

Laboratorio – 3: Inscribir dispositivos en el servicio de EMS.

Objetivo: Cómo podemos enrolar dispositivos en EMS, distintas opciones de inscripción y como realizarlas.

Microsoft EMS nos permite enrolar dispositivos móviles y PCs/portátiles (Windows 10) tanto personales (BOYD) como corporativos (propiedad de la empresa, no del usuario) **manteniendo protegidos los datos empresariales**. La inscripción de un dispositivo es la primera experiencia que muchos usuarios finales tendrán al acceder a los recursos corporativos. En este laboratorio, utilizaremos **Microsoft Store** para la instalación del **App en Company Portal** (*Portal de empresa*) para poder **inscribir el dispositivo en Microsoft EMS (Intune)**.

Prerrequisitos: Tener una tenant de EMS Enterprise Mobility + Security E5 propia o trial.

Enlace paso a paso de Microsoft: <https://docs.microsoft.com/es-es/intune-user-help/enroll-windows-10-device>

Pasos a realizar:

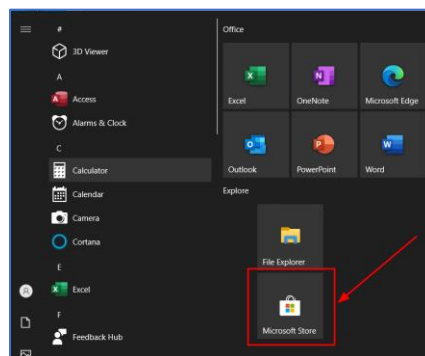
1. Desde el propio **dispositivo** (Windows, Android o iOS) procederemos a descargarnos desde la aplicación de **Microsoft Store**, el App llamada "**Portal de Empresa**". **!!! RECOMENDADO !!!**, realizar esta descarga e instalación de la misma con un usuario administrador local de la máquina en cuestión, sí no, no podremos enrolar el equipo en nuestro servicio de EMS.

El **Portal de Empresa** es una App, publicada en **Microsoft Store**, que nos permite, como **empleado de nuestra empresa**, **acceder de forma segura a los recursos** que nos proporcionan los **servicios Cloud de Microsoft** (*Office, Email y OneDrive, Azure, Dynamics 365, SSO, etc*).

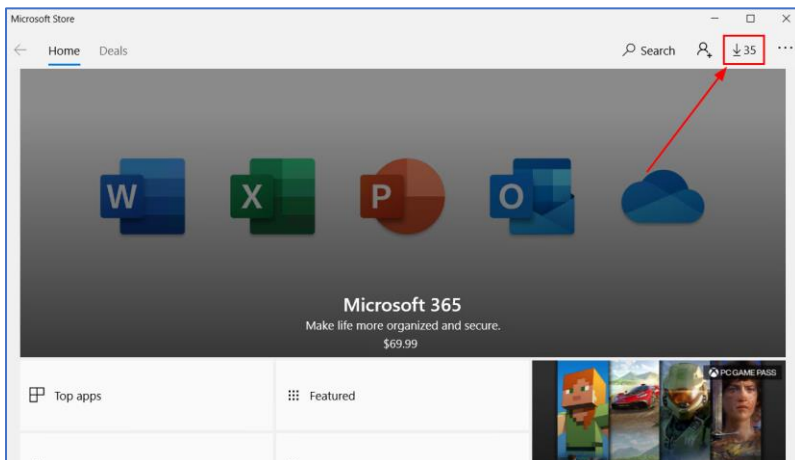
Antes de poder usar esta App, nos debemos de asegurar que tenemos la licencia de Microsoft EMS adquirida o usar un trial de este servicio y que la tenemos asignada a las cuentas de los usuarios que van a inscribir sus equipos a la tenant de la empresa.

El "**Portal de Empresa**" lo debemos **instalar** (con un usuario administrador local de la máquina o usuario de dispositivo móvil/tableta) en **cada equipo** desde **Microsoft Store**

2. Para instalar la App "**Portal de Empresa**", desde el PC/portátil del usuario con **Windows 10**, abrimos **Microsoft Store**, desde su icono en la **barra de Windows** o **buscándola en nuestro menú Inicio** (de Windows).

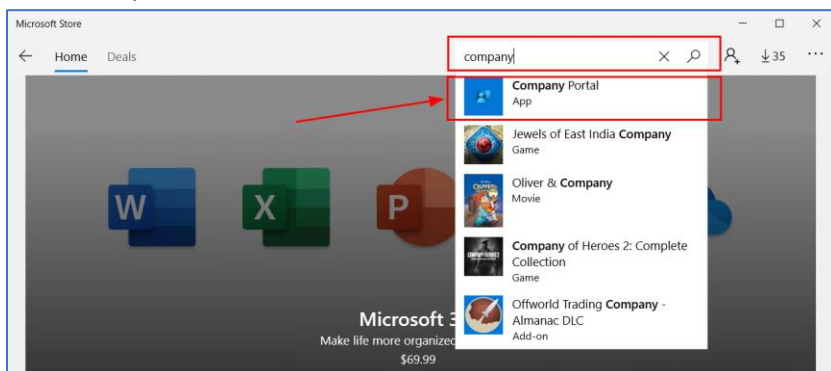


- Es recomendable **actualizar** las **Apps por defecto en Windows 10** que nos implementa **Microsoft Store**, Para ello **clic** en el icono superior derecho que es una **flecha para abajo con un nº al lado**.

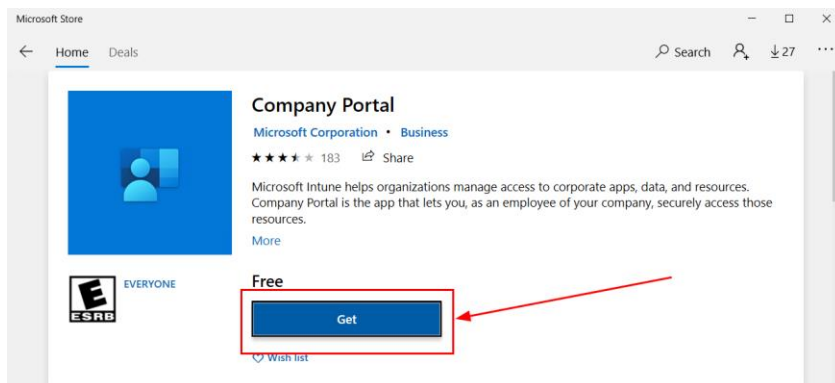


Esperar hasta que terminen todas las actualizaciones de las Apps.

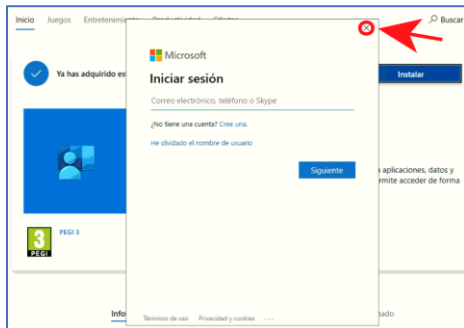
- En la ventana de **Microsoft Store** en el cuadro de búsqueda (*la lupa*) escribimos **Portal de Empresa**. Y hacemos **clic** en su **icono** para **mostrarla**:



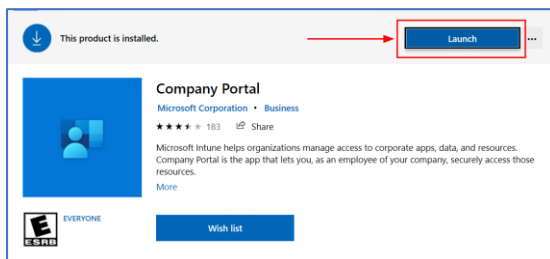
- Clic** en el **Instalar** para **implementarla** en nuestro Windows 10 (si no aparece el botón instalar utilizamos el botón Get):



6. iii **IMPORTANTE !!!**. Nos **pedirá un usuario** (un cuenta de una usuario personal, de Outlook.com, p.e, con el que podremos sincronizar nuestras Apps entre todos los dispositivos Microsoft que tengamos entre otras cosas) para **continuar con la instalación**, **NO PONER NINGUNA CUENTA PERSONAL**, este dispositivo es de empresa. Para **seguir con la instalación**, clic en la "x" tal y como se muestra en el pantallazo.



7. La instalación finalizará y podremos ejecutarla en el botón **Iniciar**:

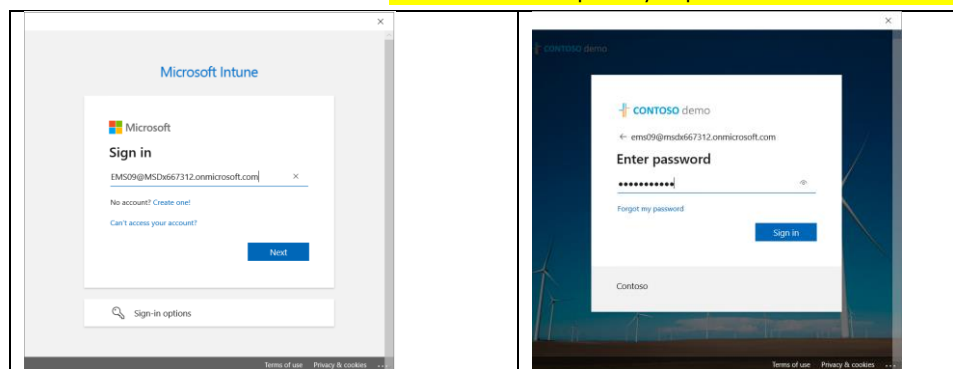


8. Nos aparecerá la ventana del **Portal de Empresa** y nos pedirá que nos **logueemos al servicio** con el usuario de **Azure Active Directory (Office 365/EMS)** que nos haya facilitado. **Cualquier usuario** al que le hayamos dado **privilegios para realizar el enroll** en nuestro Azure Active Directory, **podrá realizar este paso**.

Nosotros por motivos de simplicidad, usaremos:

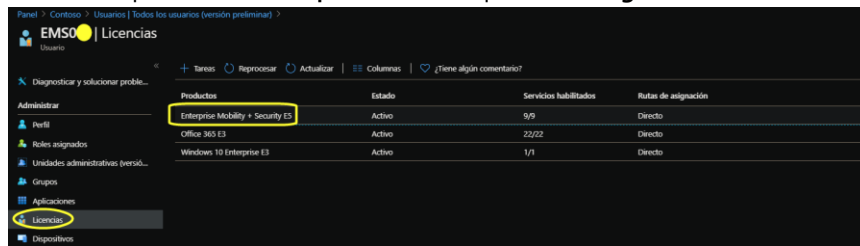
Usuario: EMSox@m365*****.onmicrosoft.com (la "x" es el usuario que os hemos dado al comienzo del curso).

Contraseña: HolaMundo01 (o la contraseña que hayas puesto cuando el sistema te obligó a cambiarla)



a. **Cuestiones a tener en cuenta.**

- i. **Tenemos** que ser un **administrador local de la máquina** para poder hacerlo. A este admin local, una vez enrolado el dispositivo se le revocarán los permisos de administrador local sobre la máquina por defecto.
- ii. Para **poder instalar cualquier software una vez terminemos en enroll del equipo como Organización**, nos pedirá un **usuario administrador de EMS para poder instalar** (sí así lo definimos en nuestra directiva). Similar a la unión a un dominio de Windows Server Active Directory a través de la característica “miembro de...” desde las propiedades de “MI PC”.
- iii. El **usuario que enrole el dispositivo** tiene que **tener asignada una licencia de EMS** dentro de la tenant.



Panel > Contoso > Usuarios > Todos los usuarios (versión preliminar) >

EMSO | **Licencias**

Usuario

+ Tareas | Reprocesar | Actualizar | 11 Columnas | ¿Tiene algún comentario?

Diagnosticar y solucionar proble...

Productos	Estado	Servicios habilitados	Rutas de asignación
Enterprise Mobility + Security E3	Activo	9/9	Directo
Office 365 E3	Activo	22/22	Directo
Windows 10 Enterprise E3	Activo	1/1	Directo

Administrador

Perfil

Roles asignados

Unidades administrativas (perso...

