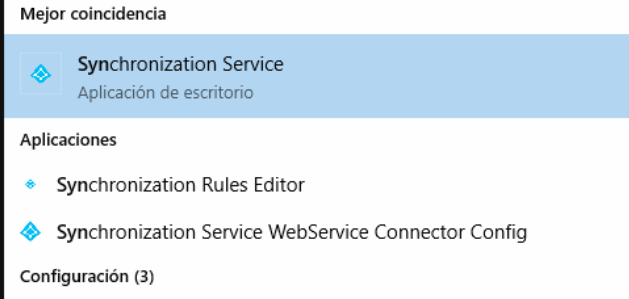


Asignemos el usuario a los grupos de personas de Otur y al grupo de personas con licencia F1 para Intune. 

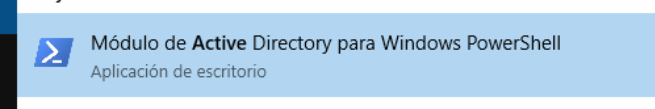


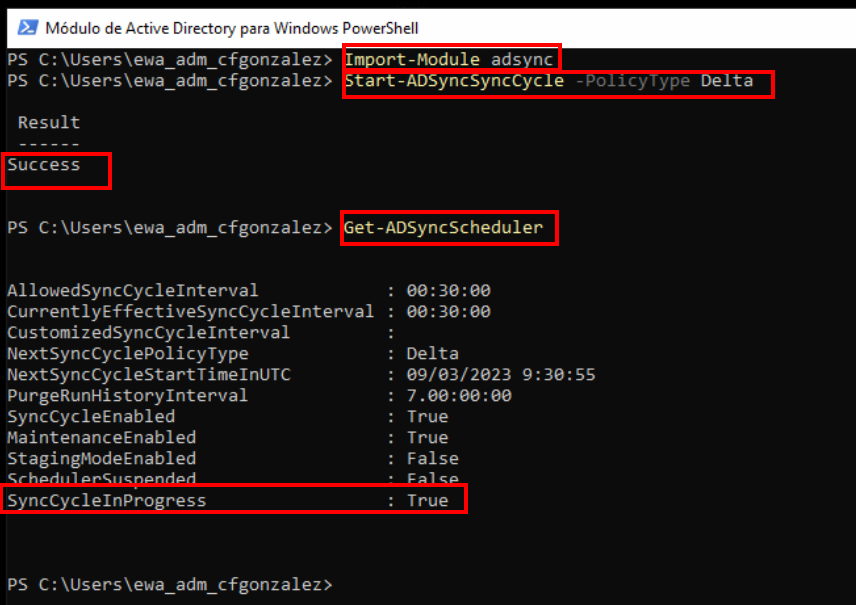
# Sincronizar el dominio

El proceso de sincronización ocurre automáticamente cada media hora, pero en ocasiones necesitamos forzarla inmediatamente. Esto se puede hacer de forma gráfica con la herramienta Synchronization Service



Pero tiene demasiadas opciones y es fácil equivocarse, por lo tanto es más cómodo usar la línea de comandos con tres simples comandos:





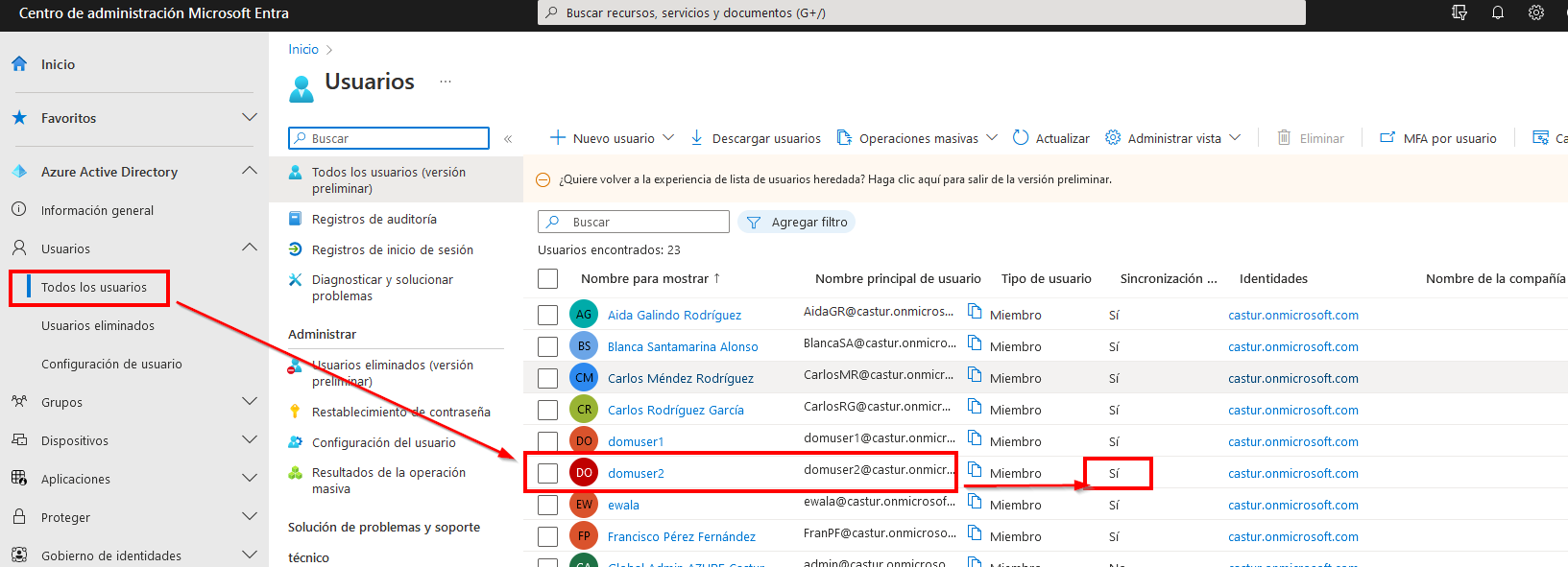
**Import-Module adsync**

**Start-ADSyncSyncCycle -PolicyType Delta**

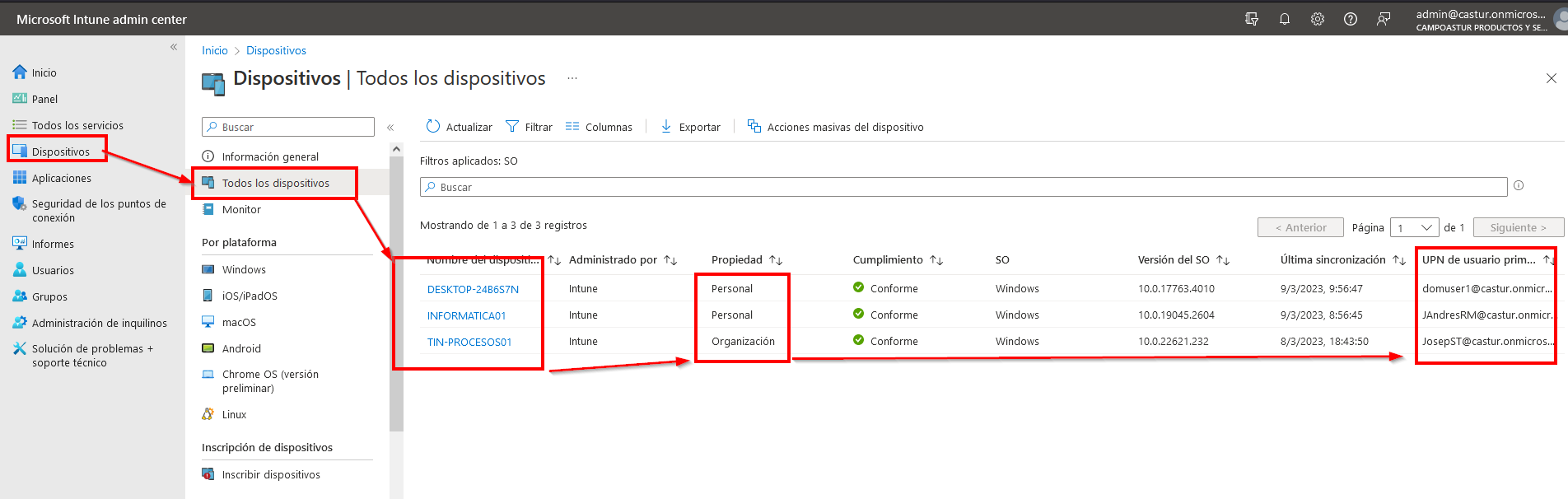
**Get-ADSyncScheduler**

# Consola de AzureAD e Intune

En la consola de Active Directory (<https://entra.microsoft.com/>) y en la de Intune (<https://endpoint.microsoft.com>) podemos ver que el usuario se ha sincronizado



