

Contenido

Laboratorio: Personalizar las opciones dentro de nuestra tenant para Usuarios en nuestro AAD.	2
Laboratorio: Comprobar propagación de cambios en el “Centro de administración de Microsoft Endpoint Manager”	7
Laboratorio: Creación de usuarios Invitados en Microsoft Azure.	9

Laboratorio: Personalizar las opciones dentro de nuestra tenant para Usuarios en nuestro AAD.

Objetivo: Personalizar las **opciones** de nuestros usuarios en AAD.

Azure Active Directory nos permite **personalizar las opciones de los usuarios** de nuestra **organización** usando el Portal de Azure. **Gestionar las Apps Empresariales, restringir el acceso** al portal de administración, **conectar** con las **cuentas corporativas de LinkedIn** y **gestionar los Usuarios Externos** a la empresa.

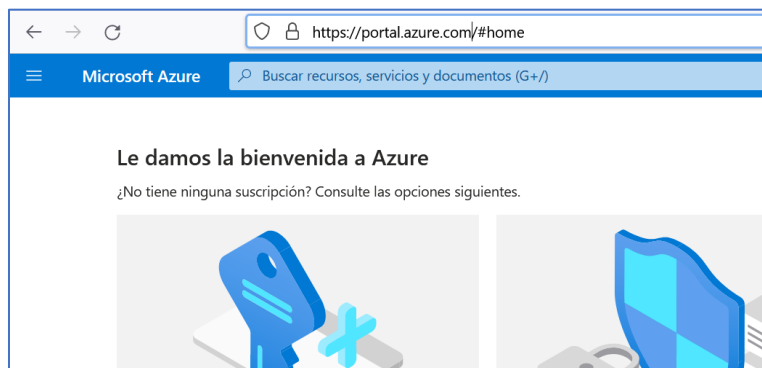
Prerrequisitos: Tener una tenant de Microsoft propia o de prueba con los planes o servicios correspondientes, Business Premium, Planes Empresa o Servicios “suelos” (*Exchange Online P1/P2, SharePoint Online P1/P2, Teams, etc*).

Pasos a realizar:

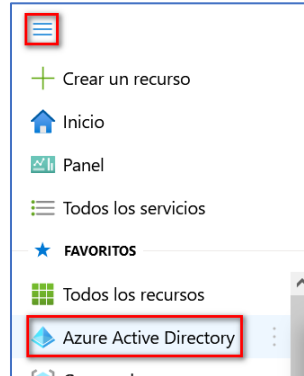
1. Logarnos al Portal Azure, en este enlace- <https://portal.azure.com/> con nuestras credenciales de admin
Usuario: EMS0x@m365*****.onmicrosoft.com (la “x” es el usuario que os hemos dado al comienzo del curso).
Contraseña: HolaMundo01 (o la contraseña que hayas puesto cuando el sistema te obligó a cambiarla)



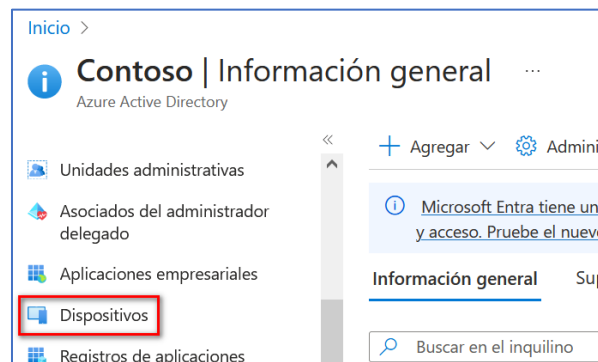
2. Aparecerá la **Dashboard de Microsoft Azure AD**.



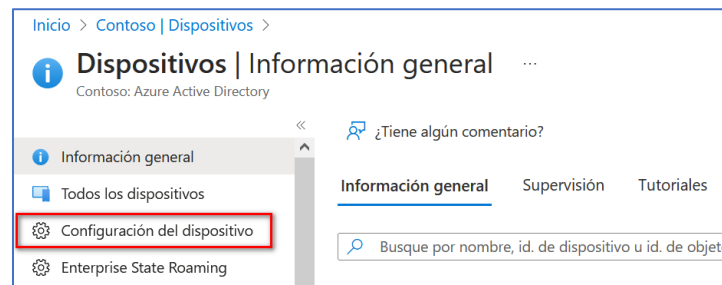
3. Clic en  Microsoft Azure en la **parte izquierda de la pantalla** para que se muestre el **menú del portal de Azure**. Clic en la *entrada: Azure Active Directory*



4. Dentro de la *sección Administrar*, clic en **Dispositivos**.



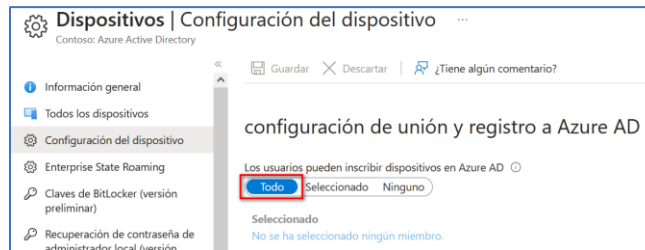
5. Clic en **Configuración de dispositivo**.