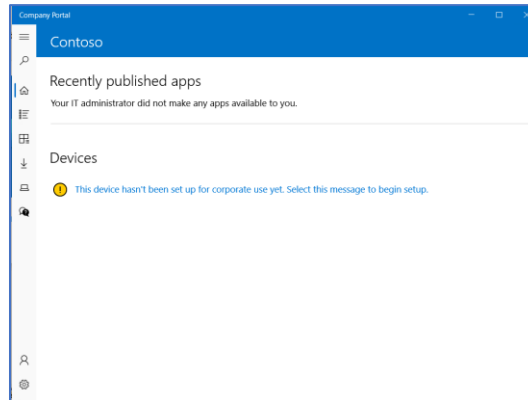
Grupos

Aplicaciones

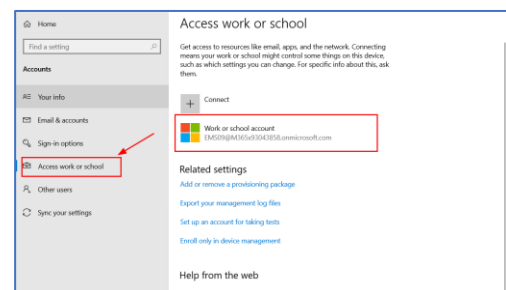
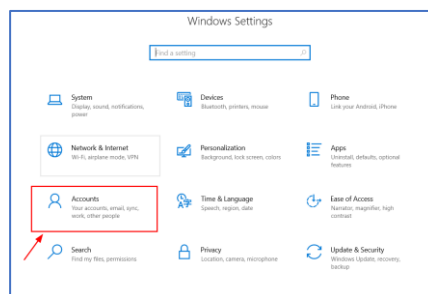
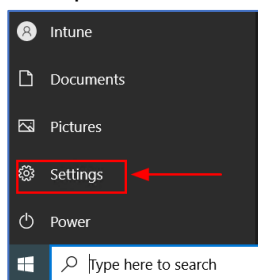
Licencias

Disponibles

9. Nos aparecerá varias ventanas informativas que tendremos que aceptar, **Clic en el botón Listo:**
10. **Realizaremos un primer login** contra el servicio de **Microsoft EMS** vía este **App** y se aplicarán las **Directivas corporativas** que el **administrador** de EMS nos haya asignado e **información relacionada de la empresa** (*Apps que el administrador publica y nos permite descargarlos*). **Aparecerá una ventana informativa** de que todo se ha establecido **satisfactoriamente** :



11. Con lo que acabamos de hacer, tenemos el **dispositivo definido** con **Personal** dentro de **EMS**. **NO** como **Corporativo**. Podemos **verificarlo** yendo al **menú Inicio** de Windows > **Configuración** > **Cuentas** > **Obtener acceso a trabajo y escuela**. Nos aparecerá la cuenta empresarial con la que hemos enroldado el dispositivo en EMS.



12. Ya tenemos **nuestra máquina enroldada como dispositivo personal** en el servicio, no tendremos disponibles la mayoría de las opciones de administración, ya que ahora mismo, **este equipo es propiedad personal del usuario NO de la empresa**

Lab – 6.2: Inscribir dispositivos en el servicio de Microsoft Intune como Organización.

Objetivo: Enrolar dispositivos en EMS, inscribiéndolos como Organización (*PROPIEDAD DE LA EMPRESA*).

Prerequisitos: Tener una tenant de EMS Enterprise Mobility + Security E5 propia o trial.

Enlace paso a paso de Microsoft: <https://docs.microsoft.com/es-es/intune-user-help/enroll-windows-10-device>

Pasos a realizar:

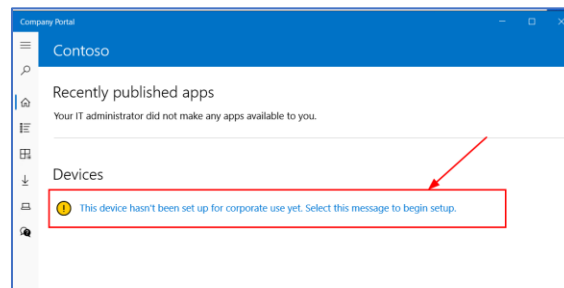
1. Segundo paso: Inscribir el equipo/dispositivo como Organización.

Para terminar la inscripción del dispositivo para este usuario ¡¡¡ **ALTAMENTE RECOMENDABLE** !!!.

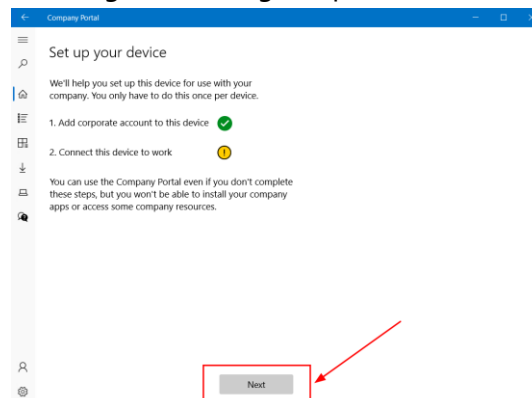
Realizar la inscripción **como dispositivo Organización** de este Windows 10.

El usuario que realice esta inscripción tiene que ser **administrador local** del dispositivo. Se le revocarán los personales de administrador local de la máquina, por defecto, una vez terminado este paso, ya que el dispositivo está enrrolado en el dominio de la tenant de Azure Active Directory de nuestra empresa.

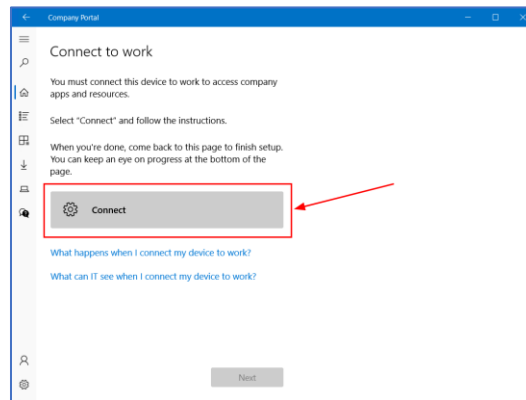
Para ello, volvemos a la **pantalla principal** de la App: **Portal de Empresa**. Clic en el **enlace de inscripción del dispositivo como Organización**.



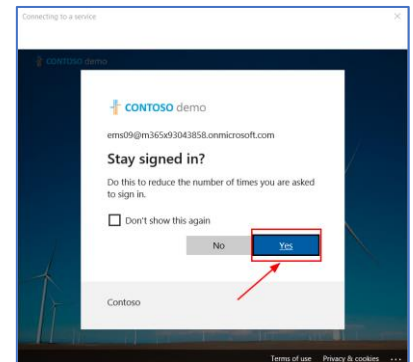
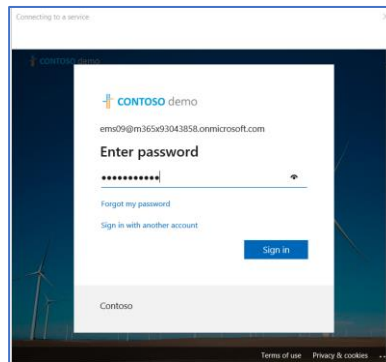
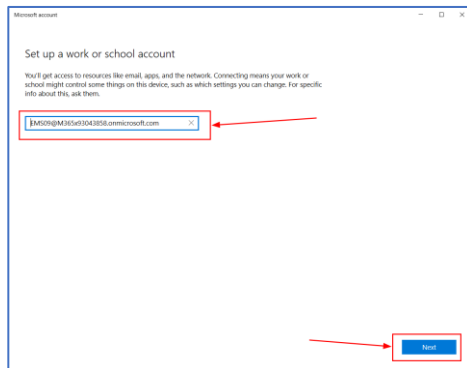
2. Nos informa que la cuenta de empresa ya ha sido creada en el dispositivo. Y ahora lo tendremos que conectar al servicio y podemos elegir una categoría para el mismo. Clic en el botón **Siguiente**.



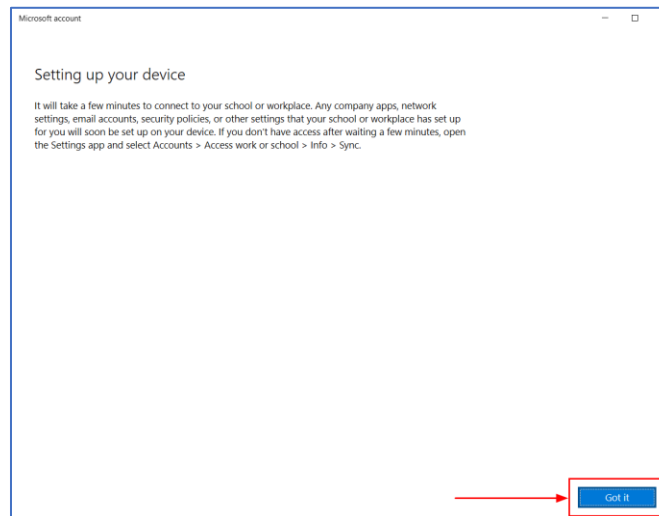
3. Clic en el botón **Conectar** para continuar el proceso de inscripción de empresa:



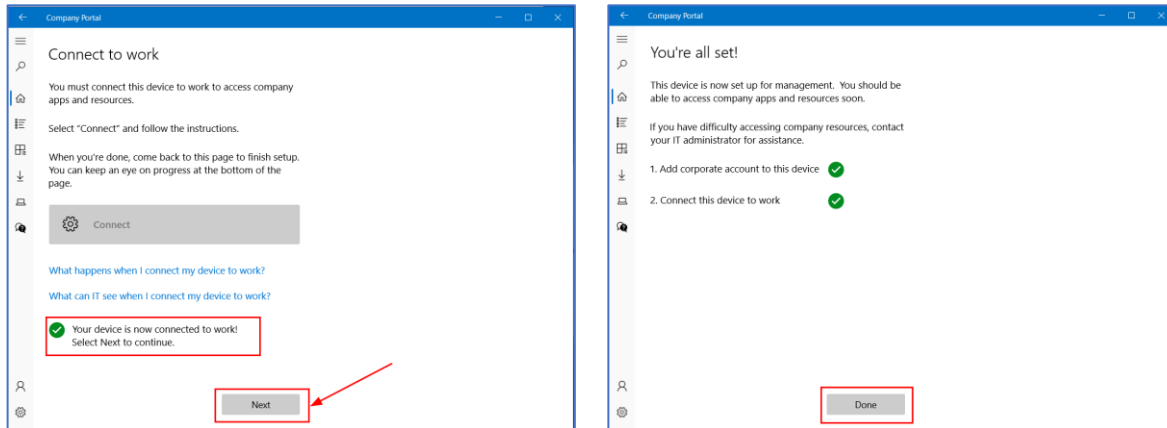
4. Nos tendremos que autenticar con nuestro usuario: EMSox@m365*****.onmicrosoft.com (podríamos usar cualquier usuario que tenga derechos en enroll asignados en nuestra tenant usuario@m365xxx.onmicrosoft.com).



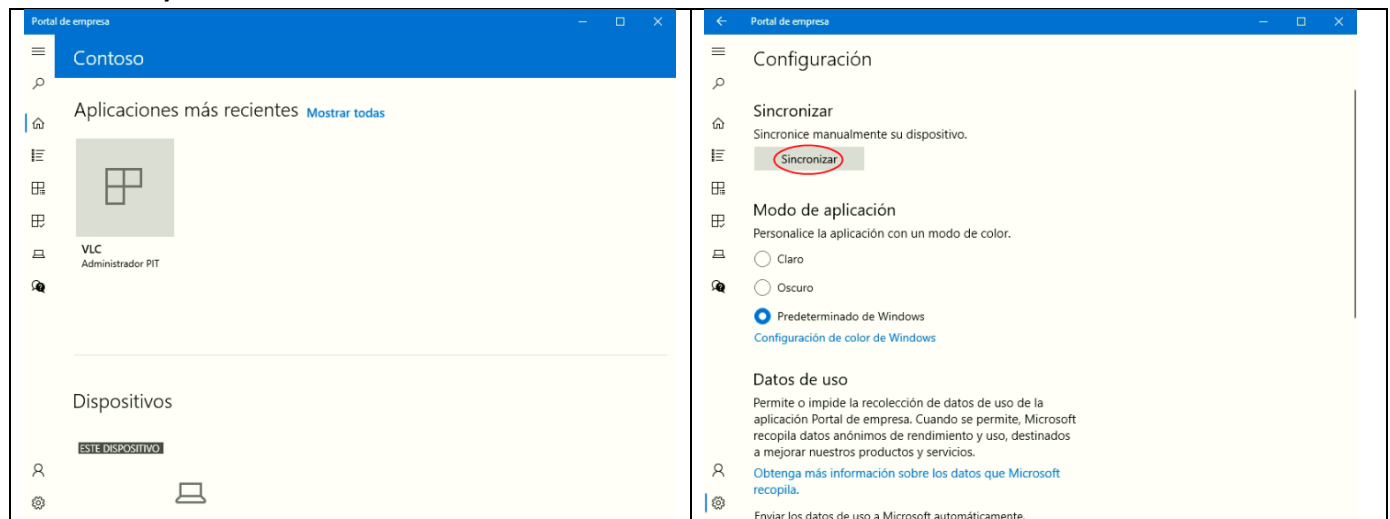
5. Nos inscribirá en el servicio y nos aparecerá el mensaje "Configurando el dispositivo":







6. Nos aparecerá el mensaje "El dispositivo ya está conectado al trabajo. Seleccione Siguiente para continuar". **Clic en los 2 botones: Siguiente** de las 2 próximas ventanas.



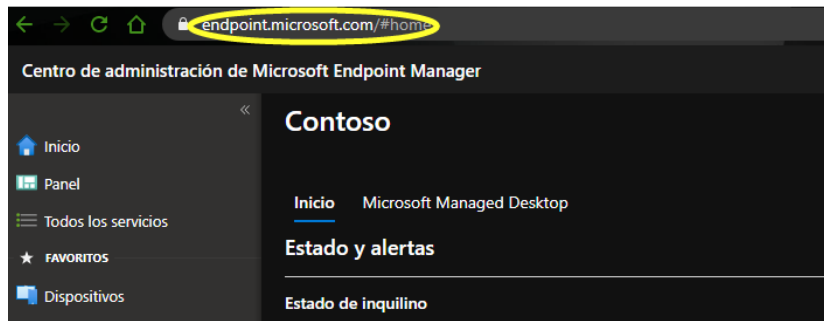
7. Dentro de **Portal de Empresa** ya nos aparece **la máquina enrolada** y podemos realizar una **sincronización** con Azure Active Directory, servicios de EMS que nuestra empresa nos entrega. **Clic en el botón Sync**:



8. **Nosotros como Administradores**, también desde el **portal de EMS**, podemos **forzar la sincronización** de los dispositivos inscritos.
9. Tendremos que ir a vía nuestro **navegador web** preferido (recomendado Google Chrome) a la siguiente URL del **Centro de administración de Microsoft Endpoint Manager**: <https://endpoint.microsoft.com/>
Usuario: EMS0x@m365*****.onmicrosoft.com (la "x" es el usuario que os hemos dado al comienzo del curso).
Contraseña: HolaMundoo01 (o la contraseña que hayas puesto cuando el sistema te obligó a cambiarla)

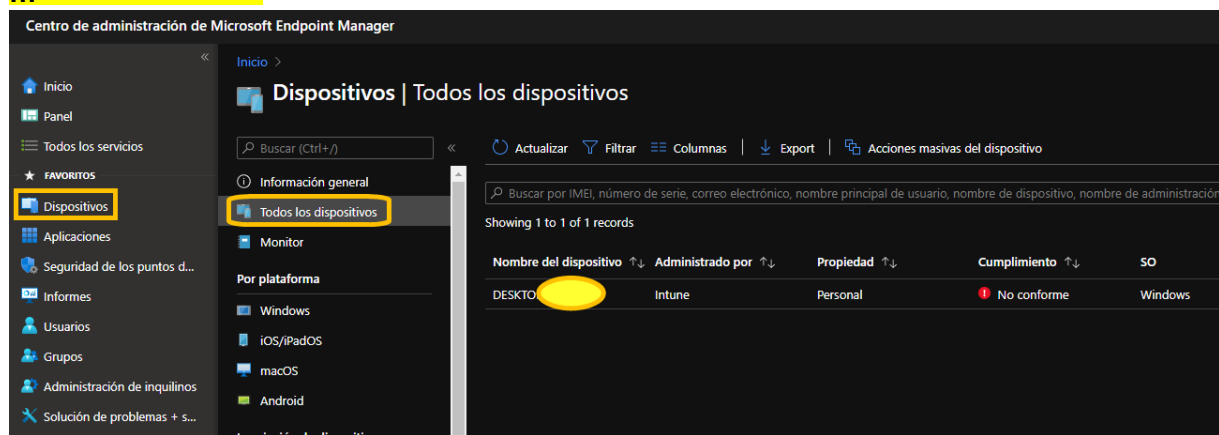
<div><h3>Microsoft Azure</h3></div> <div> Selección de la cuenta Continuar a Microsoft Azure</div> <div> EMS0@m365x414731.onmicrosoft.com : om</div>	<div> ← EMS0@m365x414731.onmicrosoft.com</div> <div>Escribir contraseña</div> <div><input type="password" value="....."/></div> <div>He olvidado mi contraseña</div> <div><input type="button" value="Iniciar sesión"/></div> <div><input type="text" value="Contoso"/></div>	<div> EMS0@m365x414731.onmicrosoft.com</div> <div>¿Quiere mantener la sesión iniciada?</div> <div><p>Haga esto para reducir el número de veces que se le solicita que inicie sesión.</p><input type="checkbox"/> No volver a mostrar</div> <div><input type="button" value="No"/> <input type="button" value="Sí"/></div> <div><input type="text" value="Contoso"/></div>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

10. Aparecerá el Centro de administración de Microsoft Endpoint Manager.

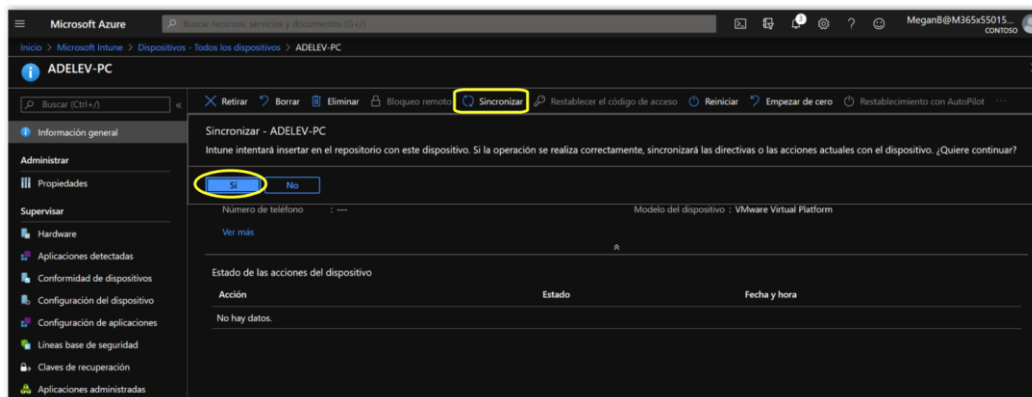


Y clic en la entrada del menú vertical de la izquierda **Dispositivos**.

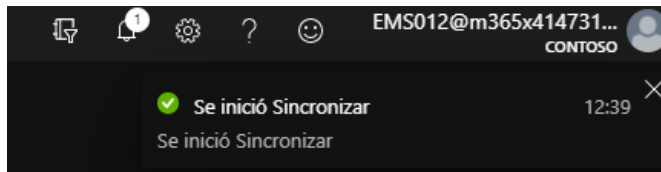
11. Clic en **Todos los dispositivos**. Veremos los dispositivos que se han inscrito en el servicio vía **Portal de empresa**. Clic en el nombre de nuestro PC o **dispositivo que acabamos de enrrolar en EMS**. Nos aparecerá tanto nuestro PC Windows 10 como el resto de nuestros compañero de curso. **¡¡¡IMPORTANTE!!!**. Clic en el nuestro.



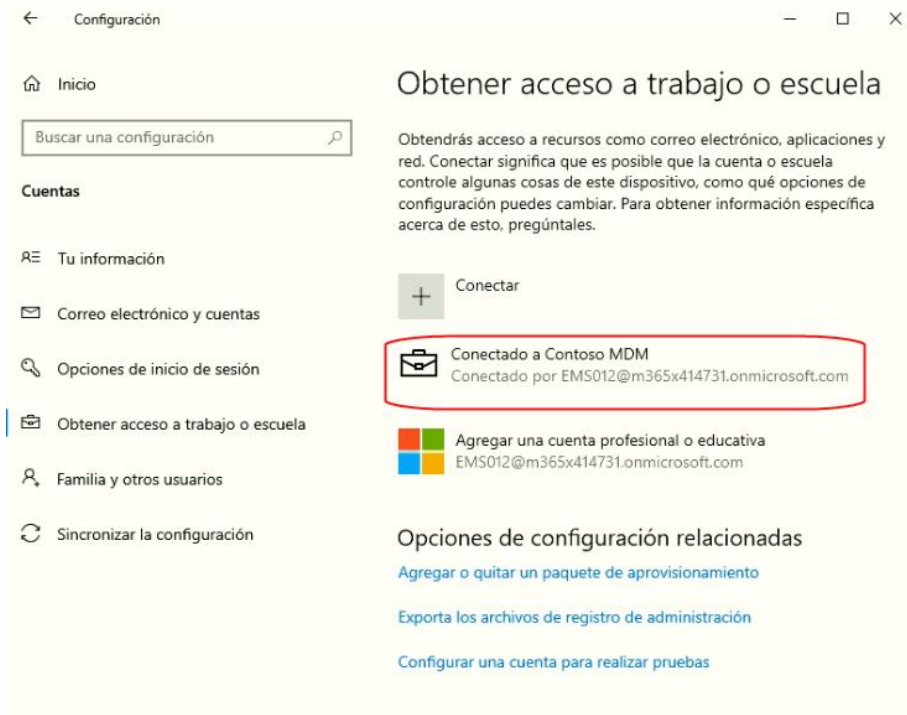
12. Clic en el botón: **Sincronizar**.



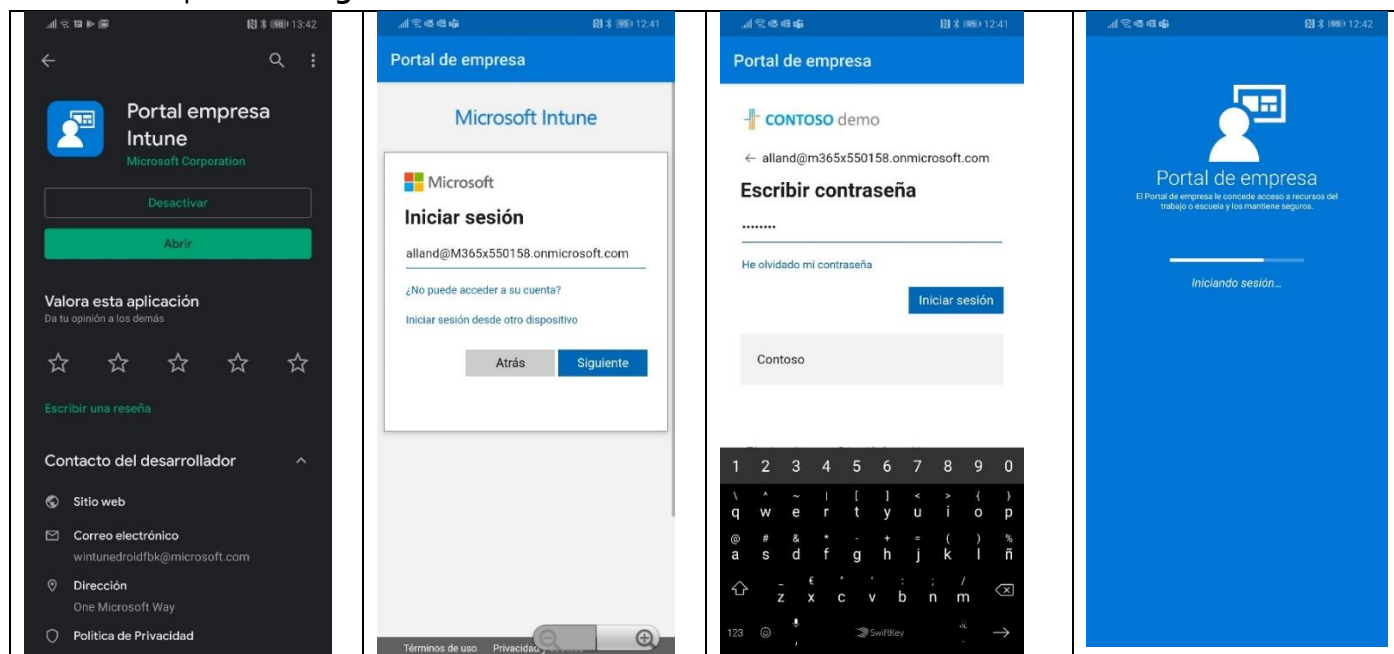
13. Aparecerá la **ventana informativa** correspondiente a esta **tarea de sincronización de dispositivos**.



14. Nos **aparecerá un nuevo usuario** dentro de nuestro Sistema Operativo: **Windows 10. Menú Inicio de Windows > Configuración > Cuentas > Obtener acceso a trabajo o escuela.**



15. Podremos usar estos mismos servicios desde una **tableta/móvil**. Para ello, buscaremos el **App Portal empresa Intune** en **Google Play** y/o **Apple Store**. La instalaremos en nuestro móvil y simplemente tendremos que hacer **login** con nuestro usuario.



Lab – 6.3: Enrolar dispositivos legacy (Windows 7) en el servicio de Microsoft Intune.

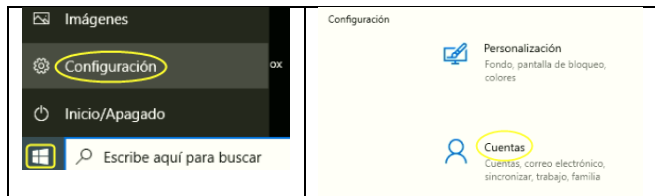
Objetivo: Cómo podemos enrolar dispositivos en modo personal que **NO** se van a convertir en corporativos, ya que son **propiedad del usuario (BOYD – No de la empresa)**, Windows 7 Pro/Enterprise por ejemplo (NO recomendado por Microsoft ya que Windows 7 ya no tiene soporte).

Microsoft Intune nos permite enrolar dispositivos móviles y PCs/portátiles **personales** para mantener protegidos los datos de nuestra compañía **SIN impactar en la gestión del dispositivo**, ya que no es propiedad de la empresa.

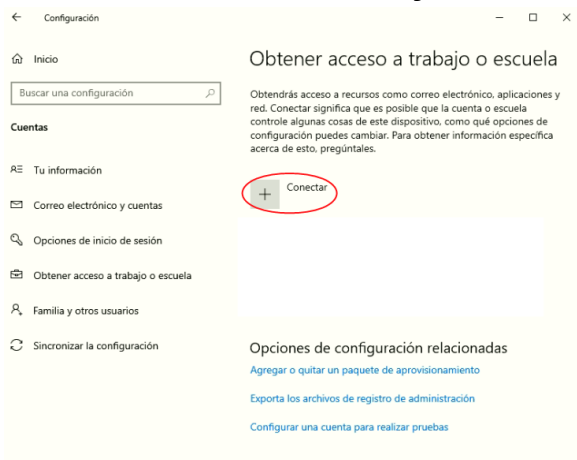
Prerequisitos: Tener una tenant de EMS Enterprise Mobility + Security E5 propia o trial.

Pasos a realizar para inscribir un dispositivo Windows 10 personal propiedad del usuario – Entorno BYOD:

1. Desde el propio **dispositivo** (Windows, Android o iOS) buscamos la entrada **Settings (Configuración)**: En Windows 10, **menú Inicio** de Windows > **Configuración** > **Cuentas**.



2. **Clic en Obtener acceso a trabajo o escuela > Clic en el botón Conectar.**



3. Nos aparecerá una **ventana** donde tendremos que hacer **login** en los Servicios Cloud de Microsoft con el email y la contraseña de un **usuario administrador local de la máquina** y con **permisos de enroll** en la tenant y seguiremos el proceso hasta finalizarlo.

Microsoft account

Set up a work or school account

You'll get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.

AdeleV@M365x000350.OnMicrosoft.com

Next

Lab – 6.4: Crear categorías para nuestros dispositivos en EMS/Intune.

Objetivo: Las **categorías** nos permiten **tener organizados** nuestros **recursos** dentro de la tenant. Podemos crear categoría en función de la ubicación geográfica de la empresa de nuestro cliente, por delegaciones (*Madrid, Barcelona, Sevilla, Bilbao, Valencia, etc*), por departamento (*comercial técnico, etc*), etc. Tenemos que tener en cuenta que algunos o muchos de estos **dispositivos** pueden **estar fuera de la empresa** con lo cual es mejor tener **una buena política de categorías** para saber en todo momento de que dispositivo estamos hablando.

Microsoft EMS nos **permite categorizar los dispositivos** enrolados en el servicio bajo los criterios que más de adecuen a nuestra forma de trabajar y a nuestra empresa.

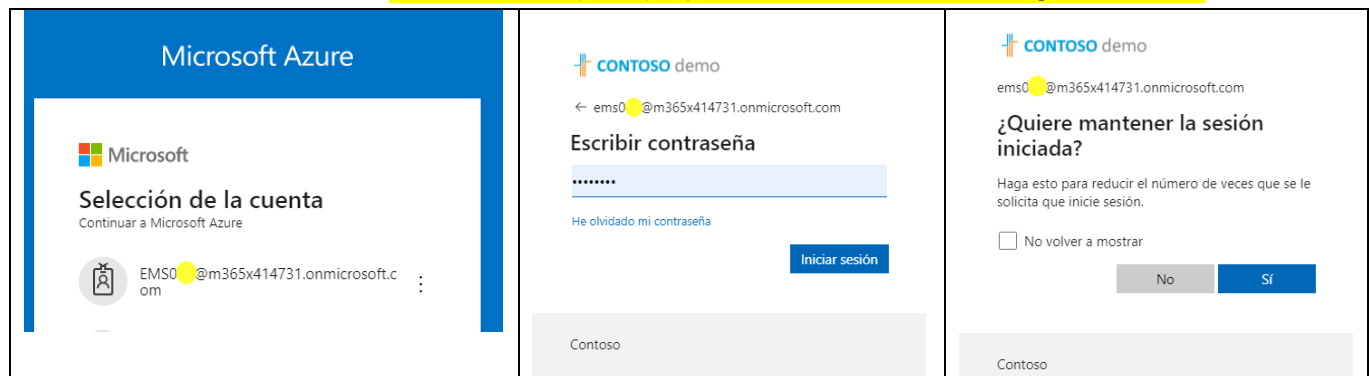
Prerequisitos: Tener una tenant de EMS Enterprise Mobility + Security E5 propia o trial.

Pasos a realizar:

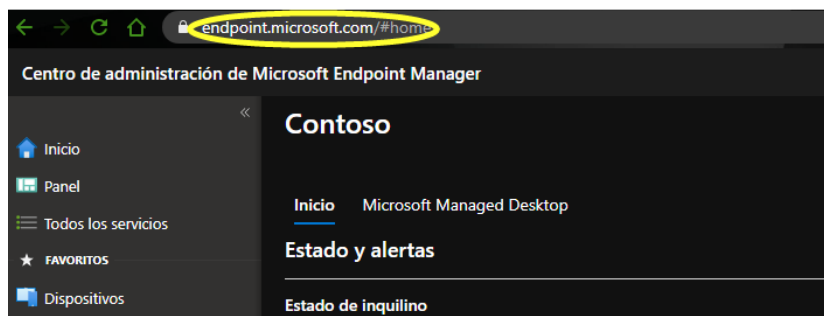
1. Logarnos con nuestras credenciales de admin al **Centro de administración de Microsoft Endpoint Manager**: <https://endpoint.microsoft.com/>.

Usuario: EMSox@m365*****.onmicrosoft.com (la "x" es el usuario que os hemos dado al comienzo del curso).

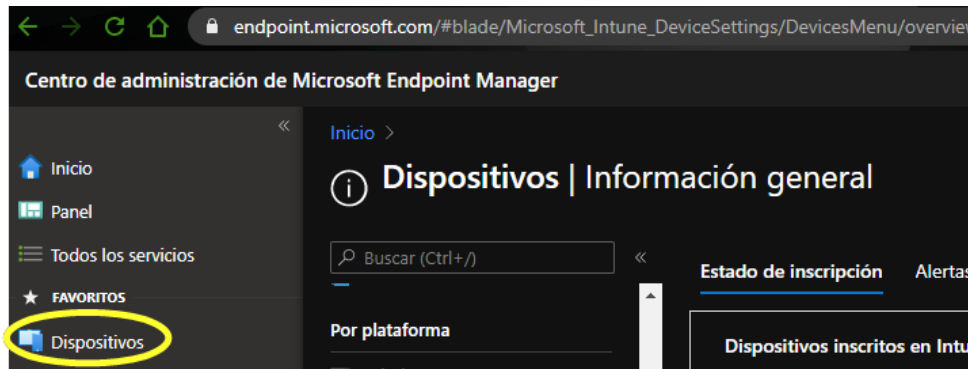
Contraseña: HolaMundoo1 (o la contraseña que hayas puesto cuando el sistema te obligó a cambiarla)



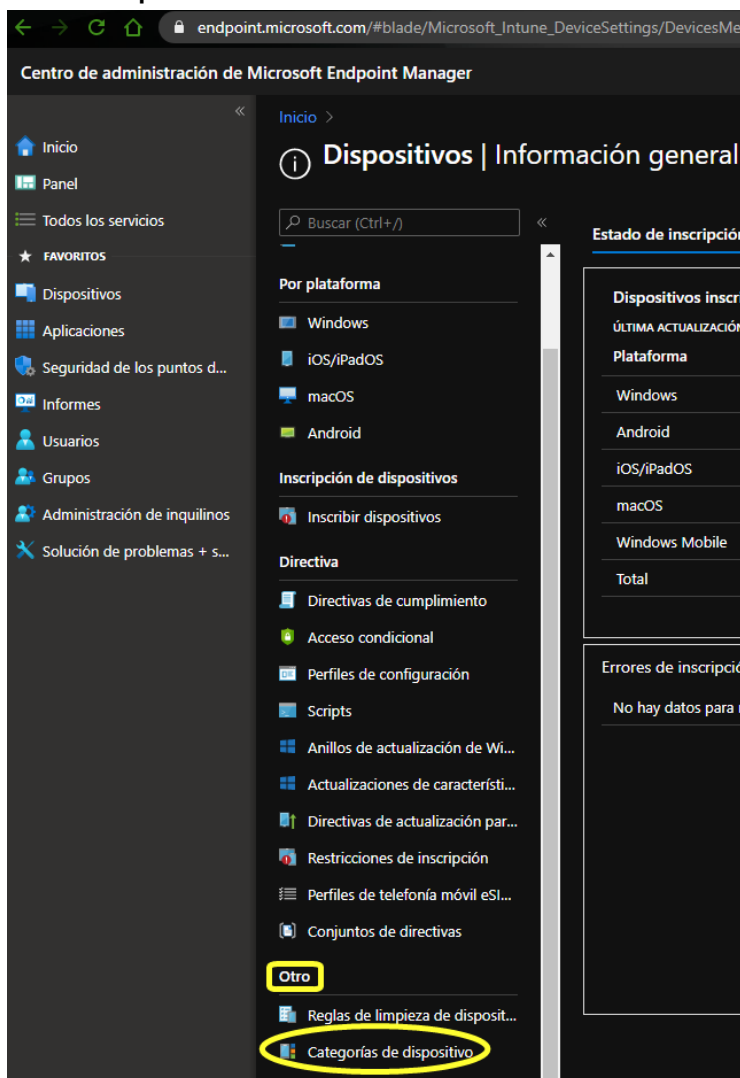
2. **Aparecerá** el Centro de administración de Microsoft Endpoint Manager.



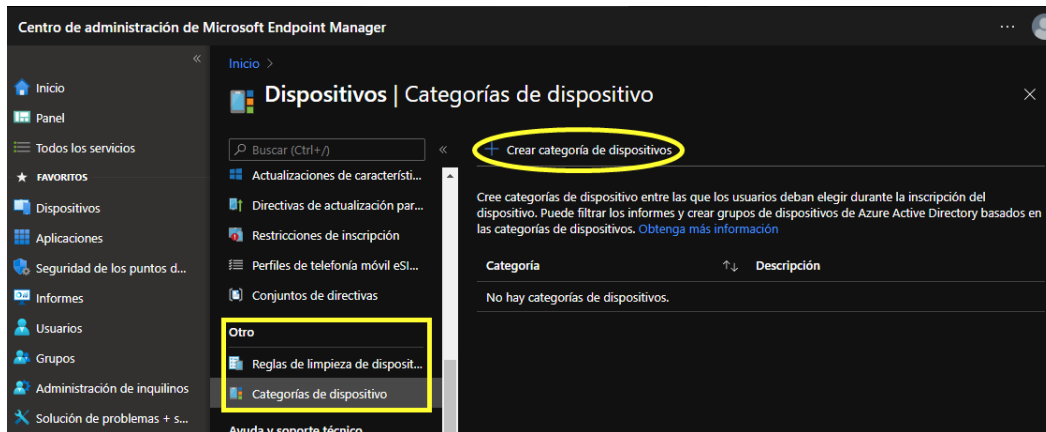
3. Clic en la entrada **Dispositivos** en el menú vertical de Azure al lado izquierdo de la pantalla.



4. Clic en la entrada del nuevo menú vertical que aparece en la pantalla dentro de la sección **"Otro"** en **Categorías de dispositivos**, si no la vemos, hacer scroll en el menú vertical de configuración, ya que está en la parte inferior.



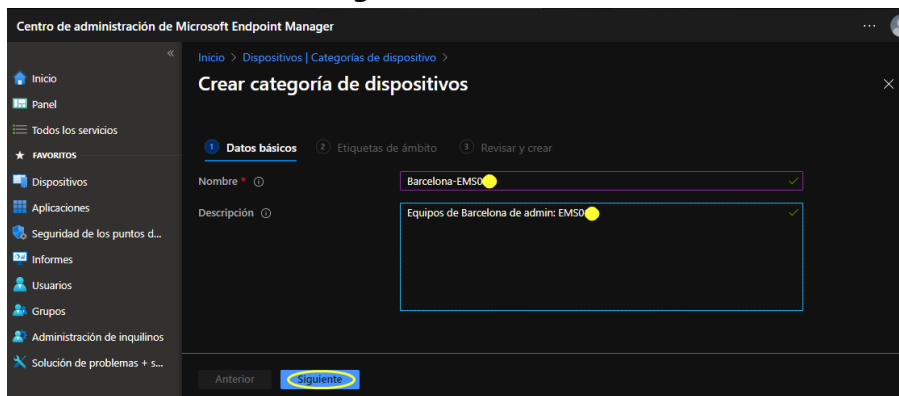
5. Clic en el botón superior + Crear categoría de dispositivos:



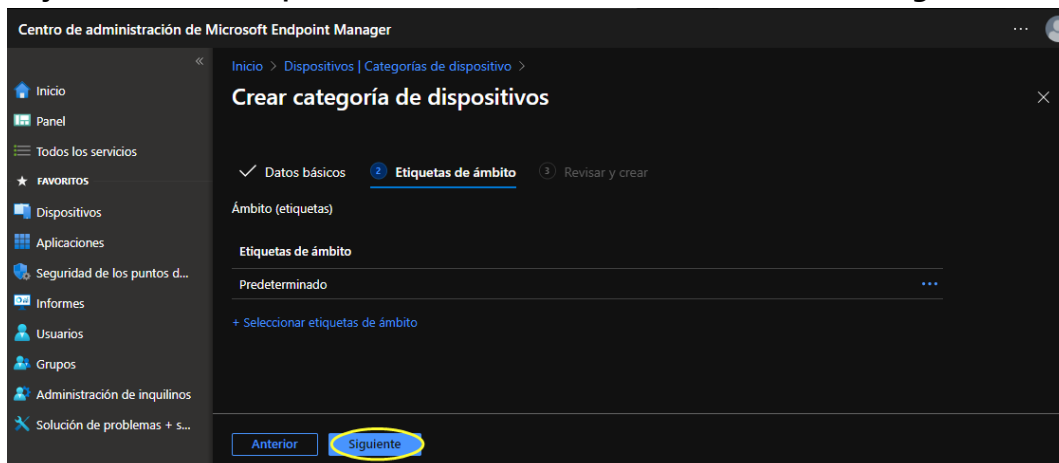
6. En la **ventana: Datos básicos**. Escribimos el nombre de nuestra ciudad o de un departamento, en este ejemplo, podemos poner:

- Nombre:** Barcelona- EMSox (la "x" correspondiente a nuestro usuario administrador)
- Podemos especificar una **Descripción**, sí queremos.

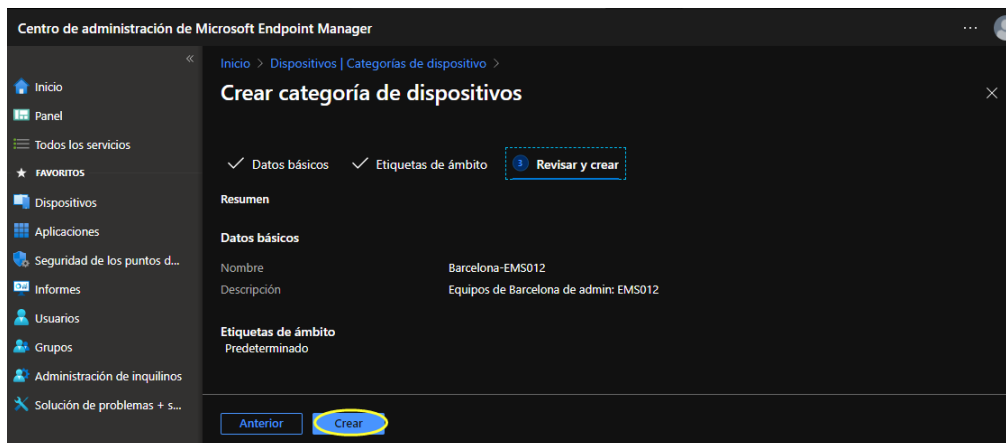
Clic en el botón: **Siguiente**.



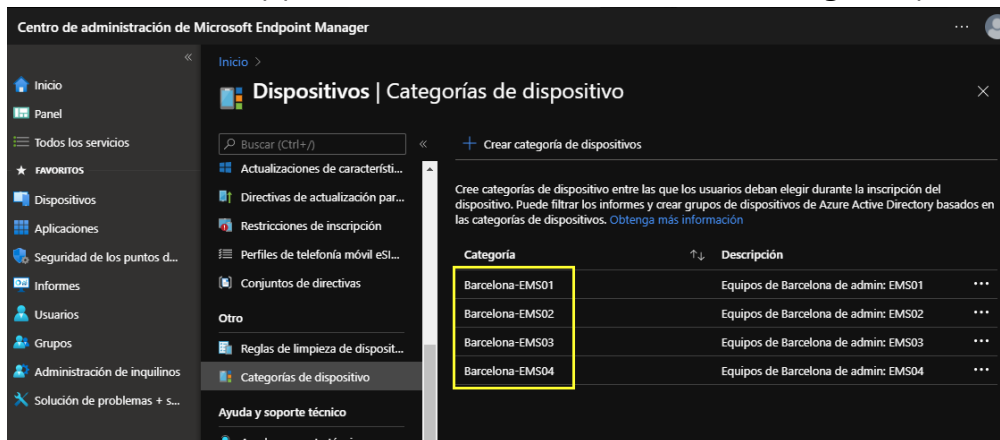
7. Dejar la **ventana Etiquetas de ámbito** en blanco. Clic en el botón: **Siguiente**.



8. Dejar la ventana Revisar y crear en blanco. Clic en el botón: Crear.



9. Aparecerá la categoría que acabamos de crear, junto con las que crearon el resto de compañeros en esta formación y podremos modificar o crear nuevas categorías para nuestros dispositivos.



iii SEGUIR ESTOS MISMOS PASOS para CREAR las CATEGORIAS!!!:
Madrid-EMSox , Sevilla-EMSox, Valencia-EMSox, Bilbao-EMSox, etc.

Lab – 6.5: Inscribir dispositivo en el proceso de instalación de Windows 10.

Objetivo: Cómo podemos enrolar un dispositivo Windows 10 durante el proceso de instalación del Sistema Operativo Windows 10 Pro o Enterprise, en Microsoft Intune.

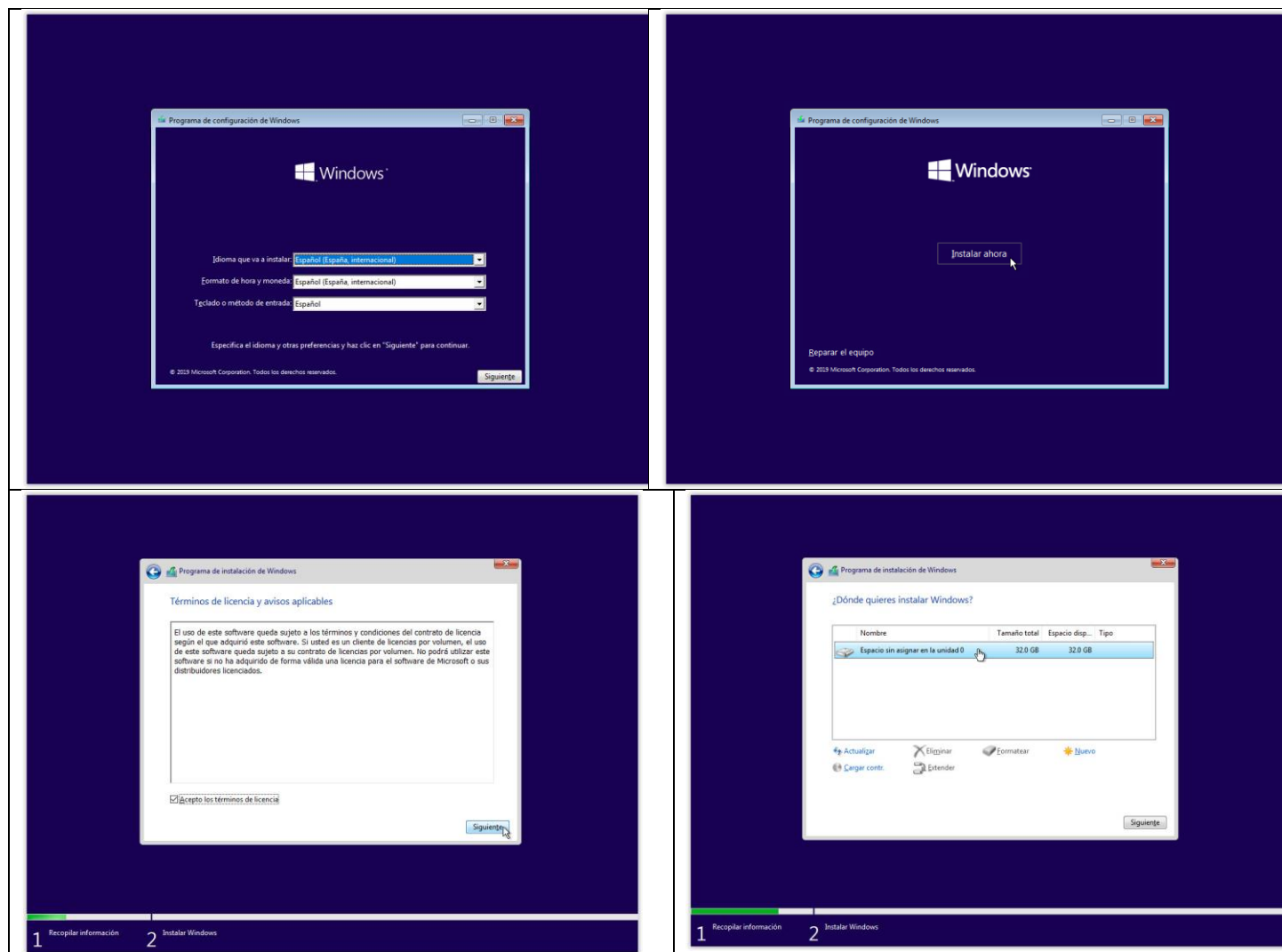
Microsoft Intune nos permite enrolar dispositivos en el proceso de instalación del SO: Windows 10 Pro/Ent.

