madriddigital
Agencia para la Administración Digital de la Comunidad de Madrid

PROGRAMA adapta

Comunidad de Madrid
CONSEJERÍA DE ADMINISTRACIÓN LOCAL Y DIGITALIZACIÓN

Guía de usuario

Doble Autenticación

Índice

1 Introducción

Este documento es la guía de uso de MFA en Madrid Digital.

1.1 ¿Qué es MFA?

MFA viene del inglés MultiFactor Authentication y permite usar un segundo factor de autenticación cuando accedemos a los servicios de Madrid Digital.

Existen tres factores de autenticación:

- Algo que sabes, por ejemplo un usuario y contraseña, un PIN de acceso a una tarjeta, etc.
- Algo que tienes, por ejemplo, un móvil, una tarjeta de coordenadas, etc.
- Algo que eres, por ejemplo, tu huella digital, reconocimiento facial, etc

Cuando se habla de Autenticación Multifactor, es usar una combinación de los tres factores anteriores.

En Madrid Digital, el MFA consistirá en saber un usuario y contraseña y tener un teléfono. Para poder usar el teléfono deberemos registrarlo previamente. Más adelante se explicará cómo.

1.2 ¿De qué métodos de autenticación dispongo?

Usando el teléfono móvil, existen hasta cuatro métodos de autenticación que podremos configurar para usarlo como método de autenticación de MFA

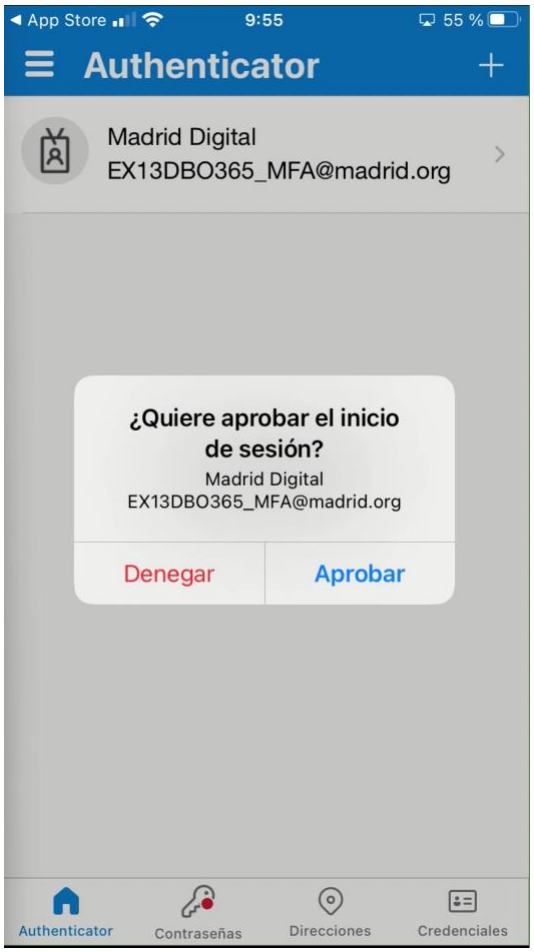
- Aplicación móvil. Es una aplicación que instalaremos en nuestro teléfono móvil llamada Microsoft Authenticator. Usando la aplicación del móvil tendremos dos métodos:
    - Notificación. Aparece una notificación en el móvil donde deberemos aprobar en caso que seamos nosotros quienes queremos acceder.

- Código de un solo uso (OTP – OneTime Password). La aplicación genera un código que se renueva automáticamente cada 30 segundos.

- Llamadas de Teléfono. Se recibirá una llamada de teléfono, se deberá contestar la llamada y pulsar la tecla #
- Mensaje de texto. Se recibirá un SMS con un código que deberemos usar para autenticarnos.

1.2.1 Aplicación Móvil – Notificación

Recibiremos una notificación al móvil, similar a la mostrada en la siguiente imagen. Deberemos pulsar el botón **Aprobar** para validar la autenticación.