En la consola de intune también se pueden ver los dispositivos administrados

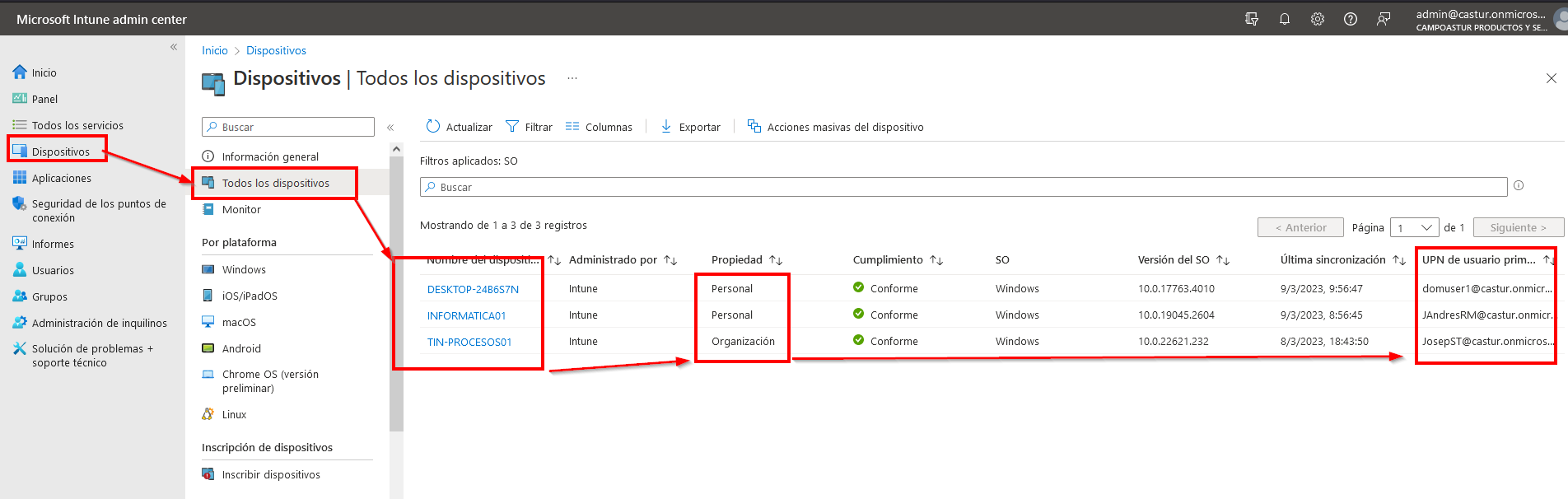


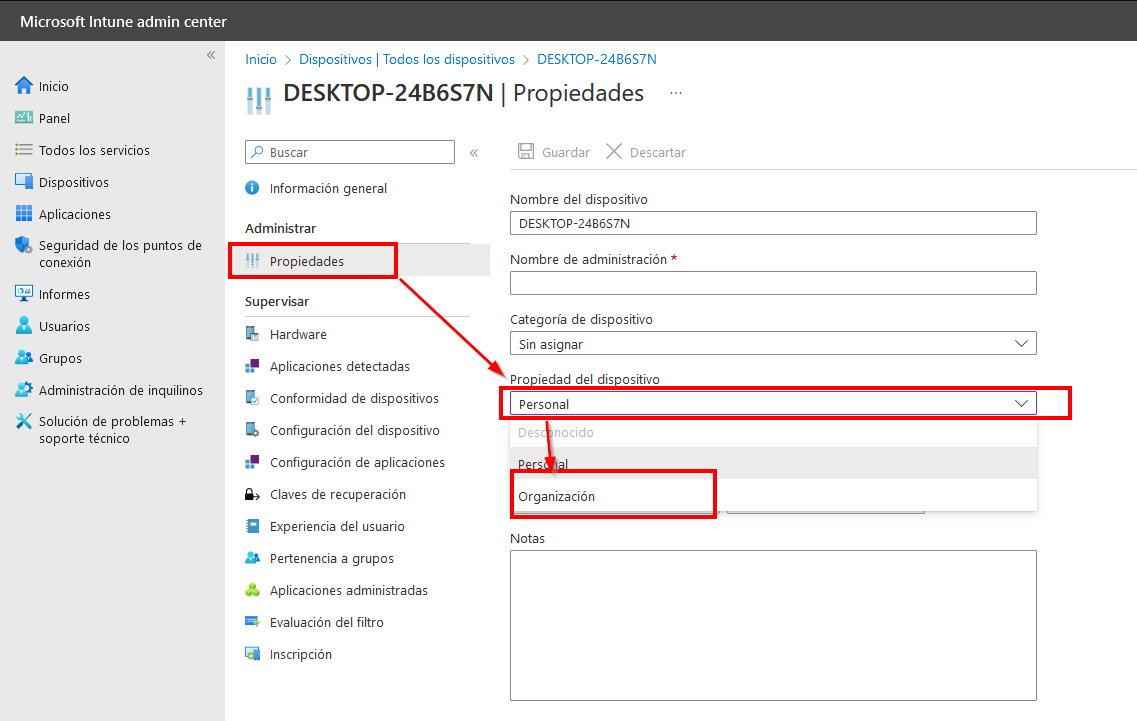
Por cada dispositivo podemos ver quien es el usuario primario, la versión del sistema y si la propiedad del dispositivo es personal o corporativa.

