TD SYNNEX

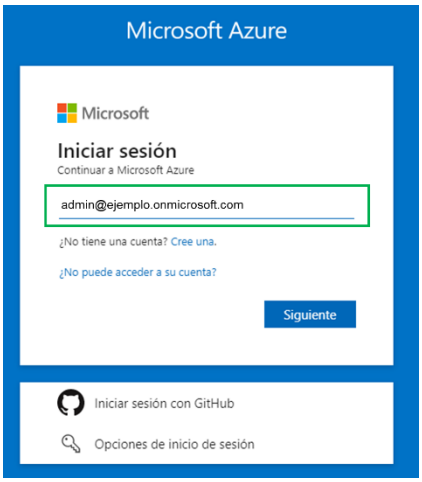
Guía Activación MFA

Paso a paso para la activación del Multi-factor de autenticación de tus usuarios desde Azure Active Directory

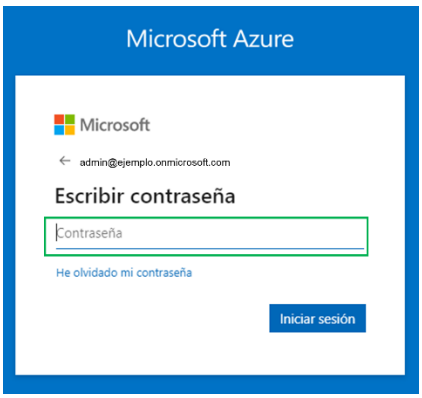
Activación de la política de MFA para tus usuarios

Paso 1: Ingresa al portal de azure: portal.azure.com

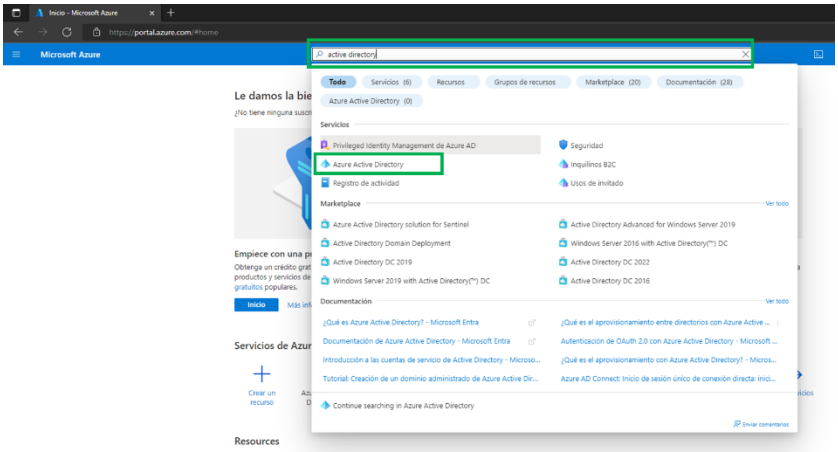
Paso 2: En la siguiente ventana coloca tu acceso de administrador global:



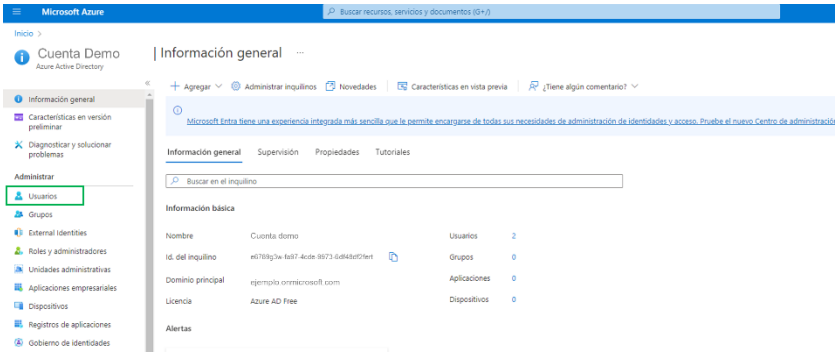
Paso 3: Escribe tu contraseña para iniciar sesión