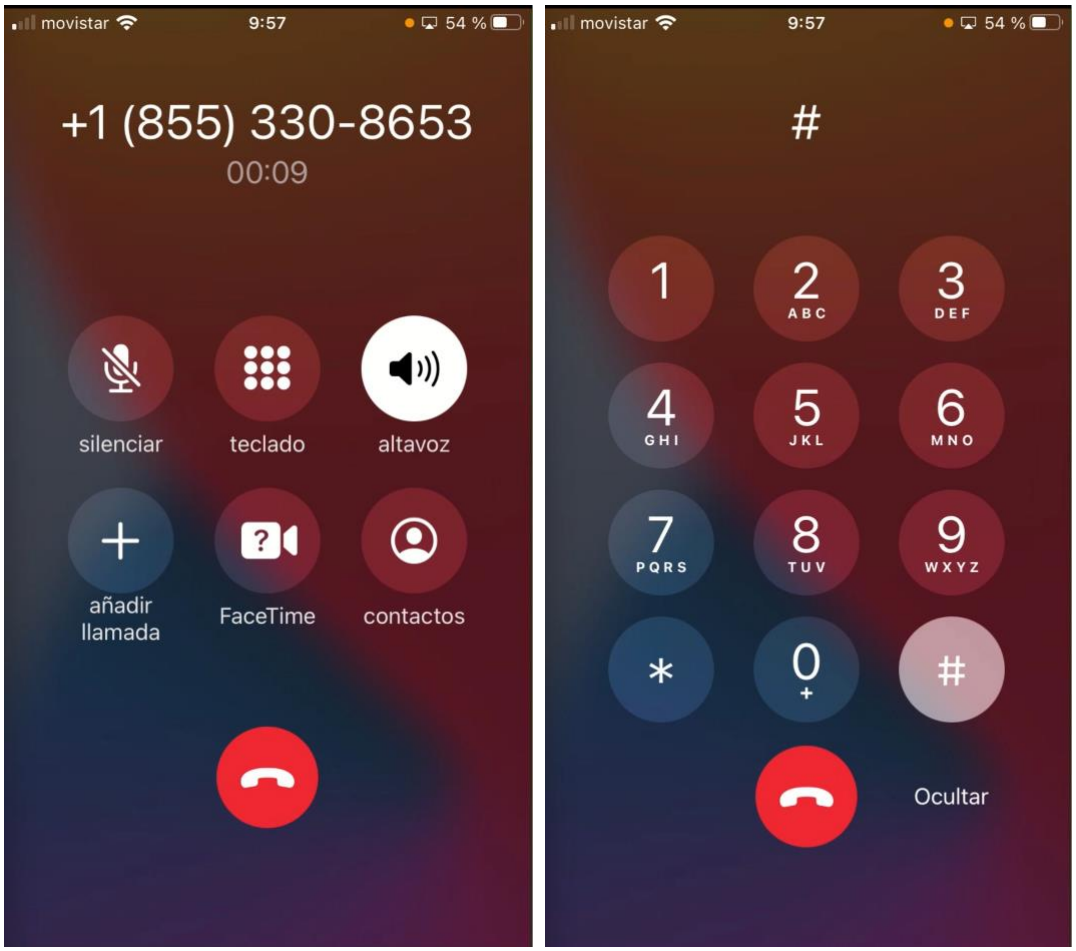
1.2.2 Aplicación Móvil – Código de un solo uso (OTP)

En la propia aplicación, si selecciona la cuenta con la que queremos acceder, podemos ver un hay un código que se genera cada 30 segundos. Este código podrá usarse como doble factor de autenticación.

1.2.3 Llamada de Teléfono

Durante la autenticación se recibirá una llamada de teléfono. Para hacer la autenticación, habrá que descolgar la llamada y se podrá oír una locución dando la bienvenida e indicando que pulsemos la tecla “almohadilla” (#).
Una vez pulsada la tecla “almohadilla”, se podrá oír una locución indicado que la autenticación del doble factor se habrá realizado correctamente.

No es necesario esperar a que termine la locución para pulsar la tecla # y finalizar la autenticación.

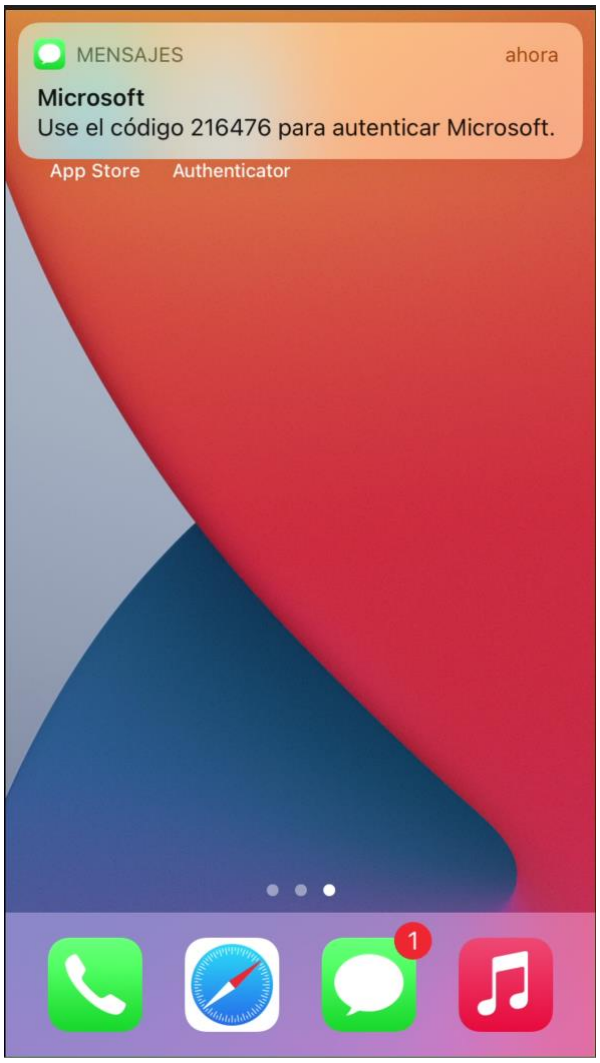


La llamada de teléfono podrá realizarse a tres números telefónicos:

- Teléfono: Correspondería a nuestro teléfono móvil habitual.
- Teléfono alternativo. Sería un número de teléfono que podríamos usar en caso de pérdida del primero.
- Teléfono de trabajo. Se puede indicar un teléfono fijo junto a una extensión.

1.2.4 Mensaje SMS

Se recibirá un código a través de un mensaje SMS, tendremos que introducir este código para realizar la autenticación.



El mensaje de texto SMS podrá recibirse en dos números telefónicos:

- Teléfono: Correspondería a nuestro teléfono móvil habitual.
- Teléfono alternativo. Sería un número de teléfono que podríamos usar en caso de pérdida del primero.

2 Proceso de Enrolado

El proceso de enrolado se denomina al proceso de configurar y registrar nuestro teléfono móvil para que sea usado como doble factor de autenticación.

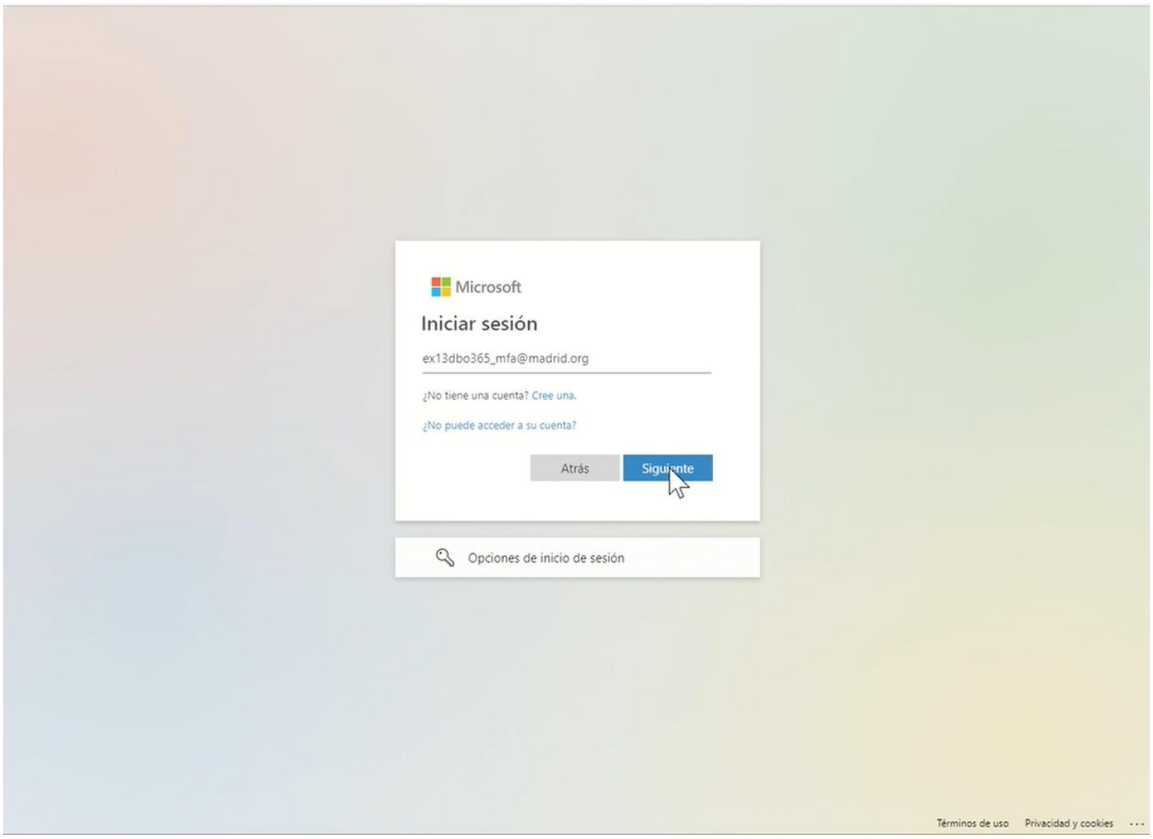
Hay un video disponible donde se puede ver todo el proceso.

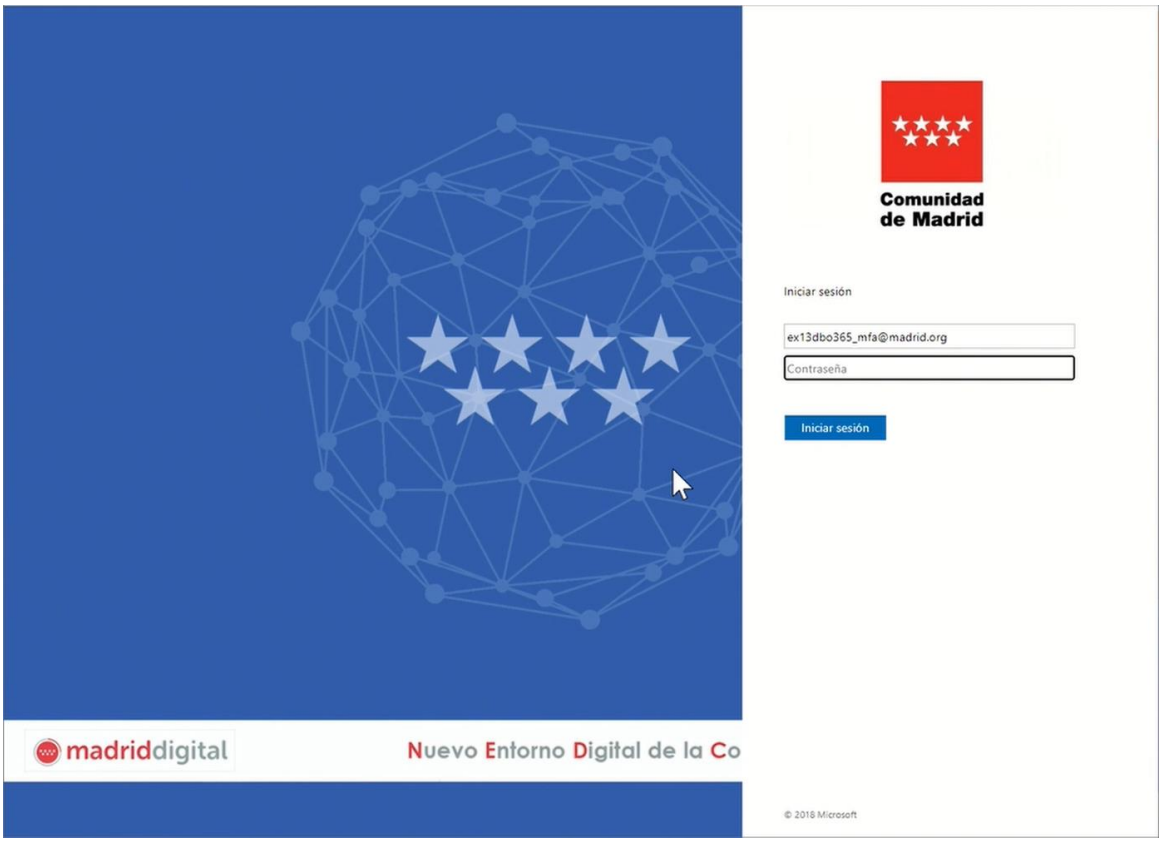
El video está disponible en el siguiente enlace.