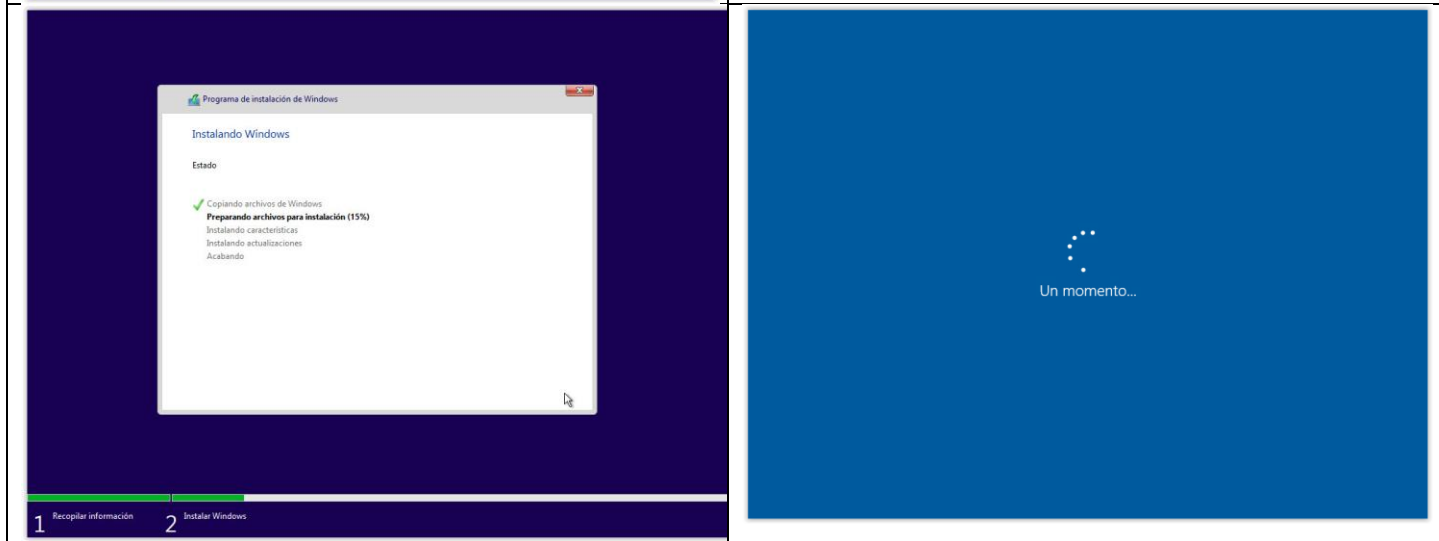
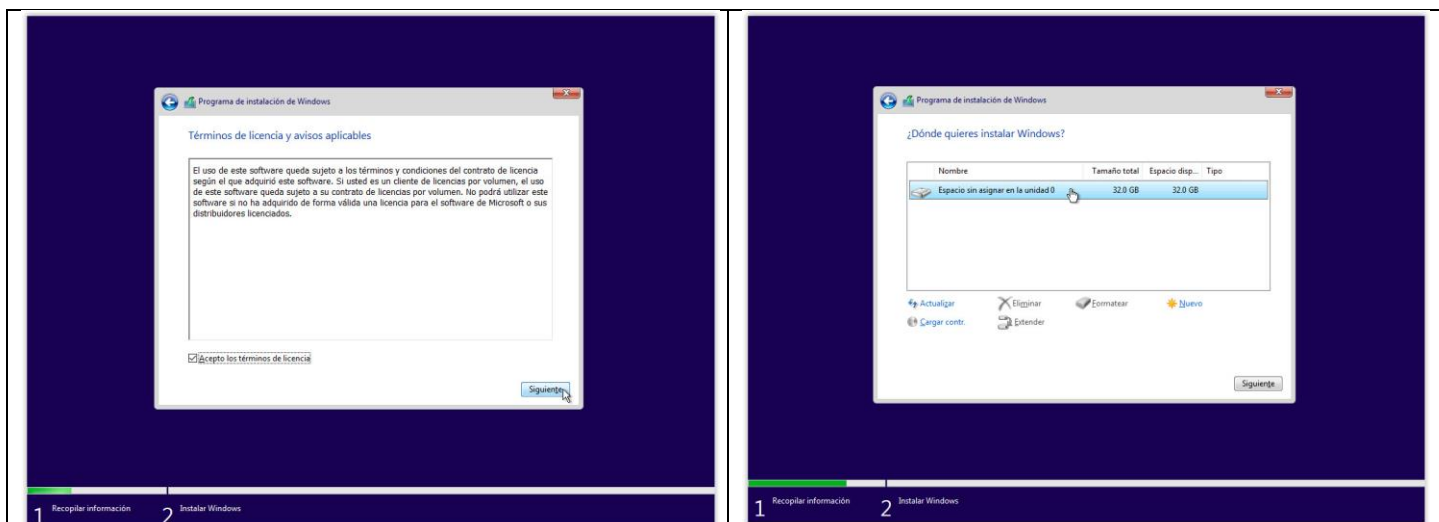
Prerequisitos: Tener una tenant de EMS Enterprise Mobility + Security E5 propia o trial.

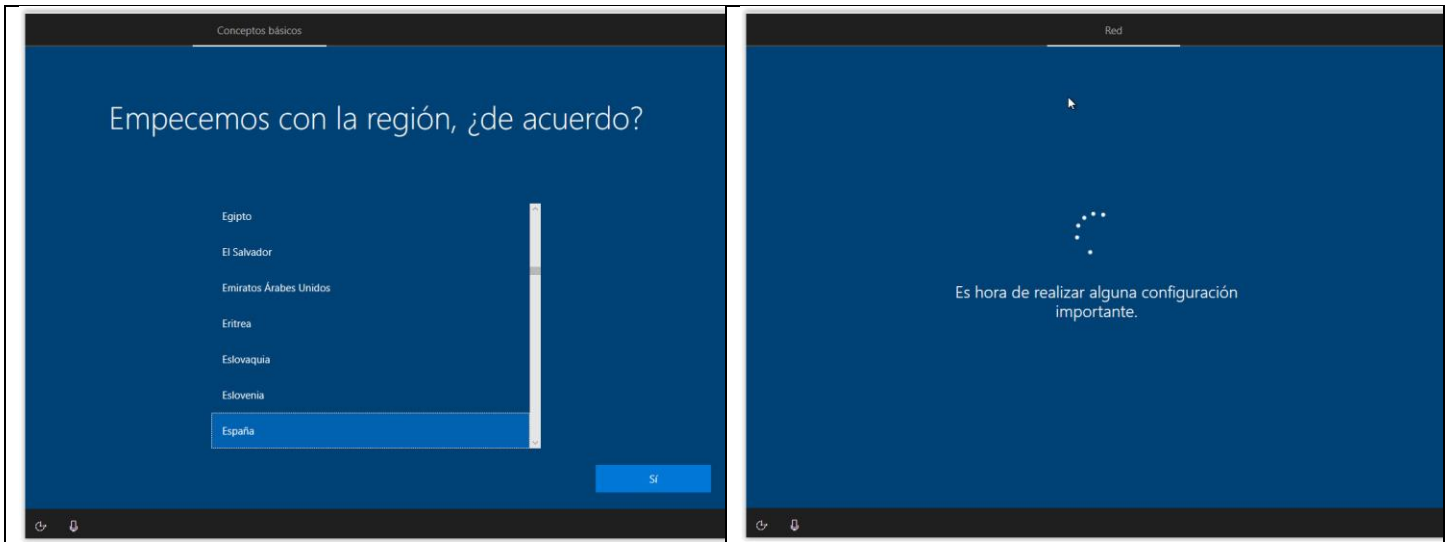
Enlace paso a paso de Microsoft: <https://docs.microsoft.com/es-es/intune-user-help/enroll-windows-10-device>

Pasos a realizar:

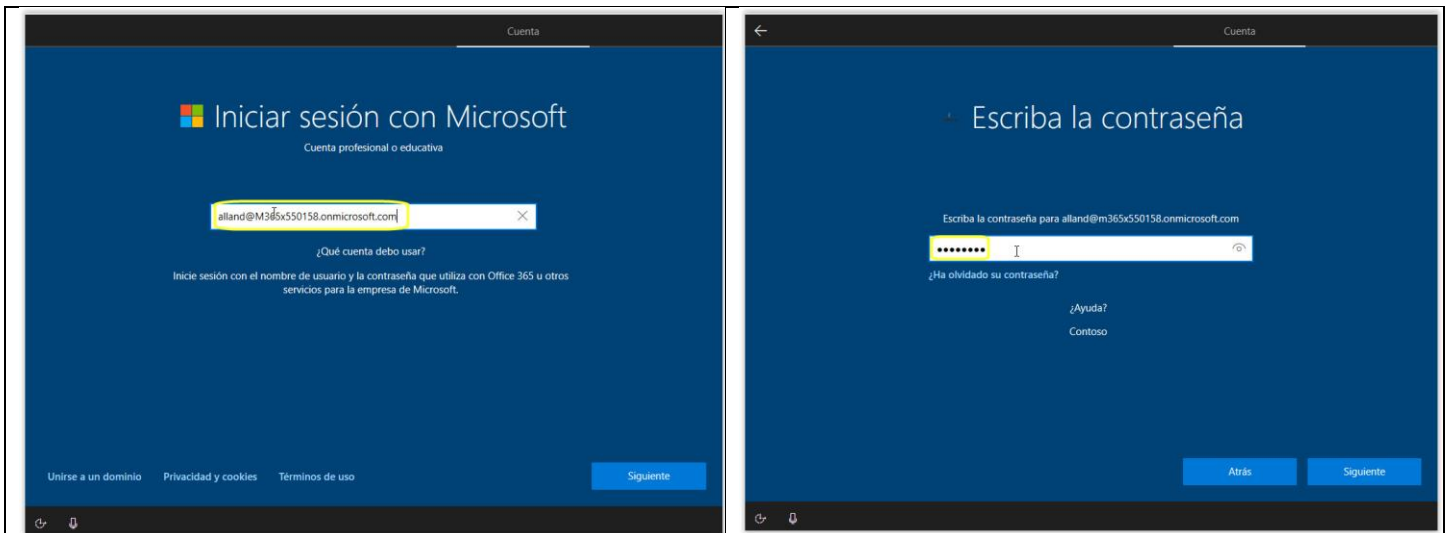
1. **Comenzamos la instalación de Windows 10 en el PC (versión Professional o Enterprise).** Comenzamos la instalación desde un **USB o DVD** con la imagen de instalación de **Windows 10 Business Editions**.

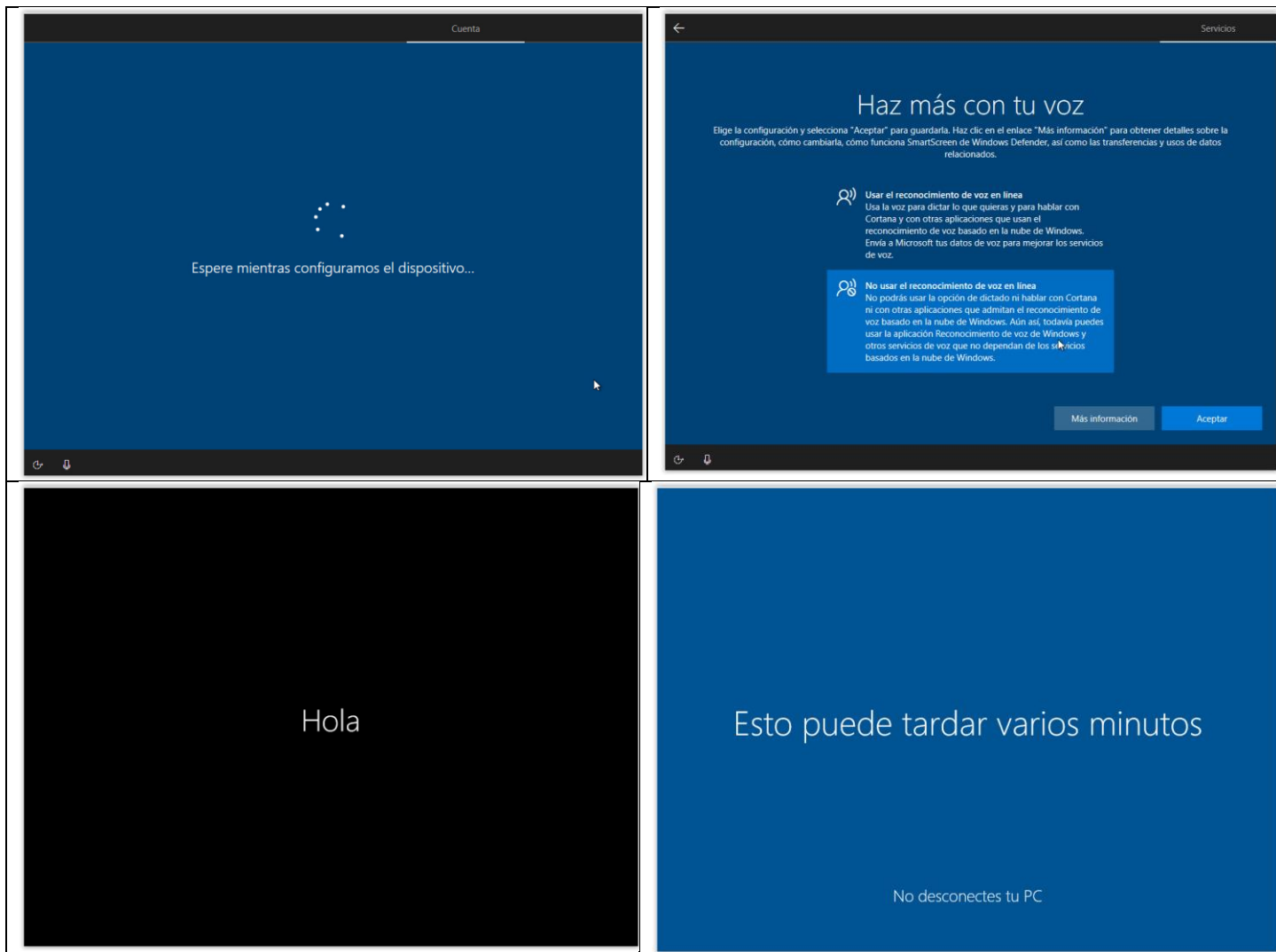




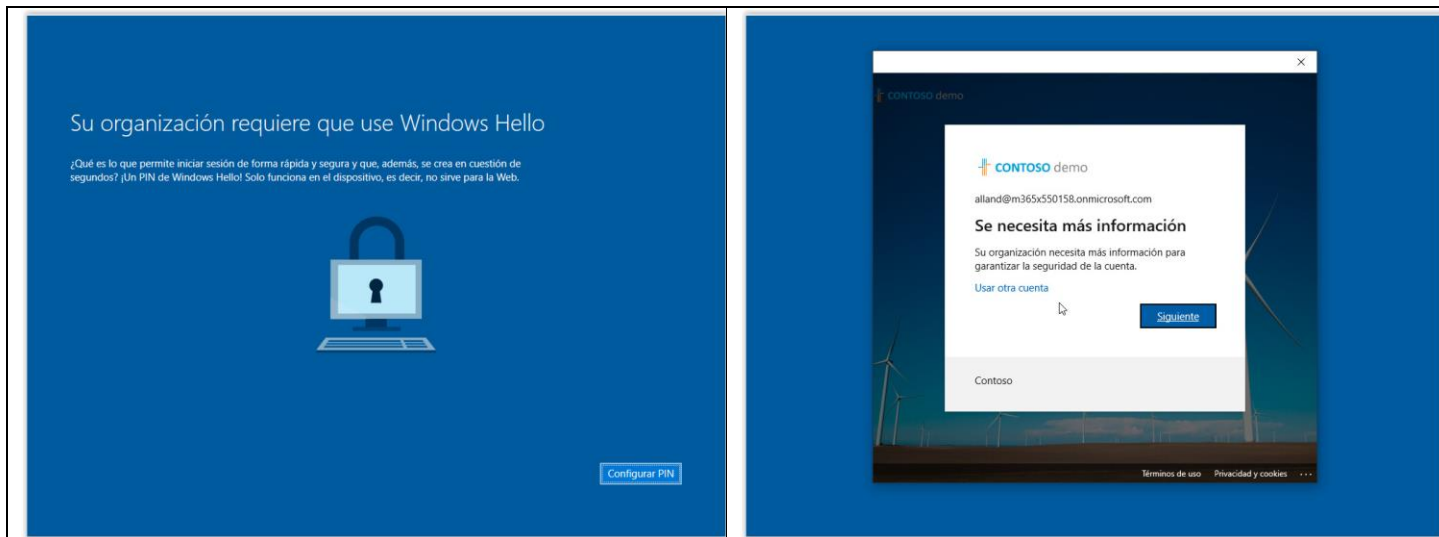



2. Iniciamos sesión con el usuario de AAD al que pertenece este dispositivo para inscribirlo en EMS/Intune: alland@m365xxx.onmicrosoft.com /Contraseña.