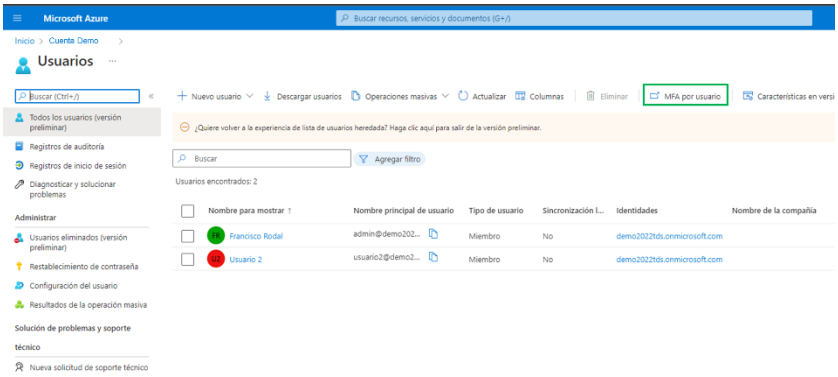
Paso 4: Dentro de Azure Portal, en la barra superior de búsqueda escribe **“Active Directory”** y posteriormente selecciona la opción **“Azure Active Directory”**



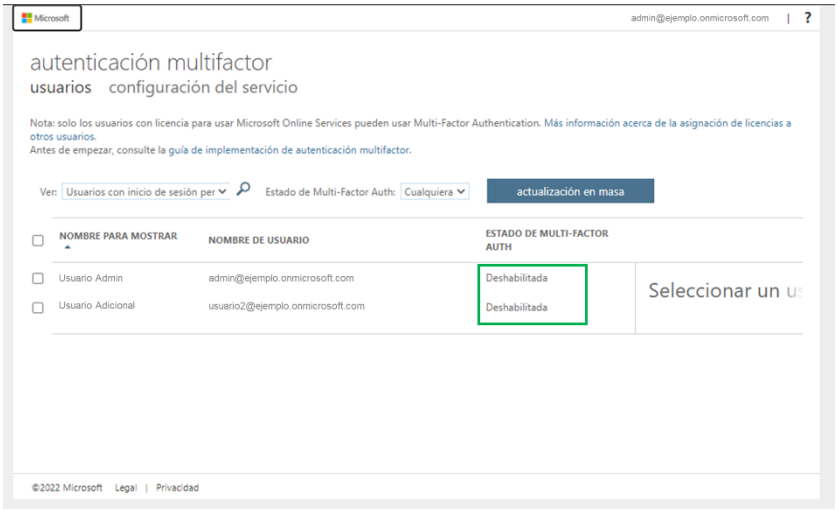
Paso 5: En la ventana que se abrirá, da click en **“Usuarios”** del menú de la izquierda



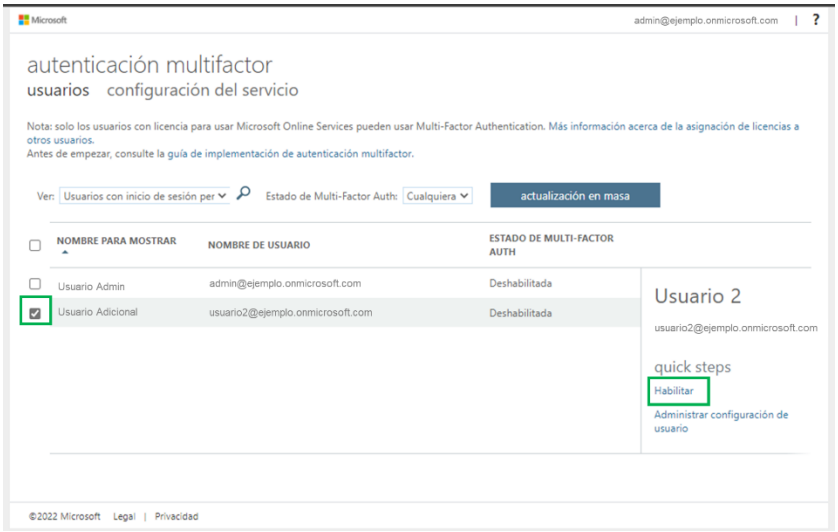
Paso 6: En la sección de Usuarios, deberás dar click en la opción **“MFA por usuario”**



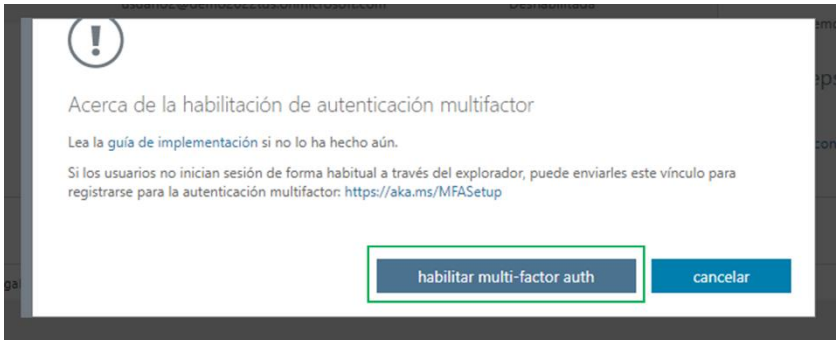
Paso 7: Se abrirá la siguiente ventana en la cual podrás validar si tus usuarios tienen habilitado o deshabilitado el MFA



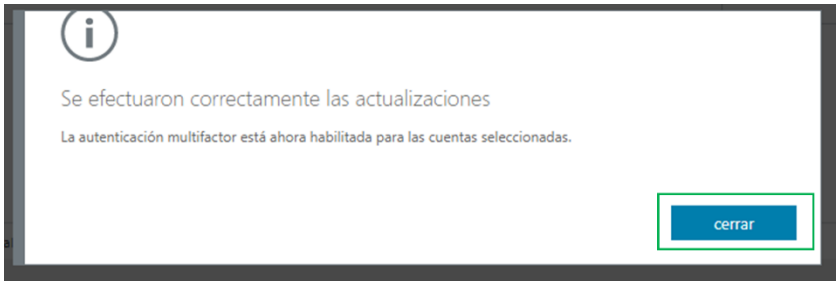
Paso 8: Para poder activar el MFA a tus usuarios, deberás activar la casilla de la izquierda de cada usuario para seleccionarlos y posteriormente en la sección **"Quick Steps"** del lado derecho deberás dar clic en **"Habilitar"**



Paso 9: Se abrirá una ventana para confirmar la activación de MFA, deberás dar clic en **"Habilitar multi-factor auth"**



Paso 10: Se desplegará un mensaje de confirmación de la activación de MFA

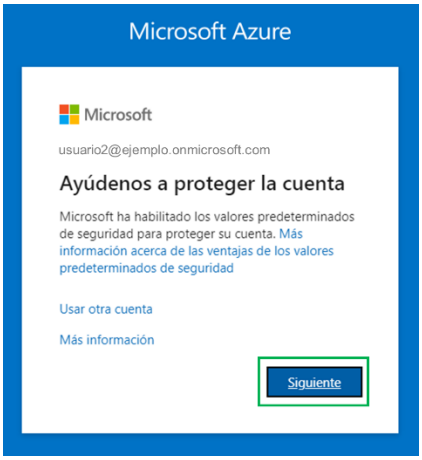


Paso 11: Recuerda cerrar tu sesión de administrador global en caso de que ya no la vayas a utilizar por el momento

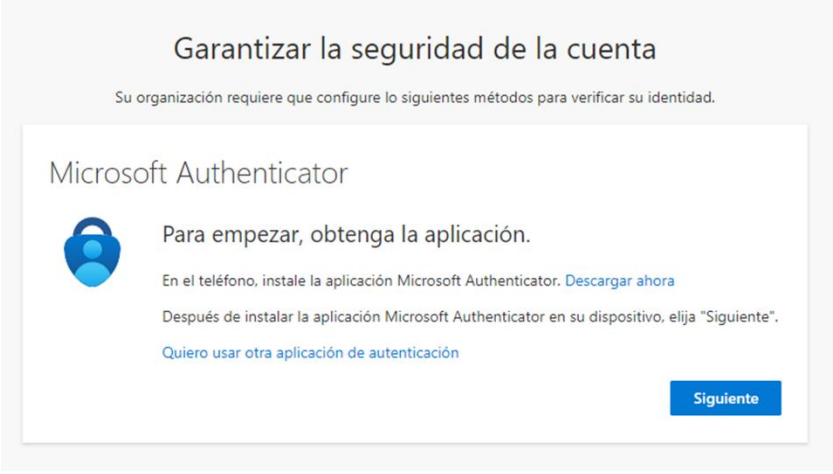
Configuración de MFA por parte del usuario

Paso 1: Iniciar sesión con tu usuario y contraseña

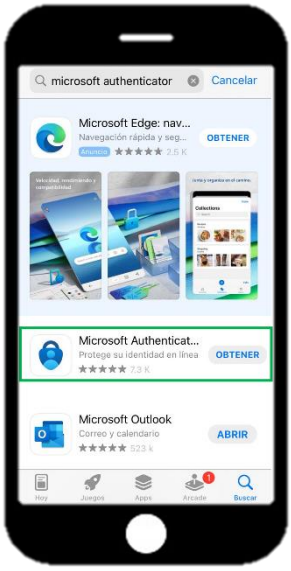
Paso 2: Te aparecerá la siguiente venta donde se te pedirá la configuración del MFA, para iniciar al configuración deberás dar clic en **“Siguiente”**



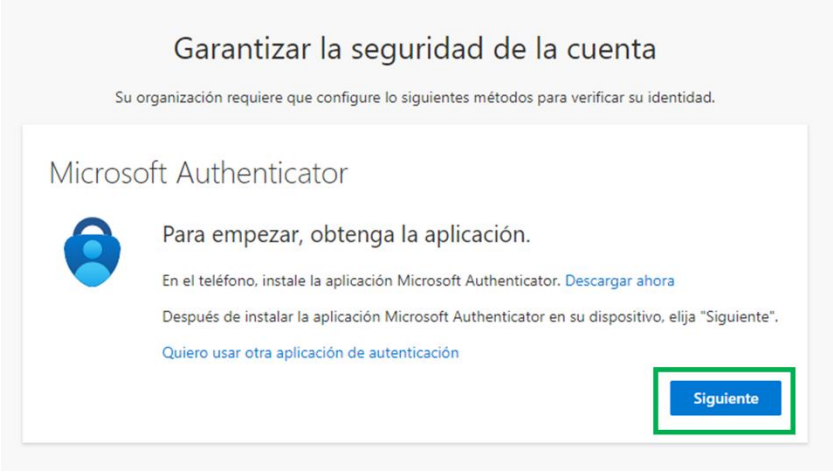
Paso 3: Verás la siguiente venta. En este punto haremo una pausa en tu computadora para que puedas instalar la aplicación Microsoft Authenticator en tu celular



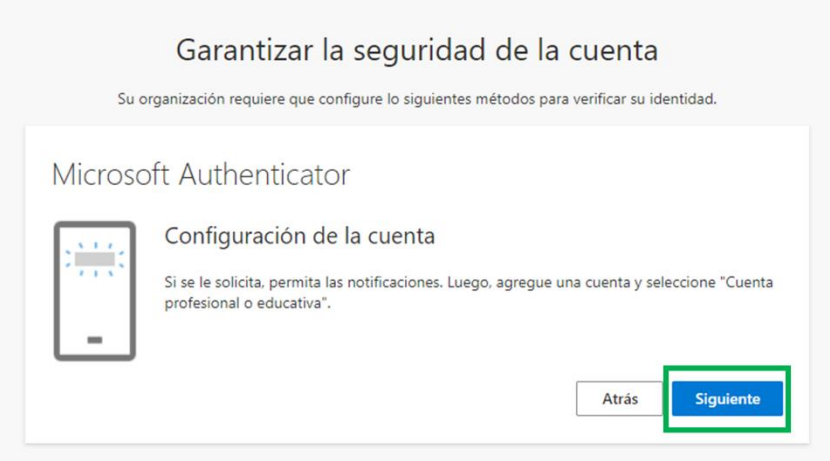
Paso 4: Entra a la tienda de aplicaciones de tu dispositivo móvil (App Store o Play Store), donde deberás buscar la aplicación **“Microsoft Authenticator”**



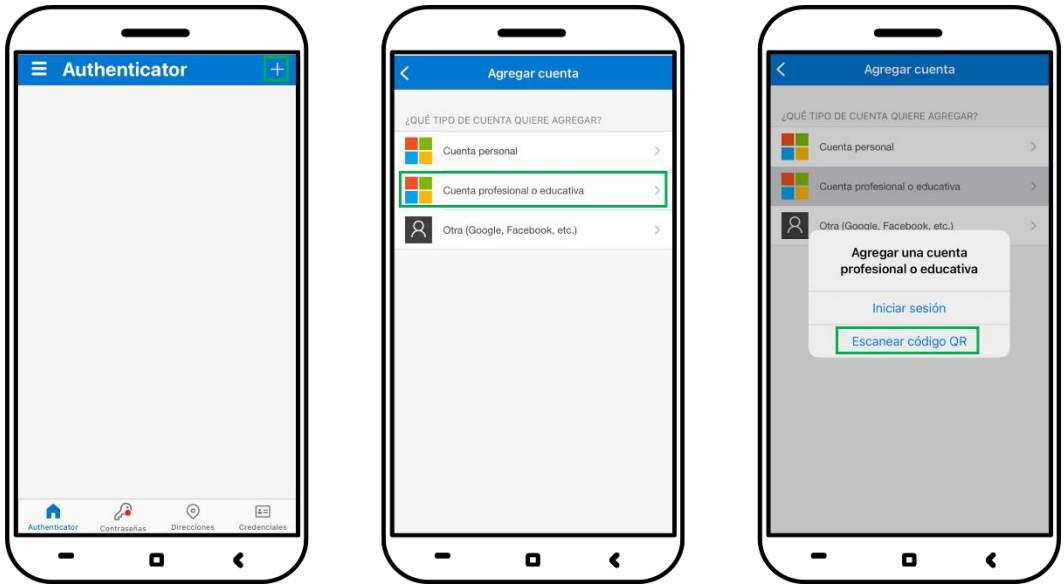
Paso 5: Una vez que hayas descargado la aplicación a tu dispositivo móvil, regresaremos a tu computadora y deberás dar click en **“Siguiente”**



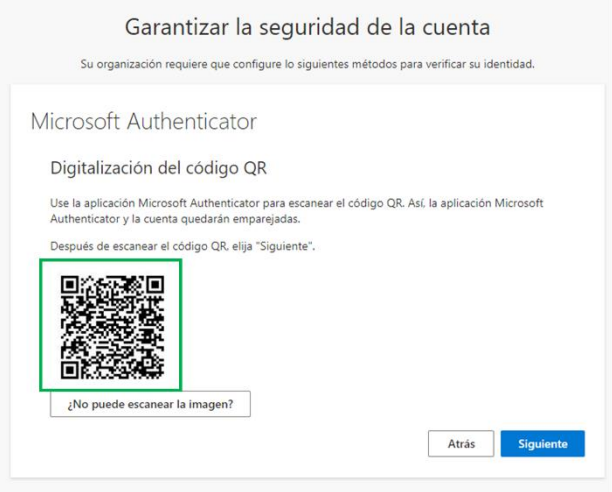
Paso 6: Te saldrá la siguiente ventana y deberás dar clic en **“Siguiente”**



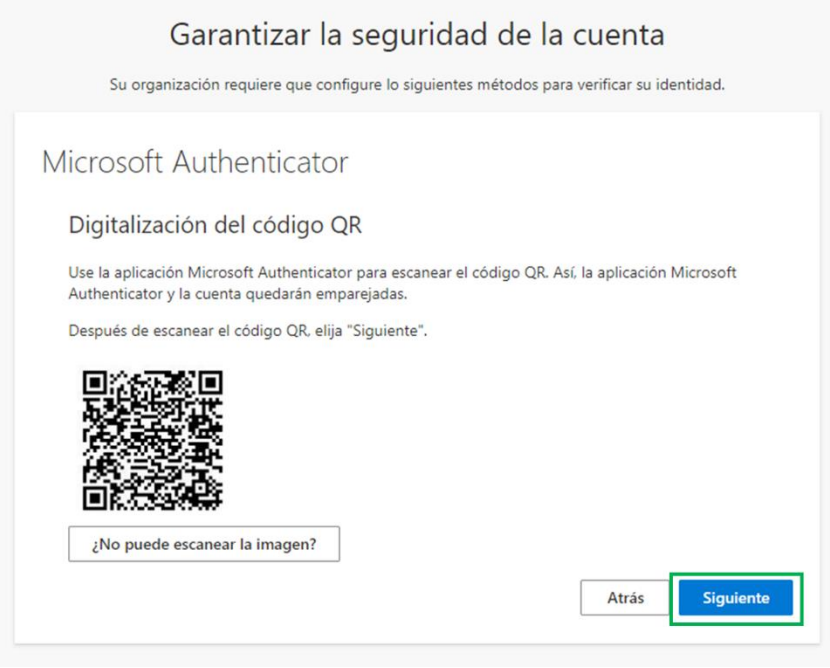
Paso 7: En la aplicación Microsoft Authenticator en tu dispositivo móvil deberás agregar la cuenta, para lo cual debrás ir al botón **“+”** y posteriormente seleccionar **“Cuenta profesional o educativa”** y seleccionarás **“Escanear código QR”**



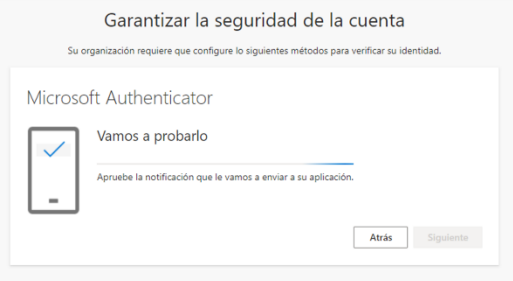
Paso 8: Se abirá una ventana para que puedas escanear con tu dispositivo móvil el código QR que se ve en tu computadora



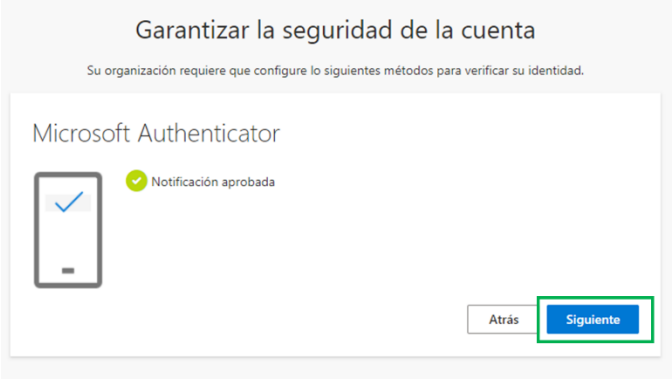
Paso 9: Una vez que hayas escaneado el código, deberás dar clic en **“Siguiente”**



Paso 10: Te pedirá realizar una prueba de aprobación desde tu dispositivo móvil



Paso 11: Una vez que hayas aprobado el inicio de sesión, verás la siguiente ventana y deberás dar click en **"Siguiente"**



Paso 12: Verás la confirmación final de la configuración de MFA

Paso 13: Como paso final te pedirá que cambies tu contraseña. Te recomendamos que tu contraseña tenga las siguientes características:

- Sugerencias para la creación de una contraseña segura:
  - ✓ Letras mayúsculas y minúsculas.
  - ✓ La contraseña debe incluir caracteres especiales.
  - ✓ La longitud de la contraseña debe ser igual o mayor a 8 caracteres.
- Pasos que debes evitar
  - x **No** debe tener espacios en blanco.
  - x **No** utilizar información personal en la contraseña (como su nombre, fecha de nacimiento, etc)
  - x **No** utilizar patrones de teclado (qwerty) ni números en secuencia (1234)
  - x **No** utilizar únicamente números, mayúsculas o minúsculas
  - x **No** repetir caracteres (111111)

Cualquier duda o comentario que tengas no dudes en contactar a José Gomez (joseg@synnex.com)