6. En la *sección: Los usuarios pueden inscribir dispositivos en Azure AD* podemos **seleccionar sí permitimos o no** que **todos los usuarios** o un **grupo de ellos**, puedan **inscribir sus dispositivos Windows 10** en *Azure Active Directory* (el resto de implementación, Windows Autopilot, Azure AD híbrido, etc funcionan en un contexto sin usuario).

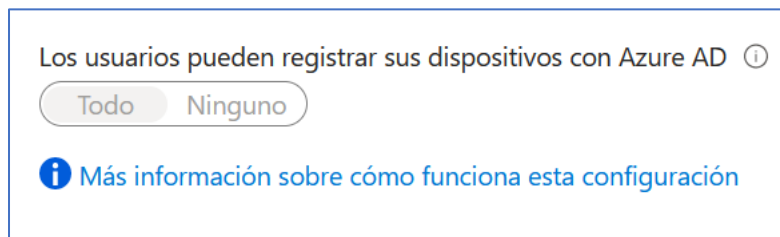
Tenemos **tres opciones**:

- **Todos.** Si *seleccionamos* esta **opción** que es la *predeterminada*, **todos los usuarios** podrán **inscribir sus dispositivos**.
- **Seleccionados.** **Seleccionaremos** a un **usuario** en particular o un **grupo de usuarios** que permitimos realizar esta acción. **Clic en Seleccionado**, aparecerá una nueva ventana para **Seleccionar miembros**, *marcando* la casilla correspondiente **al/os usuario/s** o **los grupos** que queramos y **clic en Seleccionar**.
- **Ninguno.** **NO permitimos** que **ningún usuario** **inscriba sus dispositivos** en Azure Active Directory. **Dejamos la opción que aparece por defecto: Todos.**



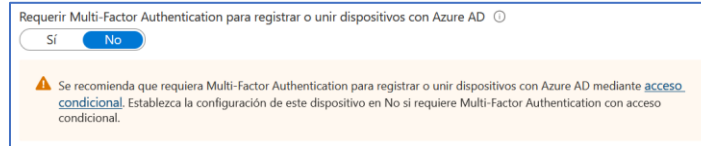
7. En la *sección: Los usuarios pueden registrar sus dispositivos en Azure AD*. Podemos elegir **sí permitimos a todos o a ningún usuario** **registrar** sus dispositivos **dentro del servicio de Intune**. **Va ligada al punto anterior**, aquí **nos permite seleccionar de forma granular** **quien** queremos que pueda **unir sus dispositivos** a *Azure Active Directory (Workplace Join)*. Si vamos a usar **Microsoft Endpoint Manager** para administrar **dispositivos móviles**, **ESTÁ opción sería OBLIGATORIA**.

NOTA: Si en el punto anterior de configuración (6 de este manual) seleccionamos que todos los usuarios pueden inscribir sus dispositivos este botón aparecerá deshabilitado.

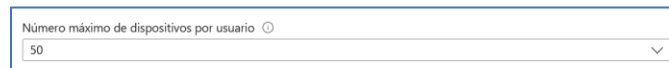


Más información: <https://learn.microsoft.com/es-es/azure/active-directory/devices/device-management-azure-portal#configure-device-settings>

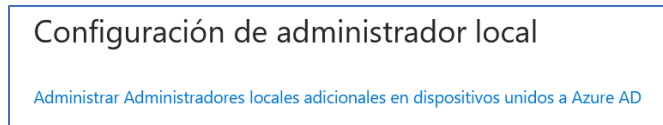
8. Podemos **requerir** o **no** que se solicite el **MFA** (*múltiple factor de autenticación*) en el *proceso de inscripción de los dispositivos* para poder *unir los dispositivos*. Cuando está establecido en "Sí", se **requerirá que el usuario use el MFA** cuando **inscriba un nuevo dispositivo** a Azure Active Directory.



9. También podemos **establecer un número máximo de dispositivos** que pueden unir cada usuario.

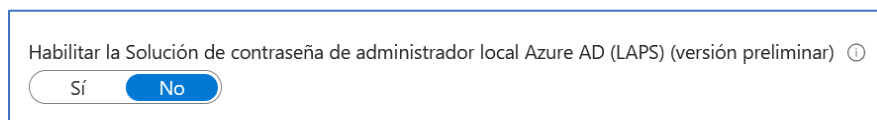


10. En la sección: **Administradores locales adicionales en dispositivos unidos a Azure AD**. Podemos seleccionar un **grupo de usuarios** de Azure Active Directory que se **promocionarán** dentro de *cada uno de estos equipos (con Windows 10/11) (a partir de la Windows 10, versión 20H2)* **añadiéndose** con el rol de **Administrador local** en cada uno de estos **PCs/portátiles**.



Más información: <https://docs.microsoft.com/es-es/azure/active-directory/devices/assign-local-admin>

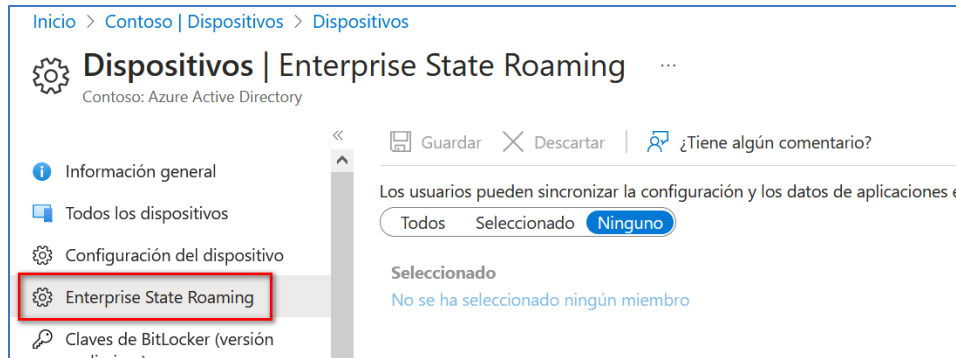
11. Podemos usar la capacidad de **gestión de contraseñas locales** de cada una de nuestras **PCs/portátiles** gracias a la compatibilidad de **Azure AD (LAPS)**.



Más información: <https://learn.microsoft.com/es-es/windows-server/identity/laps/laps-scenarios-azure-active-directory>

12. Podemos impedir que los usuarios puedan recuperar o no las claves BitLocker de sus dispositivos:



13. Clic en Enterprise State Roaming dentro de la sección Dispositivos.

Con esta *opción*, **entregaremos a nuestros usuarios una experiencia unificada de trabajo, tanto en Windows 10/11** (se sincronizará su configuración y los datos de las Apps, que serán guardados en la región de Azure correspondiente a la licencia de M365 que esté utilizando). **Enterprise State Roaming** (funciona de forma similar a la sincronización de configuración de consumidor de las versiones “home” de Windows 10/11):

Nota 1: Con Azure AD Premium, puede seleccionar un subconjunto de usuarios y habilitar esta característica para ellos. Sin Azure AD Premium, puede seguir usando esta característica, pero solo para todos los usuarios a la vez.
Más información: <https://docs.microsoft.com/es-es/azure/active-directory/devices/enterprise-state-roaming-enable>
Más información: <https://learn.microsoft.com/es-es/windows-server/identity/laps/laps-scenarios-azure-active-directory>

Laboratorio: Comprobar propagación de cambios en el “Centro de administración de Microsoft Endpoint Manager”

En este punto, podemos **comprobar** que todos los cambios que estamos realizando sobre el usuario de pruebas, se están *recogiendo* en el: “**Centro de administración de Microsoft Endpoint Manager**”, consola de administración con la que trabajaremos en laboratorios posteriores.

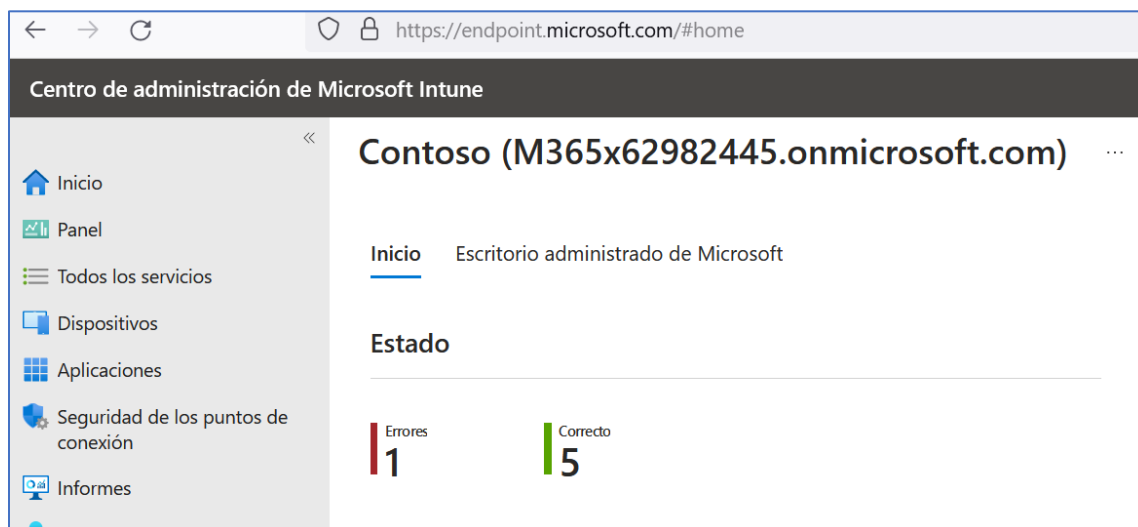
Prerrequisitos: Tener una tenant de Microsoft propia o de prueba con los planes o servicios correspondientes, Business Premium, Planes Empresa o Servicios “suelos” (*Exchange Online P1/P2, SharePoint Online P1/P2, Teams, etc*).