3. Opciones de configuración de nuestra empresa en la que forzamos el MFA de los usuarios:



 **CONTOSO** demo

Comprobación de seguridad adicional

Proteja su cuenta agregando más comprobación de teléfono a su contraseña. Ver vídeo para saber cómo proteger su cuenta

Paso 1: ¿De qué manera deberíamos ponernos en contacto con usted?

Teléfono de autenticación

España (+34)

673156795

Método

☒ Enviarme un código mediante mensaje de texto

Siguiente

Sus números de teléfono sólo se usarán para proteger su cuenta. Se aplicará la tarifa estándar de teléfono y SMS.

A screenshot of a web browser showing the Microsoft account security verification process. The browser's address bar displays 'https://www.microsoft.com/...'. The page header includes the 'CONTOSO' logo and the word 'demo'. The main heading is 'Comprobación de seguridad adicional'. Below this, a message states: 'Proteja su cuenta enviando más comprobación de teléfono a su contraseña. Ver video para saber cómo proteger su cuenta'. The next step is highlighted: 'Paso 2: Hemos enviado un mensaje de texto a su teléfono +34 673156795'. A sub-instruction says: 'Escriba aquí el código de verificación cuando lo reciba'. A text input field contains the number '4698771', and a small 'x' icon is visible to its right. At the bottom, there are two buttons: 'Cancelar' (disabled) and 'Comprobar' (active, highlighted with a mouse cursor). The footer contains the text '©2020 Microsoft | Legal | Privacidad'.

A screenshot of a web browser window showing the Microsoft account security verification process. The browser's address bar displays 'https://www.microsoft.com'. The page header includes the 'CONTOSO' logo and the text 'demo'. The main heading is 'Comprobación de seguridad adicional' (Additional security verification). Below this, a message states: 'Proteja su cuenta agregando más comprobación de teléfono a su contraseña. Ver vídeo para saber cómo proteger su cuenta' (Protect your account by adding more phone verification to your password. Watch video to learn how to protect your account). A large blue button with the text 'Paso 2: Hemos enviado un mensaje de texto a su teléfono +34 673156795' (Step 2: We have sent a text message to your phone +34 673156795) is prominent. Below the button, it says '(Comprobación correcta)' (Verification correct). At the bottom right, there is a blue button labeled 'Listo' (Ready) with a mouse cursor hovering over it. The footer contains the text '©2020 Microsoft | Legal | Privacidad'.

Seguridad de Windows

Configurar un PIN

Crea un PIN para usarlo en vez de las contraseñas. Tener un PIN hace que sea más fácil iniciar sesión en los dispositivos, las aplicaciones y los servicios.

☒ Incluir letras y símbolos

[Requisitos de PIN](#)

Proporciona un PIN que cumpla los requisitos de complejidad. El PIN debe tener al menos 6 caracteres.

Aceptar Cancelar

Seguridad de Windows

Configurar un PIN

Crea un PIN para usarlo en vez de las contraseñas. Tener un PIN hace que sea más fácil iniciar sesión en los dispositivos, las aplicaciones y los servicios.

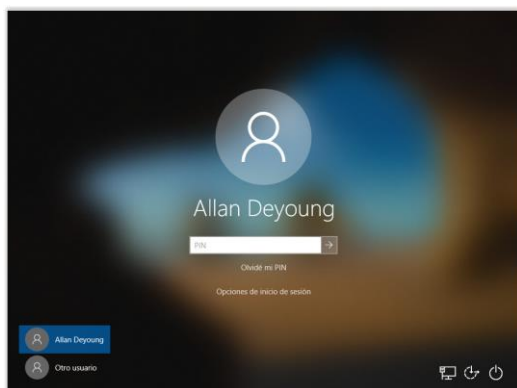
☒ Incluye letras y símbolos

[Requisitos de PIN](#)

Proporciona un PIN que cumpla los requisitos de complejidad. El PIN debe tener al menos 6 caracteres.

Aceptar Cancelar

4. Sí reiniciamos el equipo, ya nos aparecerá la opción de PIN que nos ha obligado a configurar el MFA para que este usuario: alland@m265xxx.onmicrosoft.com pueda hacer login en el equipo.



5. Lo primero, sí queremos que funcione todo correctamente, tendremos que **activar el Windows 10** y usar **Windows Update** para **obtener el último nivel de parcheado**.
6. El usuario **administrador local de la máquina** con el que hemos terminado el proceso de instalación. una vez nos hayamos enrolado el equipo se le revocarán los permisos de administrador local sobre la máquina por defecto. Para poder **instalar cualquier software** una vez terminemos en **enroll** del equipo como **Organización**, nos pedirá un usuario **administrador de Intune** para poder instalar (sí así lo definimos en nuestra directiva). ESTAMOS EN EL DOMINIO DE Azure Active Directory (Similar al domino de Windows Server Active Directory). Similar a la unión a un dominio de Windows Server Active Directory a través de la característica "miembro de..." desde las propiedades de "MI PC".
7. **Convertimos el equipo en corporativo**. Instalando el App "**Portal de Empresa**" desde **Microsoft Store** y siguiendo todos los pasos descritos en anteriores laboratorios.

Lab – 6.6: Cambiar la propiedad del dispositivo a Corporativo en la consola de Intune.

Objetivo: Cómo podemos cambiar la propiedad de un dispositivo inscrito o enrolado en EMS /Intune de **BOYD: Propiedad del usuario a Corporativo: Propiedad de la empresa.**

Microsoft Intune nos permite cambiar la propiedad de los dispositivos una vez enrolados en EMS/Intune. Las opciones que tenemos disponibles de administración varían drásticamente

1. **Dispositivo propiedad del usuario.** Podemos servirle **Apps Corporativas**, securizando los **datos empresariales**, en este caso, **NO** podremos realizar un **wipe**, o cualquier **otra acción drástica**, ya que el dispositivo **NO** nos pertenece como compañía, sino al usuario.
2. **Dispositivo corporativo.** Tendremos el **control completo** sobre el mismo, ya que es **propiedad de la empresa**.
3. **Una vez que hayamos realizado este paso. ESTAMOS UNIENDO ESTE EQUIPO AL DOMINIO DE Azure Active Directory** (Similar a la unión al con la característica “miembro de...” desde las propiedades de “MI PC” a un dominio de Windows Server Active Directory). Por lo que, si queremos **instalar algún software** o **cambiar la configuración del equipo**, tendremos que **usar un usuario admin de Intune** dado de alta en la **tenant de Microsoft 365**. Nos aparecerá la **ventana de elevación de privilegios** (Usuario admin / Contraseña), exactamente igual que en un Windows Active Directory para realizar estos cambios.

Prerequisitos: Tener una tenant de EMS Enterprise Mobility + Security E5 propia o trial.

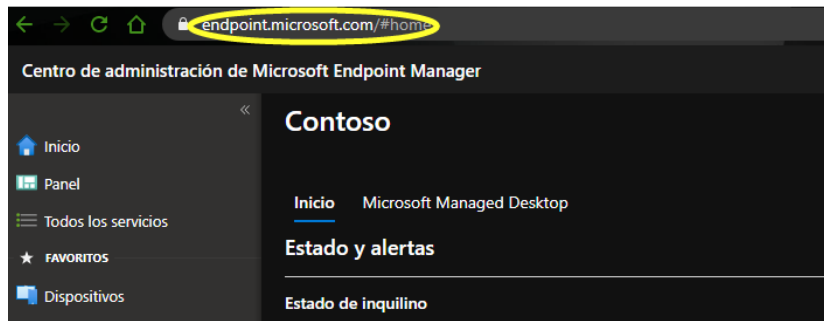
Enlace paso a paso de Microsoft: <https://docs.microsoft.com/es-es/intune-user-help/enroll-windows-10-device>

Pasos a realizar:

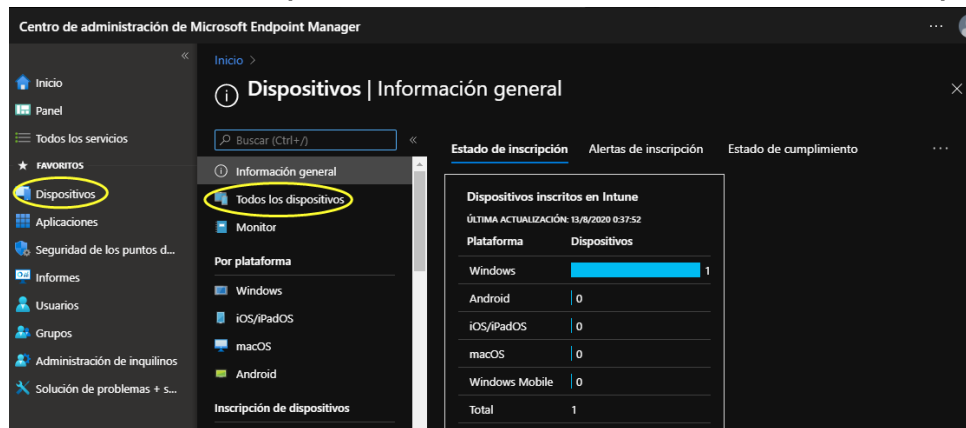
1. Logarnos con nuestras credenciales de admin al **Centro de administración de Microsoft Endpoint Manager**: <https://endpoint.microsoft.com/>.
Usuario: EMS0x@m365*****.onmicrosoft.com (la “x” es el usuario que os hemos dado al comienzo del curso).
Contraseña: HolaMundoo1 (o la contraseña que hayas puesto cuando el sistema te obligó a cambiarla)

<p>Microsoft Azure</p>	<p>CONTOSO demo</p> <p>← ems0x@m365x414731.onmicrosoft.com</p> <p>Escribir contraseña</p> <p>*****</p> <p>He olvidado mi contraseña</p> <p>Iniciar sesión</p> <p>Contoso</p>	<p>CONTOSO demo</p> <p>ems0x@m365x414731.onmicrosoft.com</p> <p>¿Quiere mantener la sesión iniciada?</p> <p>Haga esto para reducir el número de veces que se le solicita que inicie sesión.</p> <p><input type="checkbox"/> No volver a mostrar</p> <p>No Sí</p> <p>Contoso</p>
------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

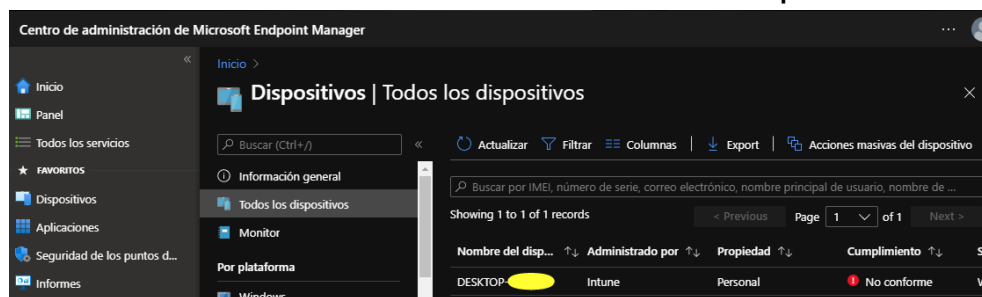
2. Aparecerá el Centro de administración de Microsoft Endpoint Manager.