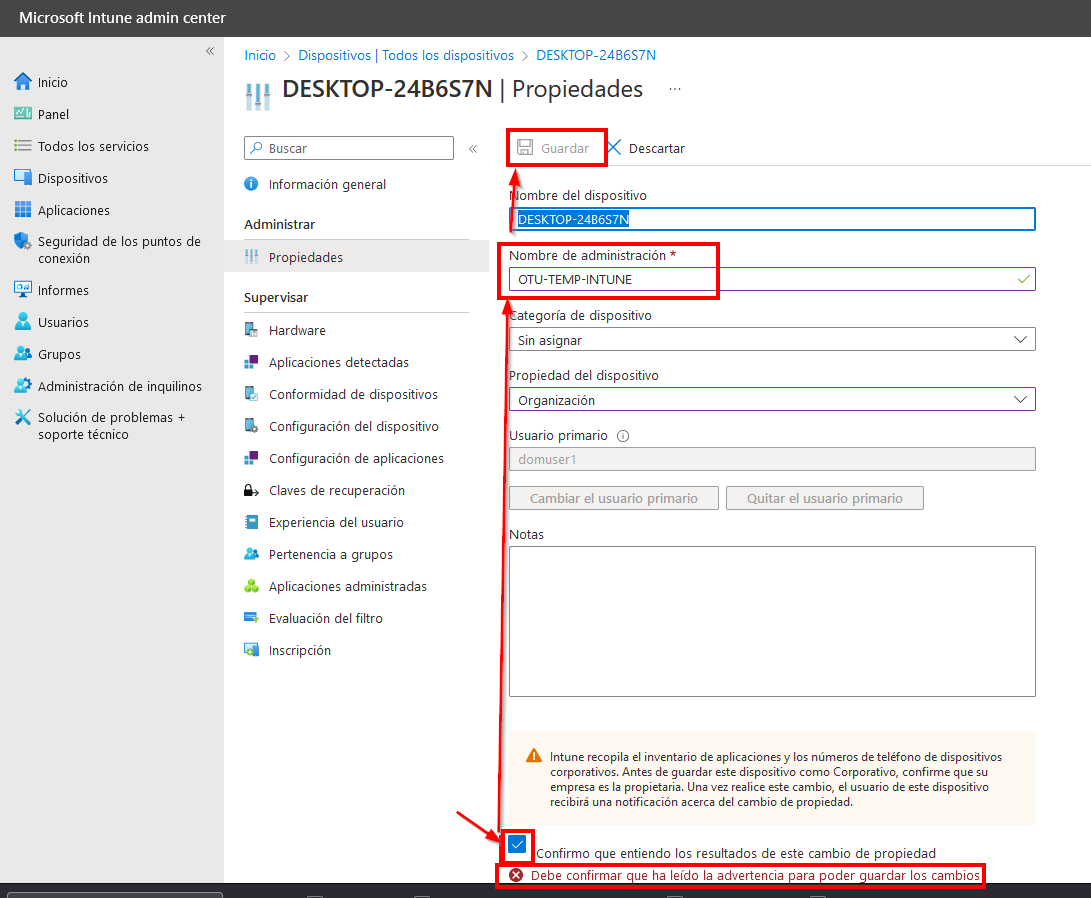
Cuando el dispositivo se fija como personal las acciones y supervisión que tiene Intune sobre el dispositivo son más limitadas puesto que se supone que el usuario puede usar el dispositivo para uso personal. En cambio, cuando el dispositivo se fija como corporativo el control y acceso son absolutos.