Pasos por realizar:

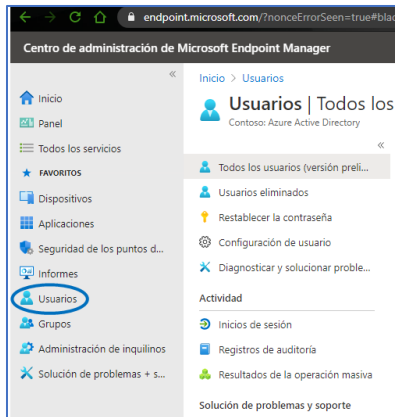
1. **Logarnos** en el Centro de administración de Microsoft Endpoint Manager, con nuestras credenciales de **admin**: <https://endpoint.microsoft.com/>.
Usuario: EMS0x@m365*****.onmicrosoft.com (la “x” es el usuario que os hemos dado al comienzo del curso).
Contraseña: HolaMundo01 (o la contraseña que hayas puesto cuando el sistema te obligó a cambiarla)



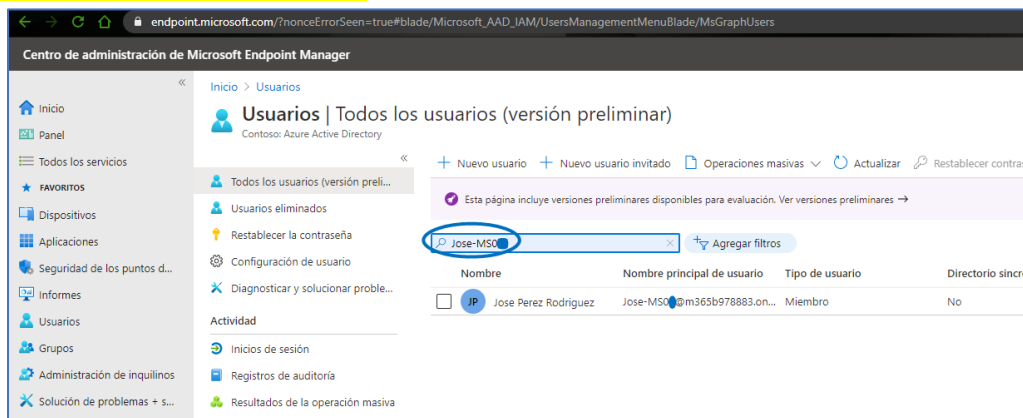
2. Aparecerá la **Dashboard** del **Centro de administración de Microsoft Endpoint Manager**.



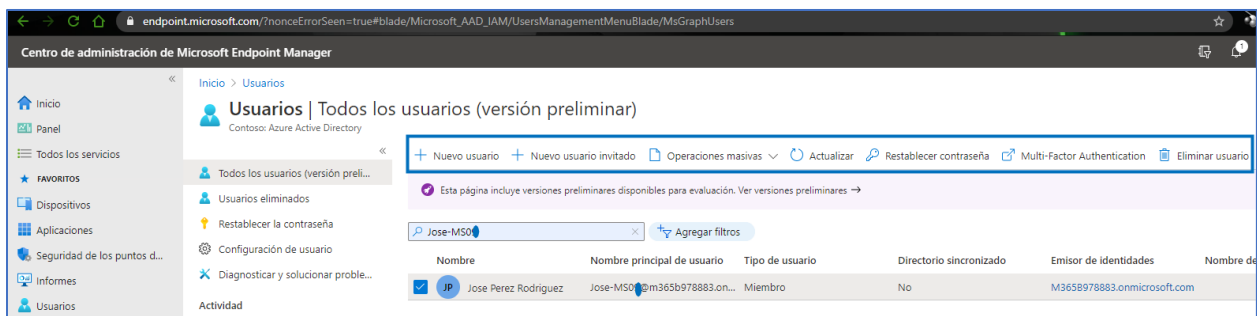
3. **Clic en la entrada del menú vertical izquierdo: Usuarios.**



4. **Buscamos escribiendo su nombre "jose-ms0x" en el campo de búsqueda (la lupa).** Para comprobar que el usuario Jose-EMS0x@m365xxxxxxx.onmicrosoft (la "x" corresponde al usuario que nos creamos en el laboratorio anterior y también a nuestro número de usuario administrador con el que hemos entrado en esta consola MS0x@....) existe.



5. Desde este *mismo portal*, podemos realizar las **tareas más cotidianas de gestión de usuarios** como podemos ver en el *menú vertical de izquierda* de la ventana de nuestro navegador. **La vista es exactamente la misma que en el portal de Azure.**



Laboratorio: Creación de usuarios Invitados en Microsoft Azure.

Objetivo: Creación de usuarios invitados por parte de admin de la tenant, para permitir a determinadas personas ajenas a nuestra empresa colaborar en tiempo real y tener acceso a determinados recursos creados en Azure Active Directory de nuestra organización.

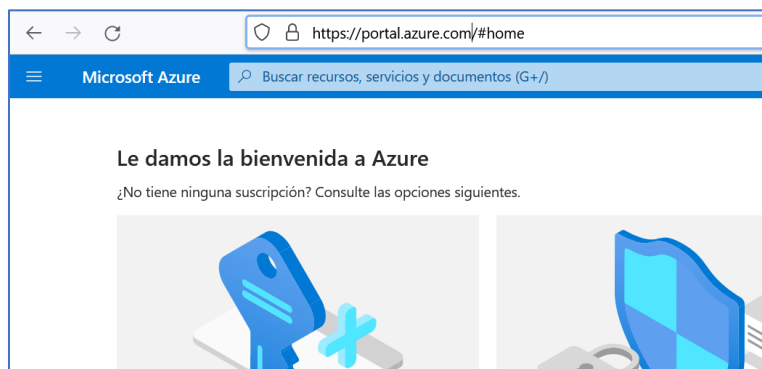
Prerrequisitos: Tener una tenant de Microsoft propia o de prueba con los planes o servicios correspondientes, Business Premium, Planes Empresa o Servicios “sueños” (Exchange Online P1/P2, SharePoint Online P1/P2, Teams, etc)..


Pasos a realizar:

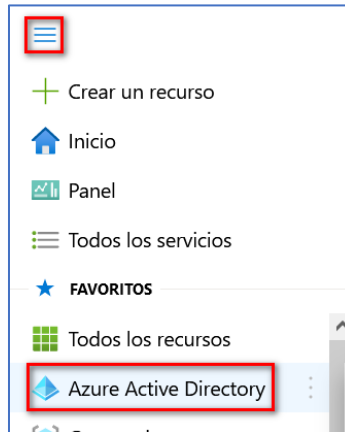
1. Logarnos al Portal Azure, en este enlace- <https://portal.azure.com/> (ya tenemos que estar logados).
Usuario: EMS0x@m365*****.onmicrosoft.com (la “x” es el usuario que os hemos dado al comienzo del curso).
Contraseña: HolaMundo01 (o la contraseña que hayas puesto cuando el sistema te obligó a cambiarla)



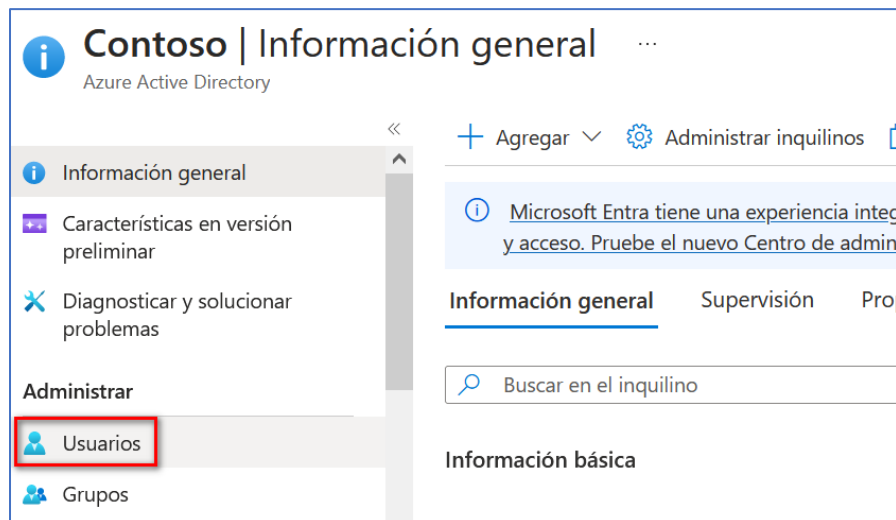
2. Aparecerá la **Dashboard de Microsoft Azure AD**.



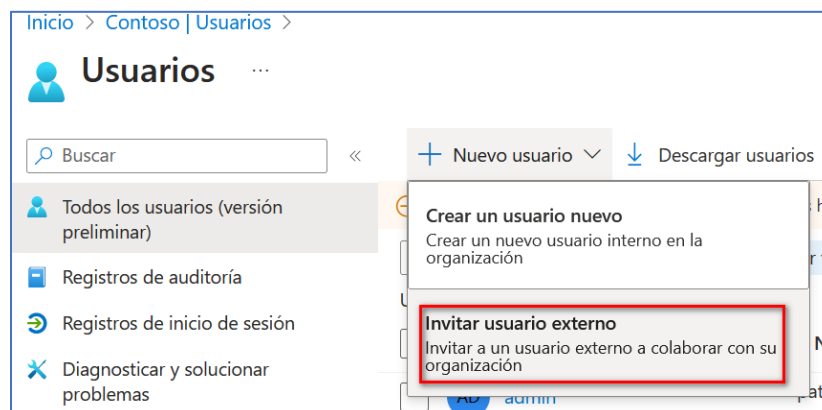
3. Clic en  Microsoft Azure en la **parte izquierda de la pantalla** para que se muestre el **menú del portal de Azure**



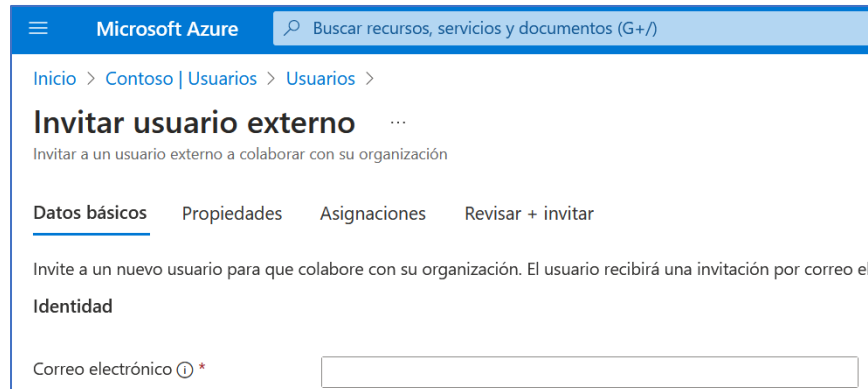
4. Clic en **Azure Active Directory**. Clic en la **sección Administrar** en la entrada **Usuarios**.



5. En la **sección: Todos los usuarios**. Clic en el **desplegable: Nuevo usuario**. Clic en **Invitar usuario externo**.



6. Se mostrará la *plantilla* de “**creación de usuarios invitados**”, con esta opción **ya seleccionada**.



Microsoft Azure

Buscar recursos, servicios y documentos (G+/)

Inicio > Contoso | Usuarios > Usuarios >

Invitar usuario externo

Invitar a un usuario externo a colaborar con su organización

Datos básicos | Propiedades | Asignaciones | Revisar + invitar

Invite a un nuevo usuario para que colabore con su organización. El usuario recibirá una invitación por correo electrónico.

Identidad

Correo electrónico ⓘ *

7. **PARTE OPCIONAL de este laboratorio**

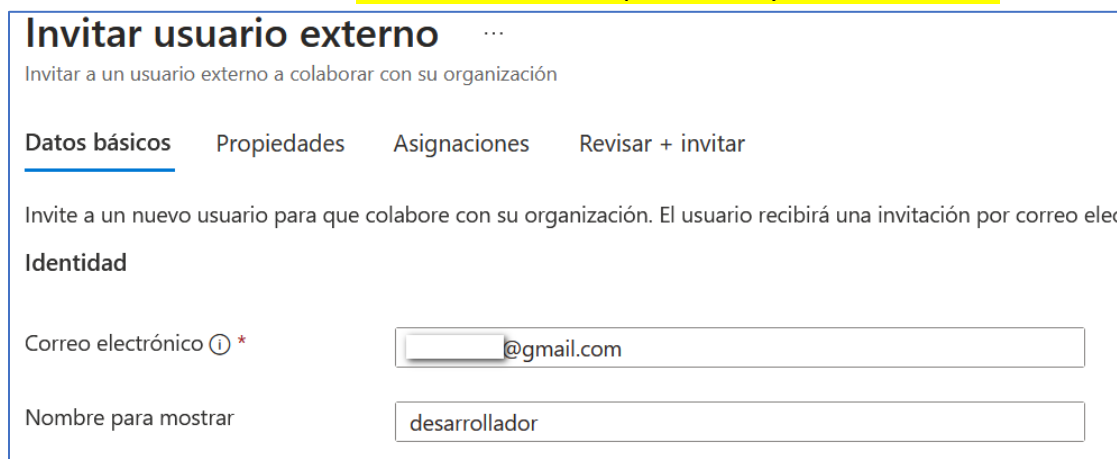
REQUERIRA QUE PONGÁIS UN EMAIL VUESTRO. *Sí queréis hacerlo. Por ese motivo es OPCIONAL.*

Crear un **usuario invitado** a nuestra tenant, **ficticio** con una cuenta nuestra de **Gmail, Outlook o la dirección de correo electrónico** que queramos (*la de nuestra empresa, por ejemplo*) **SIMULANDO** que corresponde a un **partner** que nos va a **desarrollar y publicar una App de fichaje** para la empresa de nuestro cliente:

Dentro de la *sección*: **Identidad**. **Rellenaremos** la **información** de este **usuario invitado**:

- Correo electrónico**: poner un **email** al que **TENGAÍS acceso VOSOTROS** para realizar la prueba. En el pantallazo aparece un **email inventado** (*podemos escribir CUALQUIER email nuestro de Outlook.com, Google.com, Yahoo.com, etc*).
- Nombre para mostrar**: **desarrollador**

En el **resto** de este **laboratorio**, **YO USARÉ mis datos personales y eMAIL de Gmail**. Poner el **vuestro**:



Invitar usuario externo

Invitar a un usuario externo a colaborar con su organización

Datos básicos | Propiedades | Asignaciones | Revisar + invitar

Invite a un nuevo usuario para que colabore con su organización. El usuario recibirá una invitación por correo electrónico.

Identidad

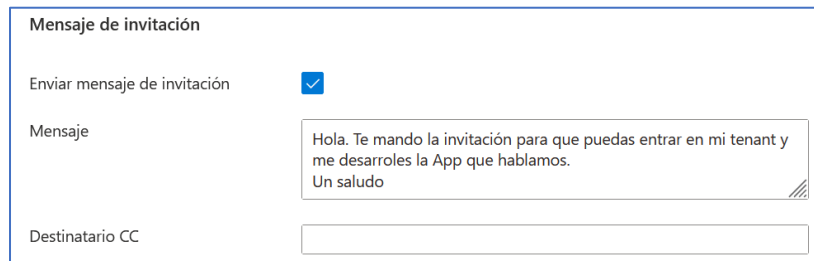
Correo electrónico ⓘ * @gmail.com

Nombre para mostrar desarrollador

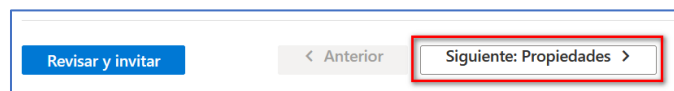
8. Dejar marca la casilla de selección: **Enviar Mensaje de Invitación.**

Podemos hacerle llegar un **texto personalizado** en el **correo de invitación** que la plataforma le hará llegar en el **campo Mensaje personal**. *(esto es opcional)*.

Y poner más destinatarios en copia el email de invitación:

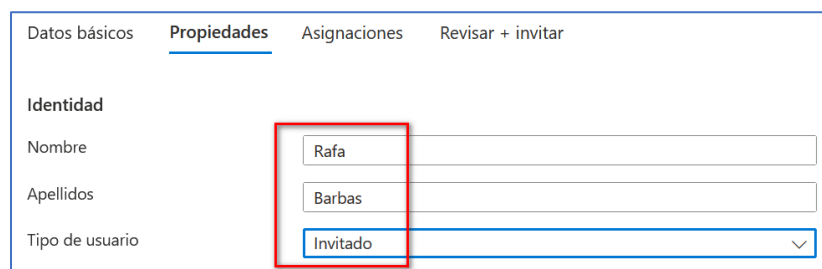


9. Clic en el botón: **Siguiente: Propiedades.**

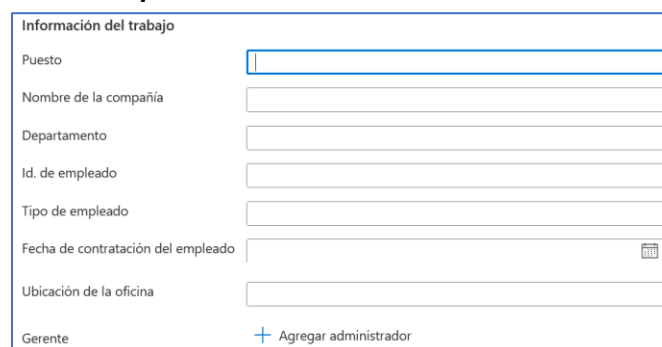


10. Dentro de la **Sección: Propiedades**: Podemos definir la información que precisemos de cada usuario invitado a nuestra tenant, basándonos en **4 campos diferenciados** la

- Campo Identidad.** Escribir el **nombre y apellido del usuario** y establecer el **tipo de usuario** como **Miembro** *(Invitado lo usaremos en otro lab)*. Escribir: **Vuestro Nombre / Apellido / Invitado**.



- Campo Información del trabajo.** Podemos agregar cualquier información relacionada con la relación contractual de este usuario invitado (como el puesto, departamento o manager). **Lo dejaremos en blanco para este laboratorio.**



- c. Campo: **Información del contacto**. Podemos agregar cualquier información de contacto. **Lo dejaremos en blanco para este laboratorio.**



Formulario de Información de contacto con los siguientes campos:

- Dirección
- Ciudad
- Estado o provincia
- Código postal
- País o región
- Teléfono de empresa
- Teléfono móvil
- Correo electrónico
- Otros correos electrónicos (+ Agregar dirección de correo)
- Número de fax

- d. Campo: **Control parental**. Para organizaciones escolares, de educación secundaria, etc, es posible que sea necesario proporcionar el grupo de edad del usuario:
- Los menores tienen 12 años
 - Los usuarios que no se consideran adultos tienen de 13 a 18 años
 - Adultos tienen 18 años o más.

La combinación del grupo de edad y el consentimiento que se proporcione en las opciones parentales determinan la clasificación del grupo de edad legal. La clasificación de grupos de edad legal puede limitar el acceso y la autoridad del usuario

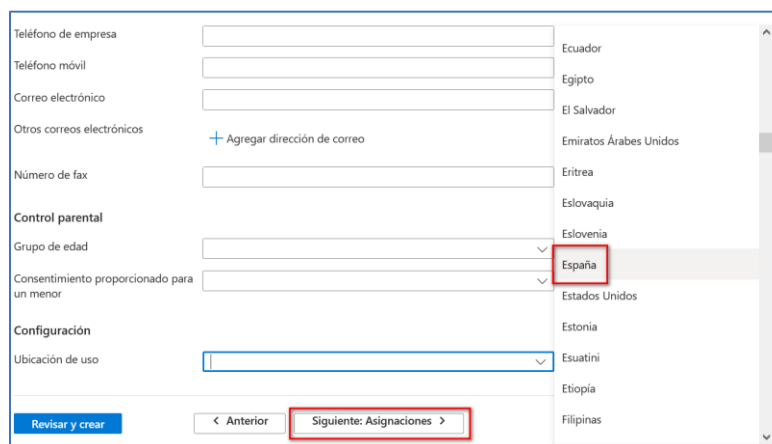
Lo dejaremos en blanco para este laboratorio.