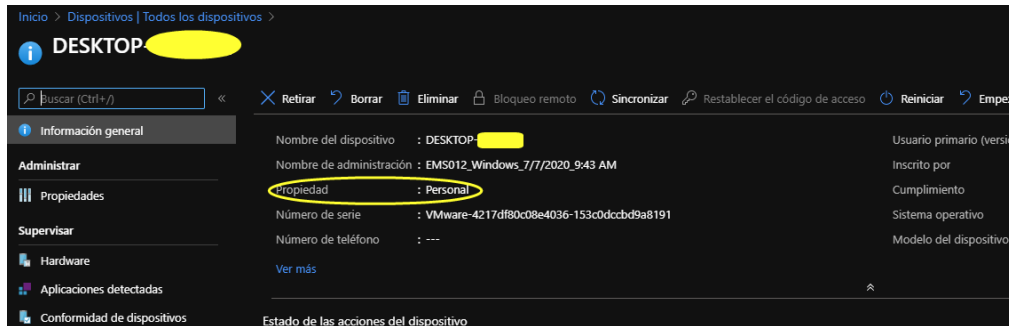
3. Clic en la entrada **Dispositivos**. En el nuevo menú Clic en **Todos los dispositivos**.



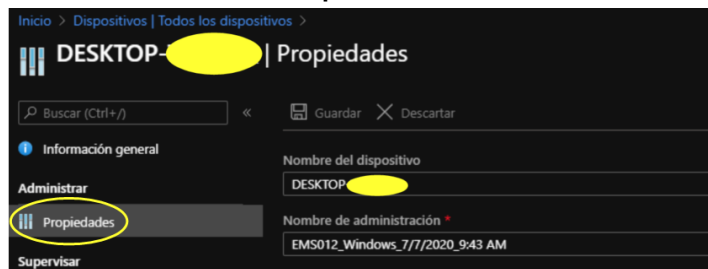
4. Veremos los dispositivos que se han inscrito, tanto el nuestro como el del resto de compañeros que están en esta formación. Clic en el nombre de nuestro dispositivo: **DESKTOP-xxxxxxx** o **EMSoxxxx**.



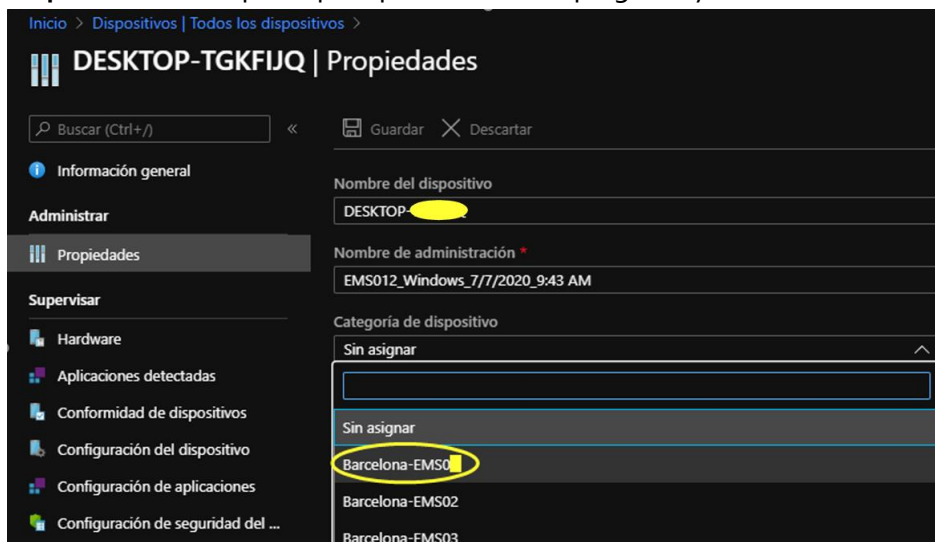
5. Nos aparecerá la **ventana de las propiedades** de este **dispositivo**, su nombre, Nombre de administración, **Propiedad: ACTUALMENTE** establecida como **personal**. Es decir, propiedad del usuario NO de nuestra empresa (BOYD).



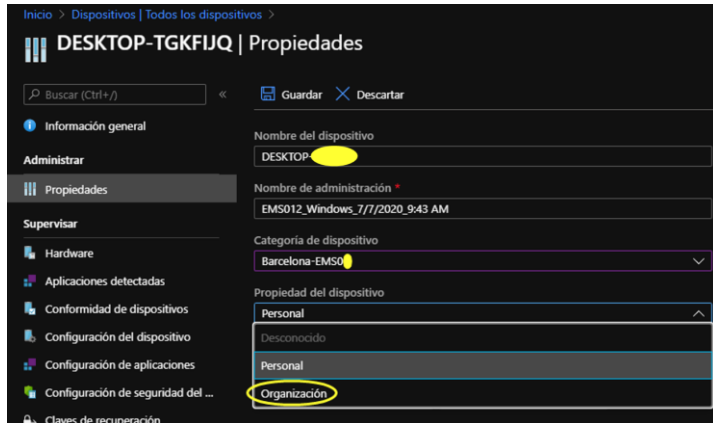
6. Clic en el menú de la izquierda dentro de la sección **Administrar** en la opción: **Propiedades**.



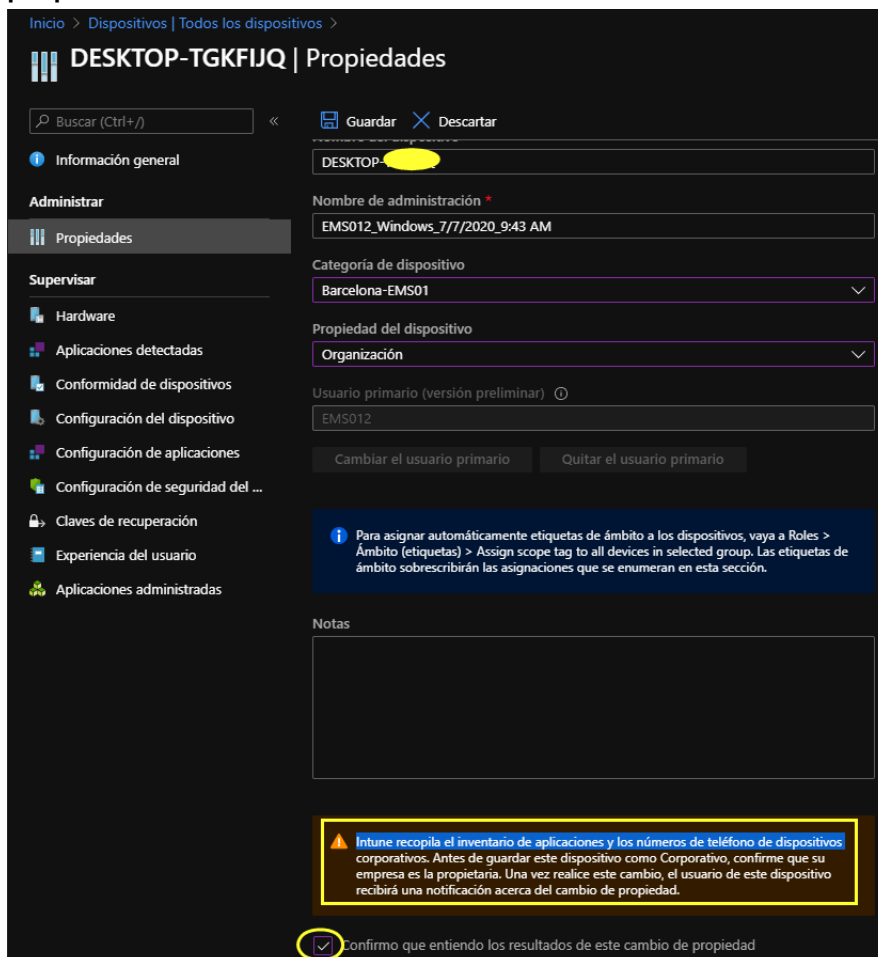
7. Aquí podríamos cambiar la categoría del dispositivo. Para ello, en la sección: **Categoría de dispositivo** > Clic para que aparezca en desplegable y clic en **Barcelona-EMSox**.



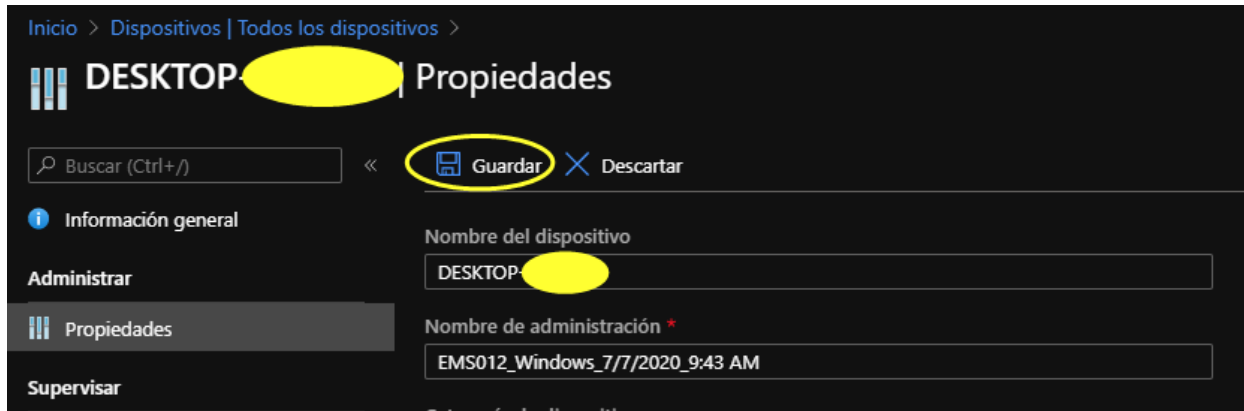
8. En la opción: **Propiedad del dispositivo:** Clic dentro del **desplegable** en el valor: **Organización**. En este punto estamos diciendo a Microsoft Endpoint Manager que este dispositivo es de nuestra empresa, con lo que podremos realizar muchas más tareas de administración sobre el mismo.



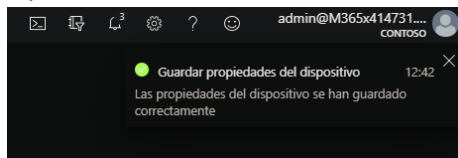
9. Nos pedirá que confirmemos el cambio de propiedad del dispositivo y nos informará de lo que esto significa. Clic en la caja de selección: "Confirmo que entiendo los resultados de este cambio de propiedad".



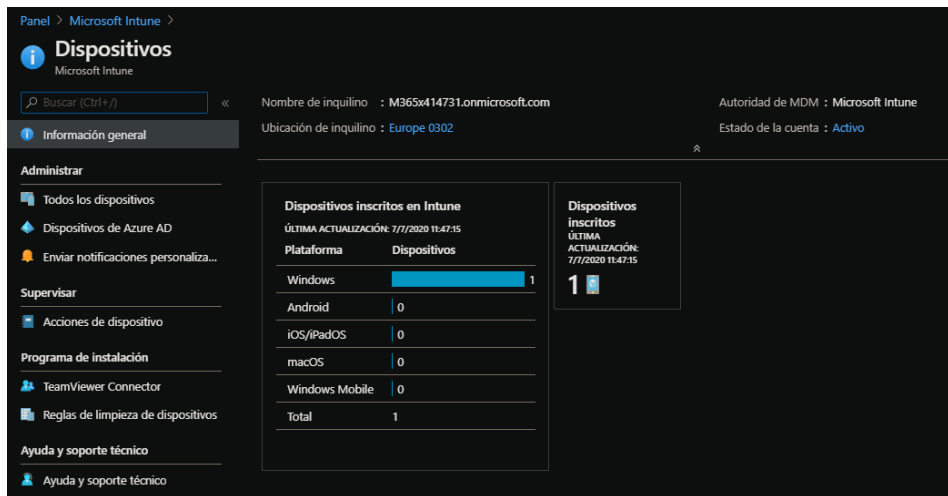
10. Clic en el botón de la parte superior de la ventana: **Guardar**, para confirmar los cambios que acabamos de realizar.



11. Aparecerá una **ventana informativa** en nuestro portal de Azure.



12. Ya nos **aparecerá el dispositivo como inscrito** en la **ventana informativa principal** del **servicio de EMS**.



El cambio de la propiedad del dispositivo puede tardar unos minutos en aparecer, ya que el Portal de empresa instalado en ese dispositivo tiene que sincronizar los cambios y esto puede demorarse en el tiempo