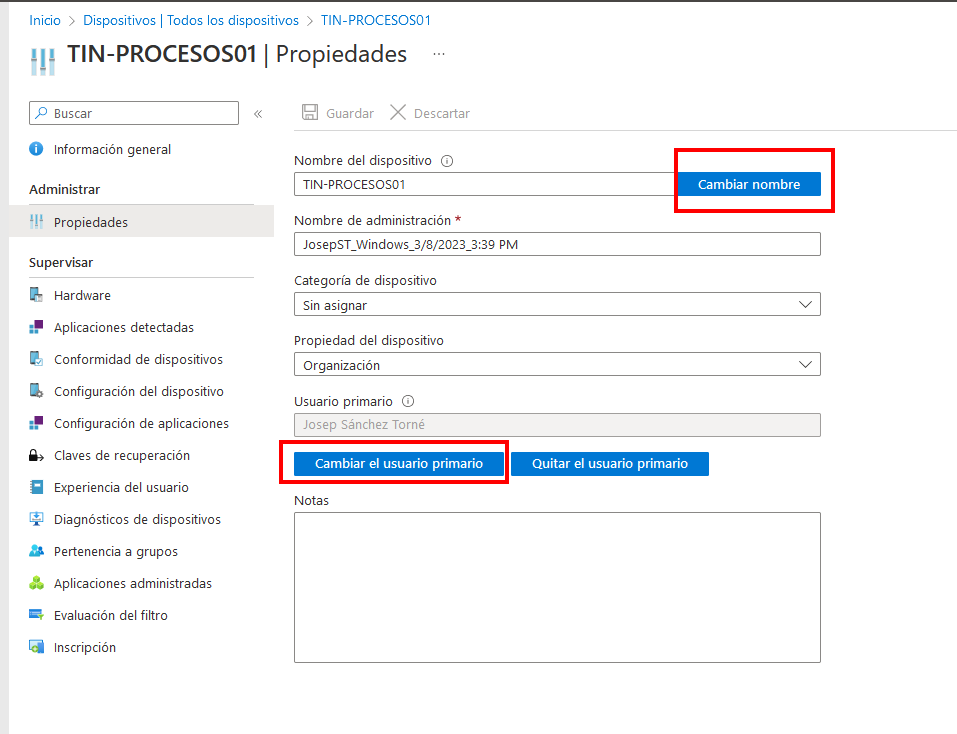
# Establecer un dispositivo como de propiedad de la organización y establecer el usuario primario.

Vamos a usar un equipo de pruebas para mostrar el proceso







Como siempre en intune el proceso de aplicar este cambio a la maquina puede llevar un tiempo que depende la sincronización y de que la maquina este activa. Una vez que la maquina se califica como corporativa se puede hacer otras acciones como inspeccionar sus aplicaciones, cambiar el nombre de la máquina o cambiar el usuario primario. Ej: 

# Asignacion de licencias

Las licencias se pueden asignar de forma manual, pero como hemos creado un grupo para esta tarea vamos a mostrar como se configura la asignación de licencias en el Azure AD:

