Contenido

Laboratorio: Habilitar Azure Multi-Factor Authentication (MFA) y comprobar su estado en nuestra tenant para Usuarios tanto dentro de nuestra empresa como usuarios externos.

Objetivo: *Habilitar* el **MFA** para un **nuestro grupo de usuarios seleccionado** de *nuestro Azure Active Directory*.

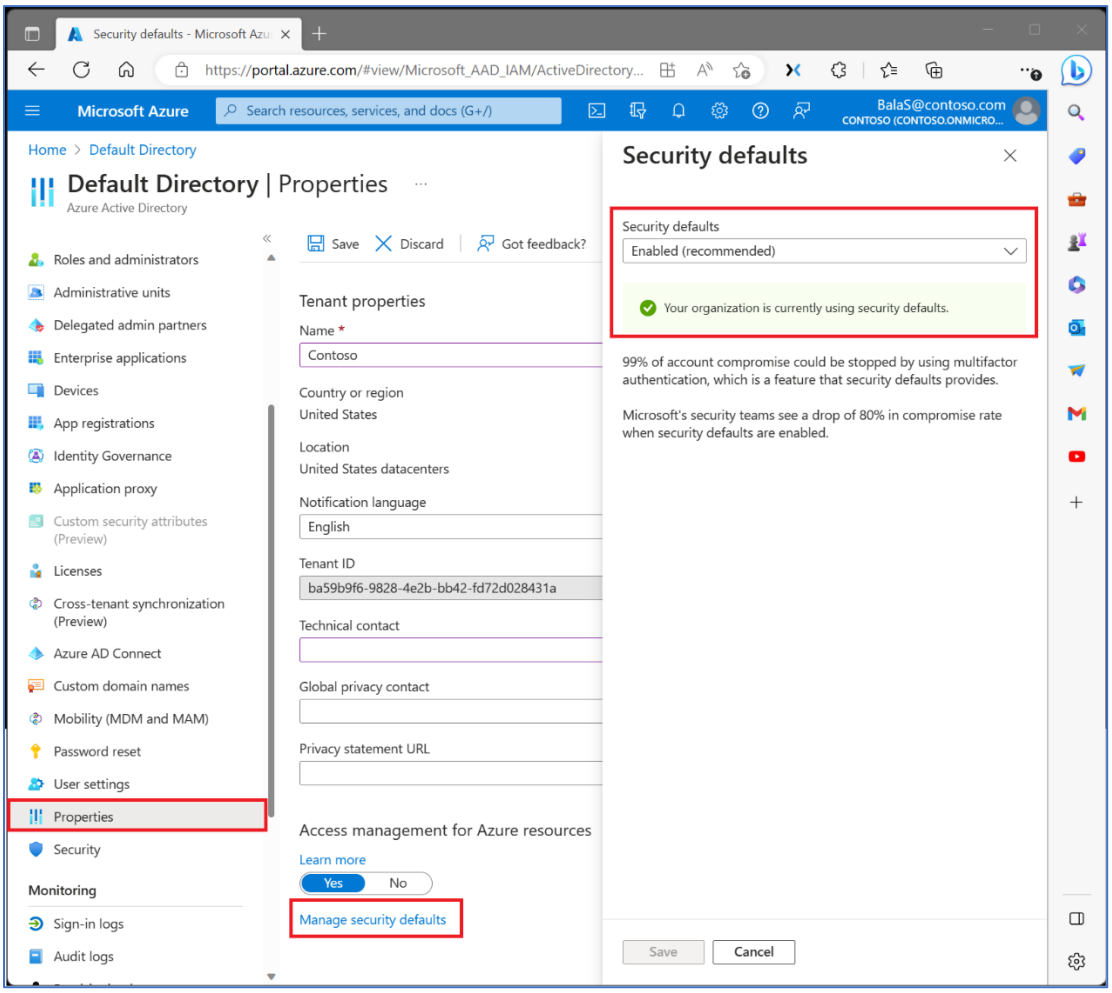
Habilitar el **MFA** en **Azure** nos **permite cambiar enfoque tradicional de seguridad** para **requerir** una **verificación basada en varios pasos**. **Funciona** tanto *Azure Active Directory* como para un servidor de *Azure MFA local*. Todos los **usuarios** con la funcionalidad de MFA habilitada tendrán la **misma experiencia**, que consiste en realizar una verificación de dos pasos cada vez que inician sesión. Al habilitar un usuario se anula cualquier política de acceso condicional que pueda afectar a ese usuario. En este laboratorio, vamos a **habilitar** la **Autenticación** de **Múltiples Factores** en Azure y comprobar cómo es desde el punto de vista del usuario. SÓLO habilitaremos el MFA para nuestro grupo.

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

Microsoft tiene, ahora mismo, 2 tipos de configuraciones de MFA en cada tenant, podemos acceder a ellas tanto desde el portal de Azure como el portal de Entra ID *(el año que viene solo se podrá hacer desde aquí)*:

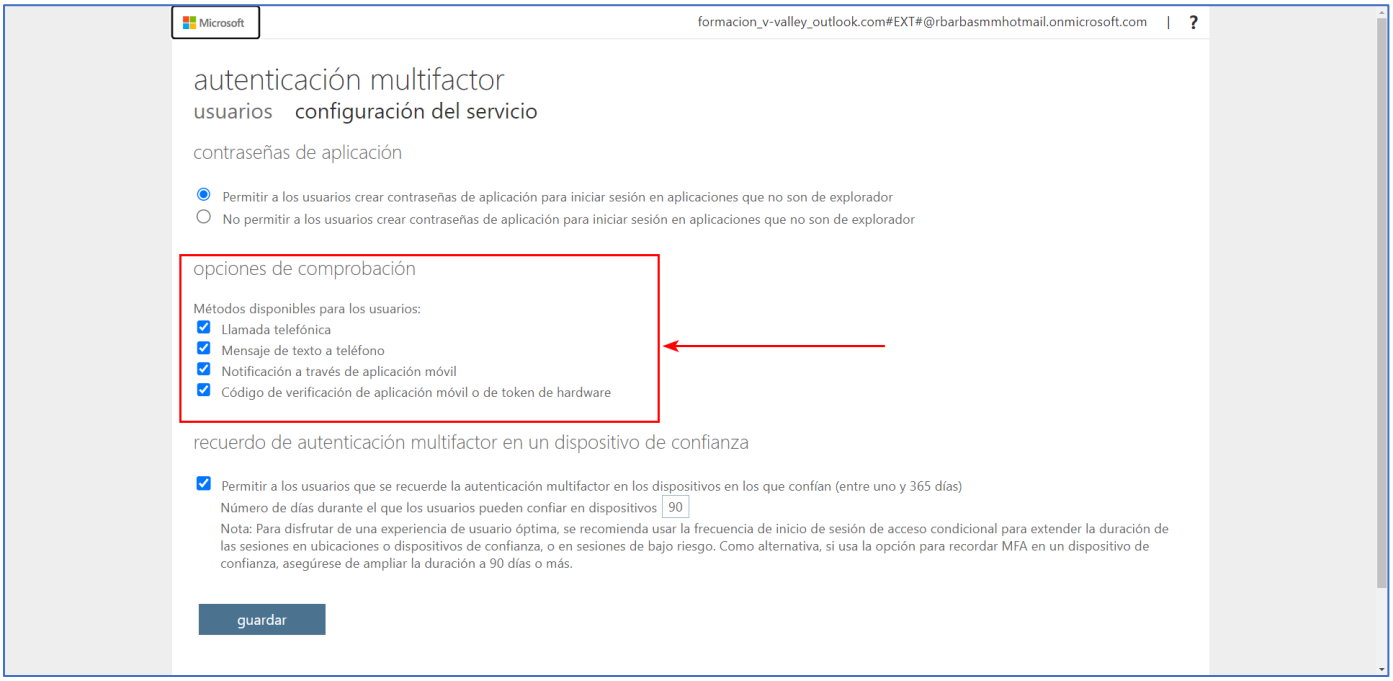
1. Es la configuración con los valores "**predeterminados de seguridad**" **por defecto** aplicada por Microsoft.
   Es la opción de **MFA para todos los usuarios de la tenant.**
   Esta opción se puede deshabilitar, sí se **deshabilita** NO le saltará el MFA a los usuarios al realizar el login con su cuenta de Microsoft 365 (*esto NO está RECOMENDADO por Microsoft sí no se habilita el MFA por usuario que es el siguiente punto*) siguiendo estos:

   - Inicie sesión en Azure Portal como administrador de seguridad, administrador de acceso condicional o administrador global.
   - Vaya a Azure **Active Directory** > **Propiedades**.
   - Seleccione **Administrar valores predeterminados de seguridad**.
   - Establezca "*Valores predeterminados de seguridad*" en Habilitado o Deshabilitado.
   - Seleccione **Guardar**.



Toda la información la pueden encontrar en esta URL: https://learn.microsoft.com/es-es/entra/fundamentals/security-defaults#disabling-security-defaults

2. **MFA por usuario**. Es la opción recomendada por Microsoft sí vamos a utilizar políticas de acceso condicional para entrar a los recursos de nuestra tenant. Al acceder nos da estas opciones



Microsoft **OBLIGA** para todos los usuarios que tengan un ROL dentro del IAM del portal de Azure a cualquiera de los niveles de:

- Tenant/s
- Suscripcion/es
- Grupo de Recursos
- Recurso individual.
- Apps o cualquier otro recurso desplegado dentro de la tenant y las suscripciones de Azure

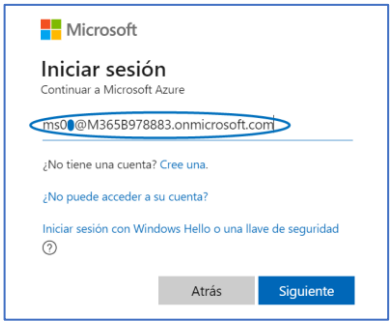
Para Apps, procesos y/o otros componentes desplegados en Azure, Microsoft RECOMIENDA implementar una "identidad administrada" que NO está sujeta a MFA.

Más información sobre "identidades administradas": https://learn.microsoft.com/es-es/entra/identity/managed-identities-azure-resources/overview

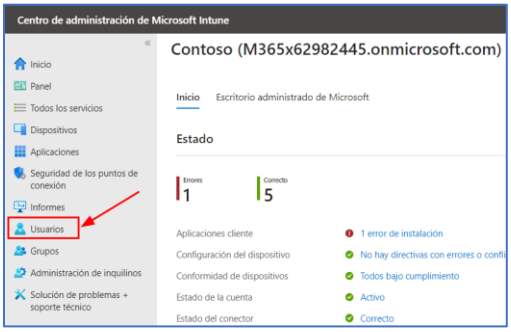
Como Asignar roles a una Identidad administrada: https://learn.microsoft.com/es-es/azure/role-based-access-control/role-assignments-portal-managed-identity

Pasos a realizar en la configuración de la SEGUNDA opción de MFA: "*MFA por usuario*":

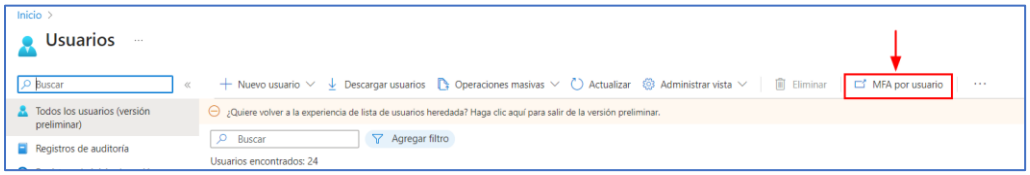
1. **DESDE** el *portal de administración* de **Microsoft Endpoint Manager** *(podríamos también hacerlo tanto desde el Centro de administración de Microsoft 365 como desde el portal de Azure)*, como **admin** de la tenant en este enlace: https://endpoint.microsoft.com/
   Usuario: EMS0x@m365********.onmicrosoft.com *(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)



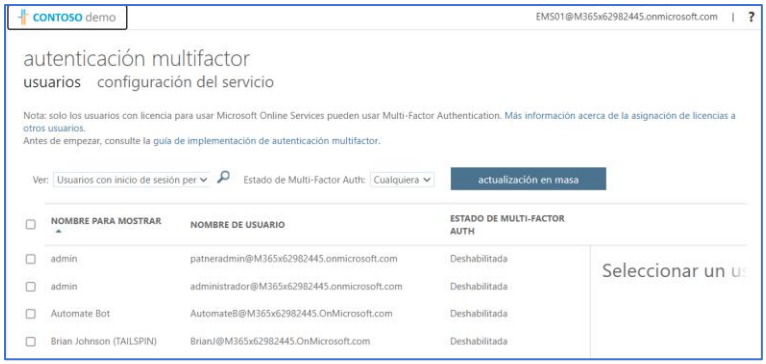
2. En la **Dashboard**. **Clic** en la **entrada** del menú vertical izquierdo: **Usuarios**.



3. **Clic** en el **botón MFA por usuario** en la barra horizontal.

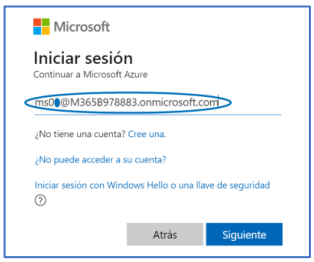


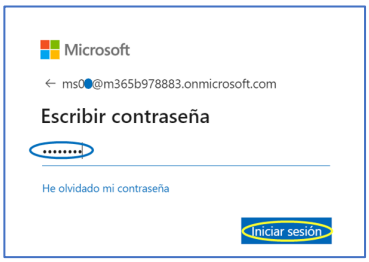
4. Se *abrirá* una *nueva pestaña/ventana* de nuestro navegador, donde tendremos que **volver a logarnos**.


CONTOSO demo
EMS01@M365x62982445.onmicrosoft.com
autenticación multifactor
usuarios
configuración del servicio
Nota: solo los usuarios con licencia para usar Microsoft Online Services pueden usar Multi-Factor Authentication. Más información acerca de la asignación de licencias a otros usuarios.
Antes de empezar, consulte la guía de implementación de autenticación multifactor.
Ver: Usuarios con inicio de sesión per
Estado de Multi-Factor Auth: Cualquiera
actualización en masa
NOMBRE PARA MOSTRAR
NOMBRE DE USUARIO
ESTADO DE MULTI-FACTOR AUTH
admin
patneradmin@M365x62982445.onmicrosoft.com
Deshabilitada
admin
administrador@M365x62982445.onmicrosoft.com
Deshabilitada
Automate Bot
AutomateB@M365x62982445.OnMicrosoft.com
Deshabilitada
Brian Johnson (TAILSPIN)
BrianJ@M365x62982445.OnMicrosoft.com
Deshabilitada
Seleccionar un u

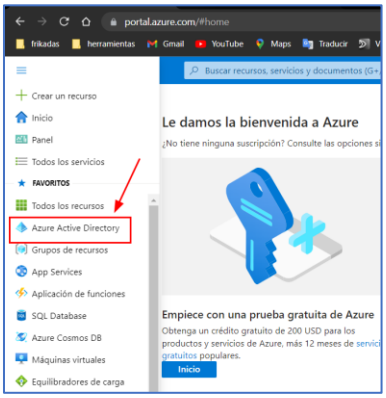
A este mismo portal de administración de MFA podemos acceder desde los otros portales de administración *(tanto el de Microsoft 365 como el de Azure)*

1. Sí nos **Logamos** en el **Portal Azure**, credenciales de admin: https://portal.azure.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)

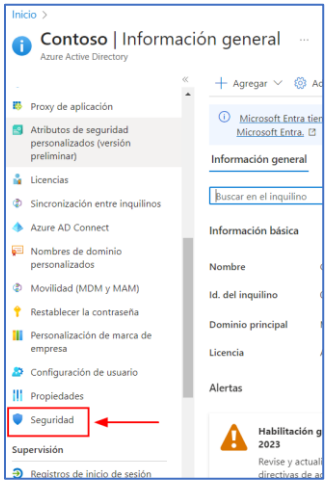




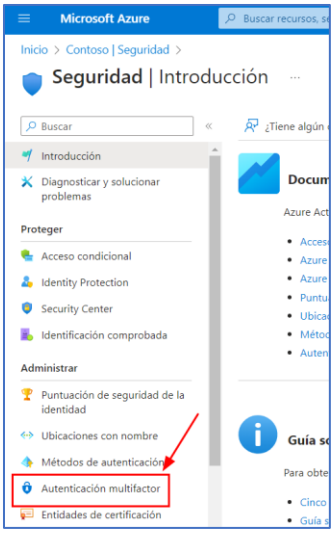
2. **Clic** en **Azure Active Directory**.



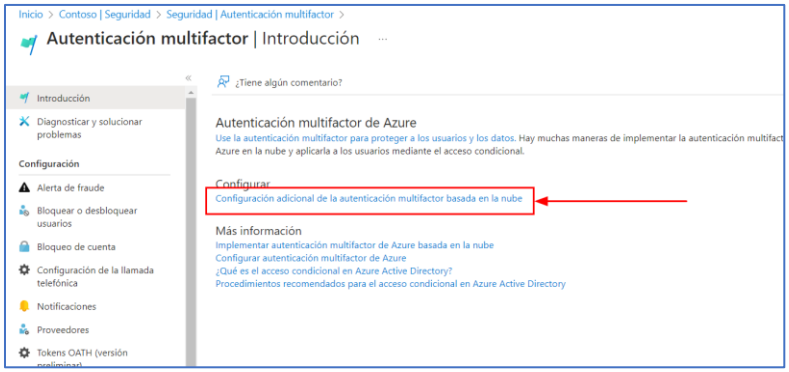
3. **Clic** en el **menú de la izquierda** en la **opción**: **Seguridad**, dentro de la *sección*: *Administrar*.



4. **Clic** en el **menú de la izquierda** en el **enlace**: **Autenticación multifactor**.

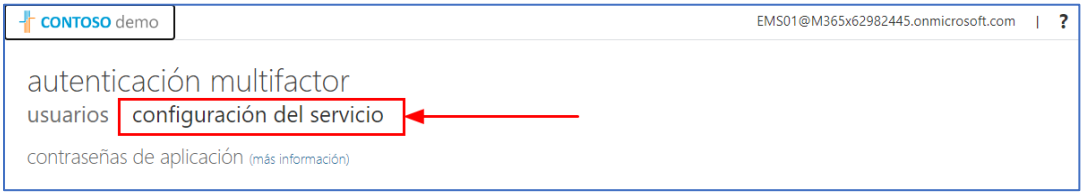


5. **Clic** en la *sección*: **Configurar > Configuración adicional de MFA basado en la nube**.



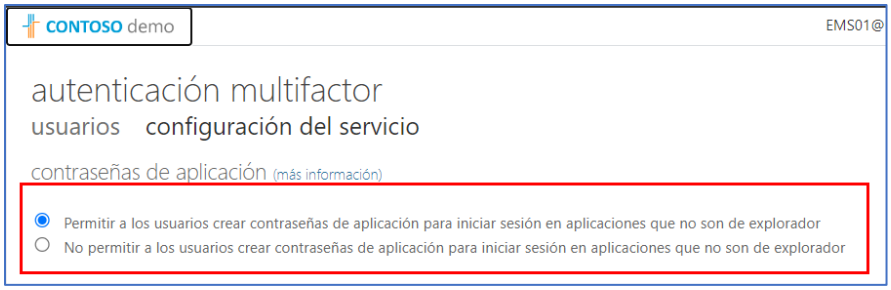
6. **Tanto sí hemos seguido un path o el otro para llegar…**
   Nos **aparecerá** una **nueva pestaña** o **ventana** de **nuestro navegador dónde** podremos configurar el **factor de múltiple autenticación (MFA).**

7. La **ventana de configuración** de **MFA** *está dividida en 2 pestañas*: **usuarios** y **configuración del servicio**.
   a. Comenzamos por la **Pestaña: Configuración del servicio. Clic** en **ella**, para **poder configurar** las **opciones** que **permitimos usar** a nuestros usuarios en el **proceso de logardo** basado en **MFA** *(esta configuración la tiene que realizar un usuario con rol **administrador global** de la **tenant)***:

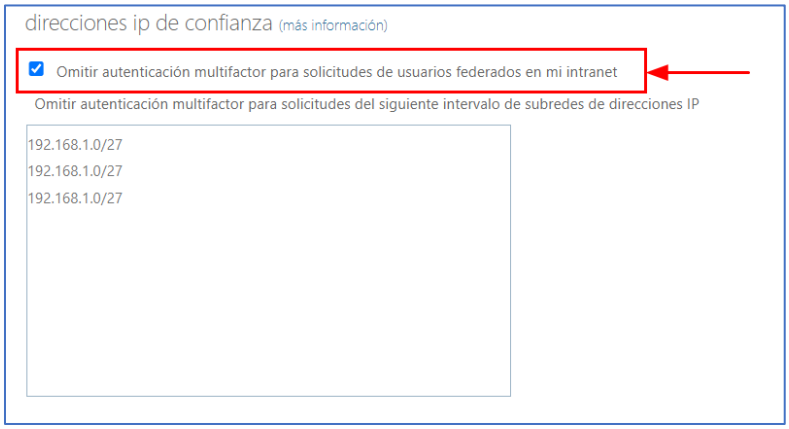


Esperar un momento a que **carguen** las **opciones** de **configuración**.
En esta **pestaña** podremos **configurar**:

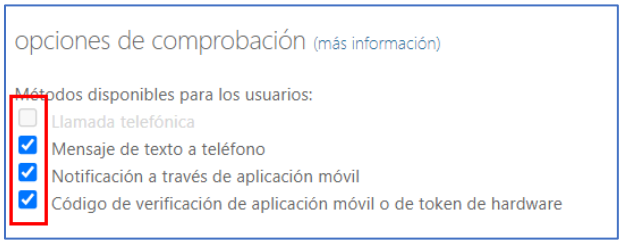
- **Sí permitimos** a los **usuarios crearse contraseñas** para **Apps** que **NO** sean un **navegador** o **no**. Por ejemplo, usaremos esta contraseña en la configuración de un cliente de correo en una tableta/móvil o para una App propietaria de otro fabricante *(una impresora multifunción que envía emails)*.



- **IPs confiables**: **NO pediremos el doble factor de Autenticación** a los **usuarios** que estén **dentro de nuestras oficinas** o **conectados por VPN**, definiendo uno o varios **rangos de dirección IPs**: **192.168.1.0/27**.

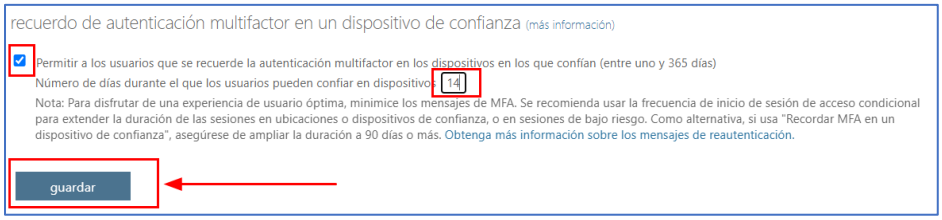


- **Definimos** los **métodos** de **comprobación** que **facilitaremos** a **nuestros usuarios**:
  - Llamada telefónica *(no disponible en nuestra tenant)*.
  - Mensaje de texto a teléfono.
  - Notificación a través de aplicación móvil.
  - Código de verificación de aplicación móvil o de token hardware.

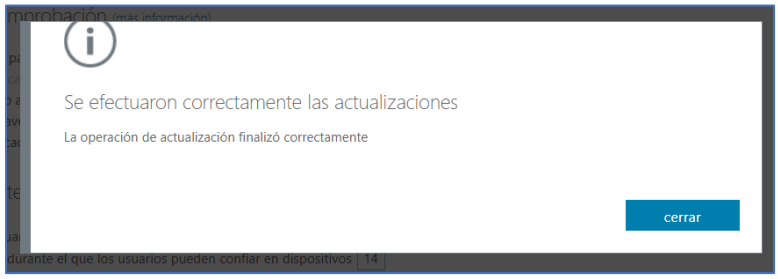


- **Qué número de días permitimos** que en los **dispositivos** ya usados por nuestros **usuarios no les vuelvan a pedir login**: **14 días** (*en este ejemplo, por defecto 90 días. El rango es entre 1 a 365 días máximo*).

  Clic en el **botón save** para salvar los cambios:

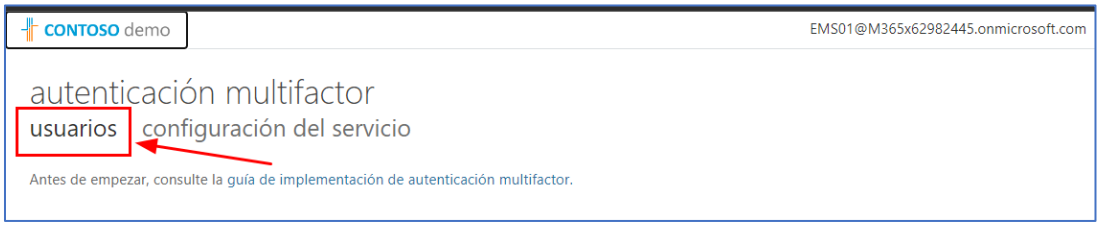


- **Nos aparecerá** la **ventana** de **confirmación** de los **cambios** que acabamos de realizar:

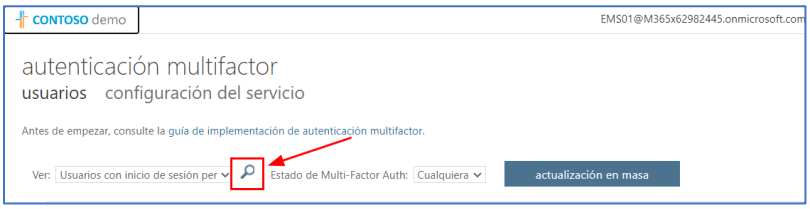


b. **PESTAÑA Usuarios.**

Clic en la pestaña **Usuarios** de la ventana principal de la **página de multi-factor Authentication.**

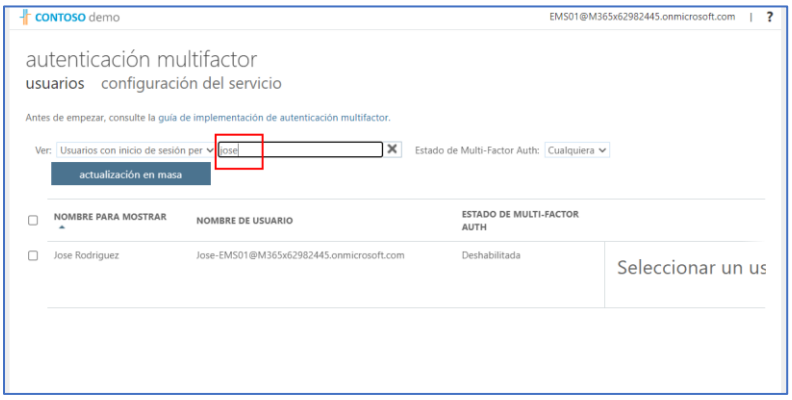


- **Podremos seleccionar** o **buscar**, en nuestro caso lo haremos así, **el/los usuario/s** a los que queremos **habilitarles** el uso del **MFA** en sus **procesos de login** *(Microsoft **RECOMIENDA** que por lo menos, TODOS los usuarios con el rol de administrador globales de las tenants tengan habilitado MFA)*.
  Clic en el **botón**: **lupa** para que aparezca el cuadro de texto para poder **escribir** el **nombre del usuario** *que nos creamos en laboratorios anteriores:* jose-EMS0x@m365********.onmicrosoft.com *(la "**x**" es el usuario que los instructores os daremos al comienzo del curso)*



¡¡¡ **CUIDADO EN ESTE PUNTO**!!!
¡¡¡ SÓLO SELECCIONAR NUESTROS USUARIOS sí estamos dispuesto a dar nuestro número de móvil para poder hacer el login una vez le hayamos habilitado el MFA !!! ¡¡¡ EN NINGÚN CASO SELECCIONAR todos los usuarios !!!. ¡¡¡ Por favor, Mucho cuidado en este punto, ya que tod@s estamos trabajando sobre la MISMA Tenant !!!.
¡¡¡ **CUIDADO EN ESTE PUNTO**!!!

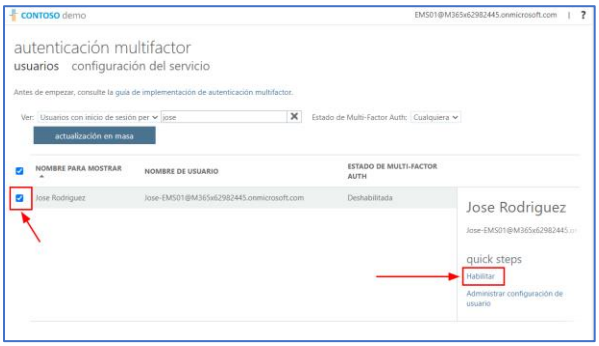
c. **Nos aparecerá todos los usuarios** "*jose*" que *hemos creado cada uno de los asistentes a esta formación en el laboratorio anterior*.
Elegir el "**VUESTRO**": "***Jose-EMS0x@m365xxxxxxx.onmicrosoft.com***" (La " x" corresponde al número del usuario admin que os dimos al comienzo del curso).

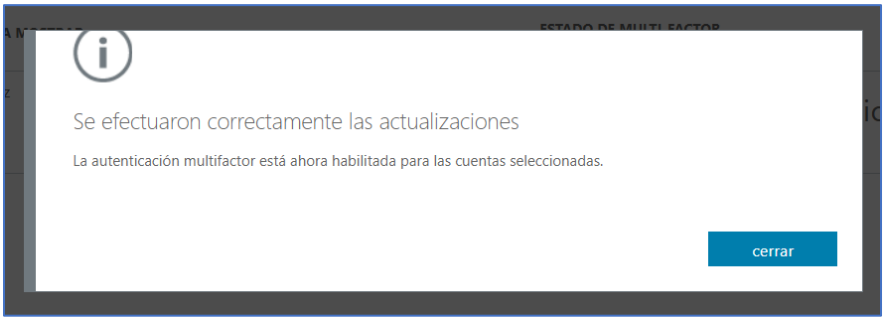


d. **Clic** en las **cajas de selección de la izquierda** de la **página** para **seleccionar el o los usuarios** que **queramos**, nos **aparecerán** sus **propiedades.**

e. ¡¡¡ CUIDADO!!!, Por favor, PARAR AQUÍ… **NO HACER Clic** en **Habilitar** en el **lado derecho** de la **ventana**, en el **enlace: Habilitar**

f. **Sí hacemos clic** tendremos **QUE SER CONSCIENTES** de que sí **no queremos perder** el **login** de este usuario **DEBEREMOS:**
   - **Proporcionar** un **móvil al cual debemos tener acceso**, SI NO PERDEREMOS EL LOGIN de este usuario**.**
   - **Un método** de **acceso la próxima vez** que nos loguemos en la tenant, **por lo que sí no estamos dispuesto. AQUÍ NOS PARARIAMOS.**





Laboratorio: Login del usuario: jose-EMS0X@... al que acabamos de habilitar su MFA.

PARTE OPCIONAL de este laboratorio.
REQUERIRA QUE PONGÁIS VUESTO MÓVIL, sí queréis hacerlo. Por ese motivo es OPCIONAL.

Objetivo: Comprender las implicaciones que conlleva habilitar el MFA en nuestros usuarios y tener una guía que podremos entregar, sí lo consideramos oportuno, a los usuarios de nuestros clientes para que la sigan.

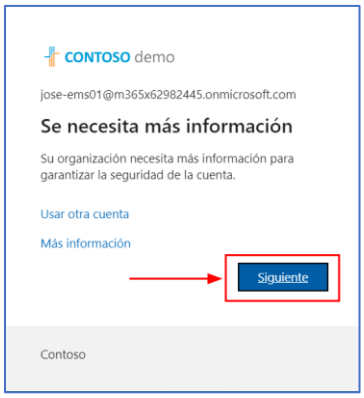
Una vez que como administradores que hemos habilitado el MFA para que **uno único o varios usuario/s**, pueda/n usar el **MFA**, **será el propio usuario** el que **tendrá** que **seleccionar** el **método** que **quiere usar en su múltiple factor de autenticación en los servicios Cloud** *(Office 365, etc)*.

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

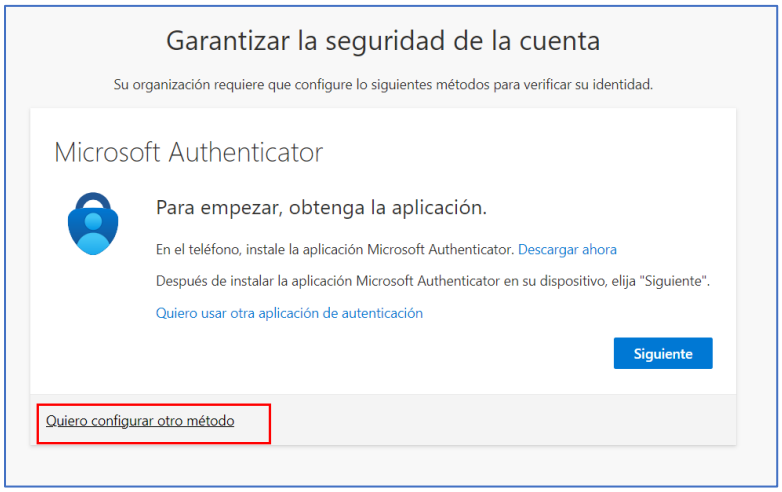
Pasos a realizar:

1. **Login** con el **usuario** al que le **hemos habilitado el MFA** en este enlace: https://outlook.office.com con su usuario y contraseña *(Jose, Rafa, etc)* para acceder vía **OWA** a su **Outlook**:
   Usuario: Jose-EMS0x@m365********.onmicrosoft.com *(la "x" es el usuario que los instructores os daremos al comienzo del curso)*
   Contraseña: Microsoft01 o la que le dimos en el laboratorio anterior.

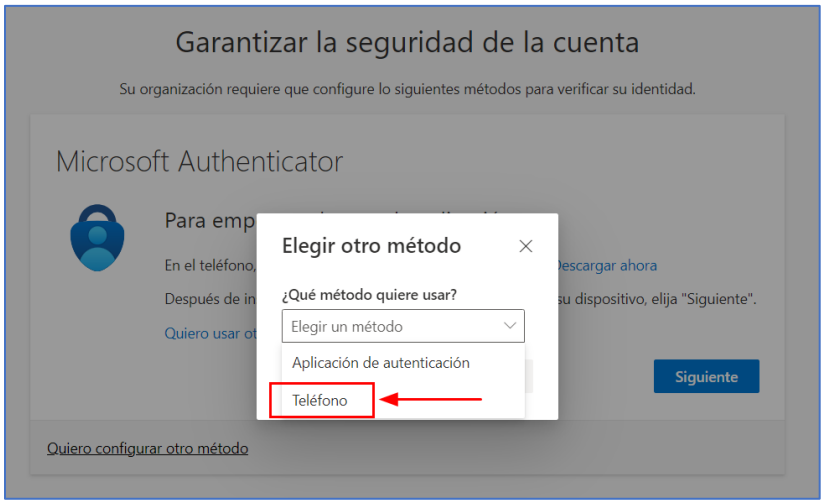
2. **Al haberle habilitado el MFA** a este **usuario**, **Microsoft** nos informará de que **necesita más información** para que podamos hacer **login** en nuestros servicios Cloud. **Clic** en el **botón Siguiente**.



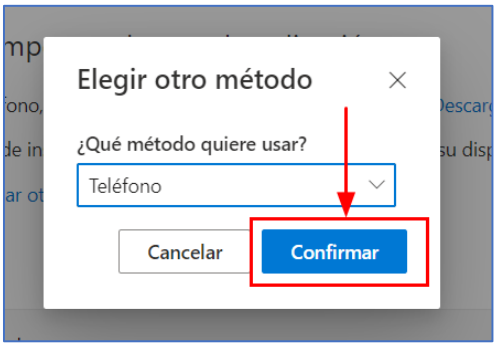
3. Nos aparecerá la ventana para "**Garantizar la seguridad de la cuenta**".
   Clic en el **enlace** de *parte inferior*: **Quiero configurar otro método**



4. En el *desplegable* **clic** en: **Teléfono**.

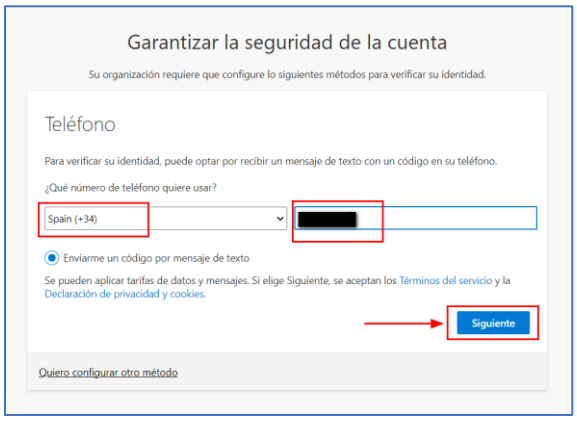


5. **Clic** en el *botón*: **Confirmar**.

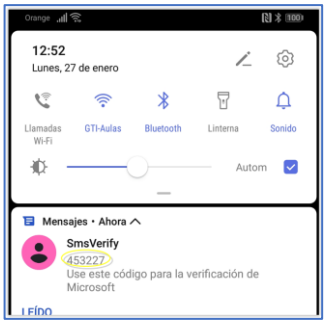


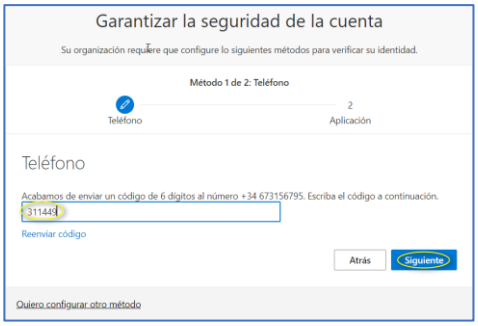
6. **Nos pedirá** la **información** correspondiente a nuestro teléfono (podemos poner el mismo número de móvil para todas nuestras cuentas Cloud de Microsoft):
   a. **País** del terminal. *Seleccionar*: **Spain**.
   b. **Número de móvil** al que se **enviará el código de acceso MFA**.

   Clic en el *botón*: **Siguiente**.

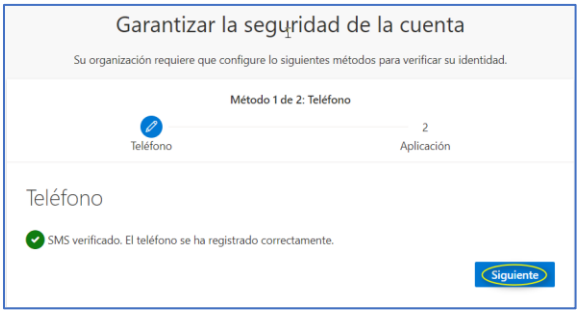


7. **Nos enviará a nuestro móvil** un **código de comprobación** que tendremos que **escribir en el campo de verificación correspondiente**:

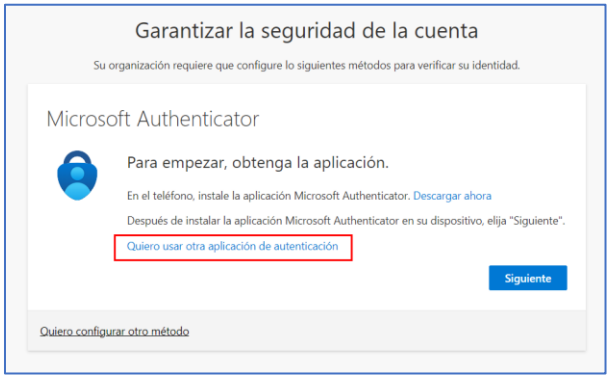




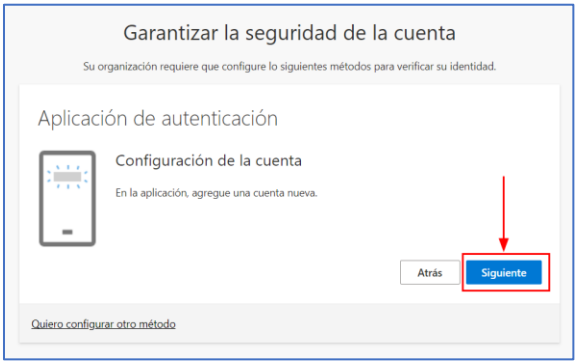
8. *Registraremos* el **teléfono** dentro del servicio.
   Clic en el *botón*: **Siguiente**.



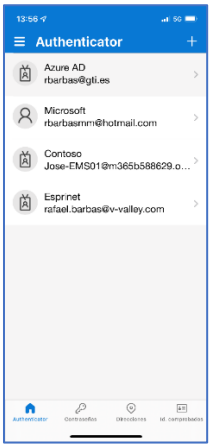
9. *Seleccionamos* **otro método de autenticación**. Podemos usar tanto la *App de autenticación que nos provee Microsoft:* **Microsoft Authenticator** en nuestros *móviles/tabletas*, como *otra App de autenticación de terceros (Google Authenticator, por ejemplo)*.
   Clic en el *botón*: **Siguiente** *(para usar **Microsoft Authenticator**)*.



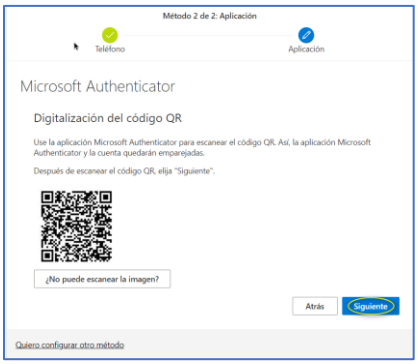
10. **Clic** en el *botón*: **Siguiente**.



11. **Escaneamos** el **código QR** en la App **Microsoft Authenticator** de nuestro móvil y lo validaremos *(podemos usar este procedimiento sí vamos a usar para una App de autenticación de terceros, Google Authenticator, etc)*.

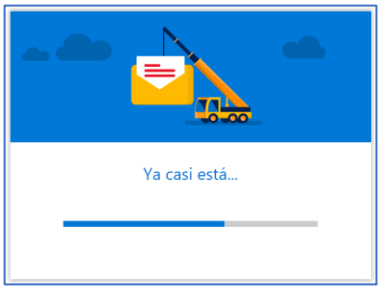


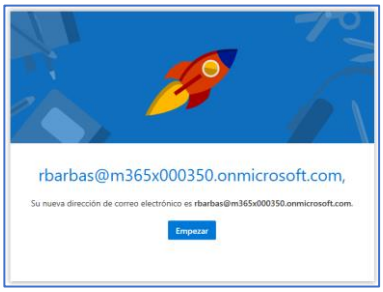
12. **Clic** en el *botón*: **Siguiente**.

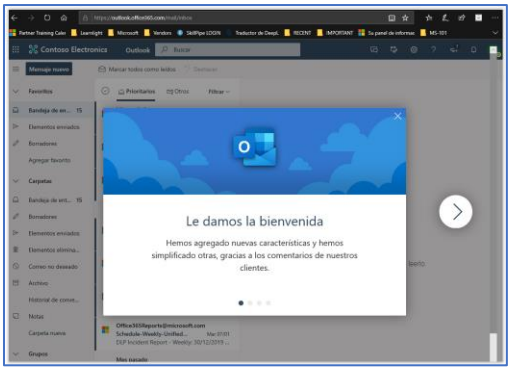


13. **Microsoft** nos facilitará un **código de App**, que podremos **usar como contraseña** para **logarnos** en las **Apps** que usemos para trabajar, **¡¡¡ COPIAR Y NO PERDER ESTE CÓDIGO !!!**:

14. **Podemos** dejar la **sesión cacheada** en este **dispositivo** y **accederemos** a nuestro correo electrónico corporativo a la App Cloud que de Microsoft a la que estemos accediendo **Sí es la primera vez** que **nos logamos aparecerán las ventanas de bienvenida:**






Contoso Electronics
Outlook
Le damos la bienvenida
Hemos agregado nuevas características y hemos simplificado otras, gracias a los comentarios de nuestros clientes.