Formulario de Control parental con los siguientes campos:

- Grupo de edad
- Consentimiento proporcionado para un menor

- e. Campo: **Configuración**. Seleccionar **España** en el desplegable (**escribir "esp" y nos aparecerá**)
Clic en botón: **Siguiente: Asignaciones**.



Formulario de Configuración con los siguientes campos:

- Teléfono de empresa
- Teléfono móvil
- Correo electrónico
- Otros correos electrónicos (+ Agregar dirección de correo)
- Número de fax
- Control parental
- Grupo de edad
- Consentimiento proporcionado para un menor
- Configuración
- Ubicación de uso

En el desplegable de Configuración, se muestra una lista de países. El país **España** está resaltado con un recuadro rojo.

En la parte inferior, se muestra un botón **Revisar y crear** y un botón **Siguiente: Asignaciones** con flechas de navegación.

Más información: <https://learn.microsoft.com/es-es/azure/active-directory/fundamentals/how-to-create-delete-users#invite-an-external-user>

11. Asignamos la pertenencia a grupos y a roles para este invitado:

Datos básicos
Propiedades
Asignaciones
Revisar + invitar

Cree hasta 20 asignaciones de grupos o roles. Solo puede agregar un usuario a un máximo de 1 unidad administrativa.

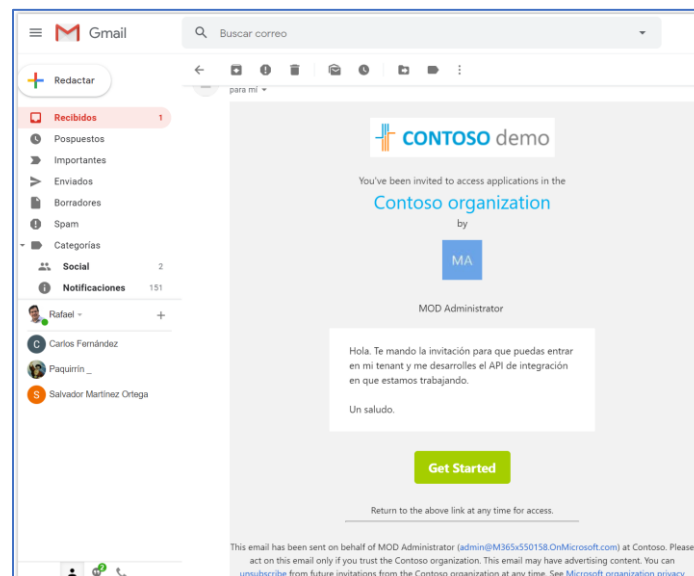
+ Agregar grupo
+ Agregar rol

No hay ninguna asignación para mostrar.

12. Clic en el botón: **Siguiente: Revisar + invitar >**.

Revisar y invitar
< Anterior
Siguiente: Revisar + invitar >

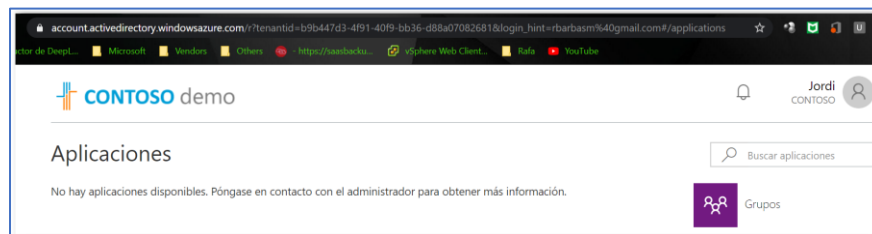
13. Si nos **logamos** en el **correo electrónico** del **usuario** al que acabamos de **invitar** (en vuestro caso el usuario vuestro de Gmail, Outlook, etc), habremos recibido el **email correspondiente** a la **invitación** y tendremos que aceptarla.



14. Este usuario invitado iniciará sesión con su cuenta de **Gmail**, en este ejemplo. **Nos pide autorización de permisos** para la cuenta.



15. Sólo tendrá acceso a lo que le hayamos permitido, en nuestro caso, **a nada** (ya que no le hemos asignado ningún tipo de licencia para que pueda acceder a alguno de los servicios de Microsoft 365):



16. En nuestro Azure Active Directory podremos **ver la actividad de este usuario invitado**, tanto en la entrada **Registros de inicio de sesión** como en **Registros de auditoría** de nuestro Azure Active Directory en la **sección Supervisión**.