De todos modos el proceso de enrolado, o registro, consistirá en los siguientes pasos:

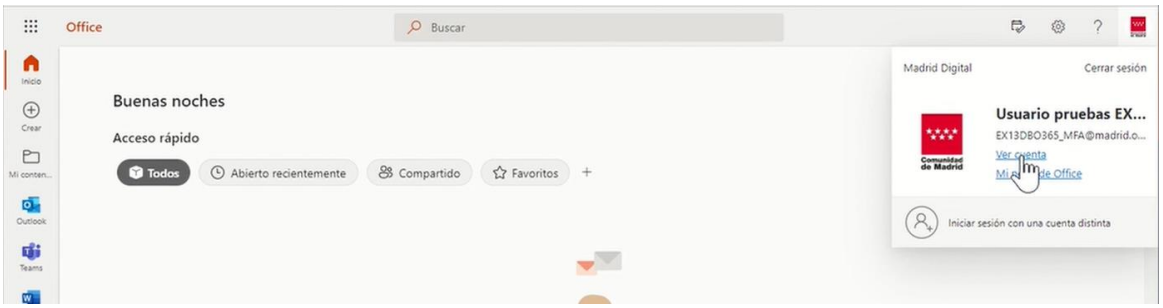
1. Se iniciará sesión en el portal de office https://www.office.com

2. Introduciremos usuario y a continuación contraseña.





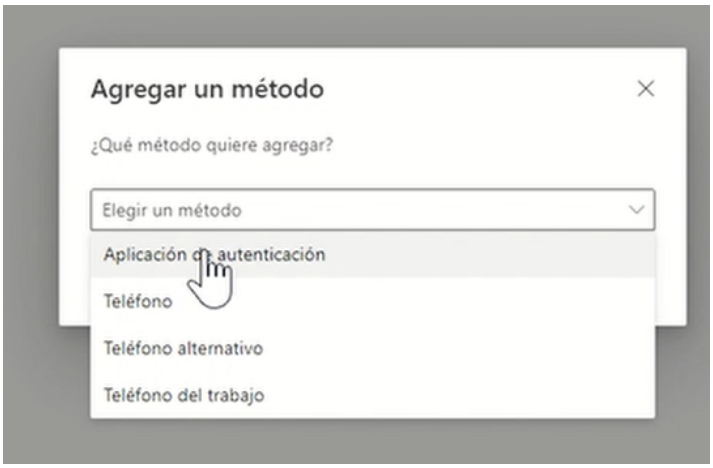
3. Dentro del portal, vamos a donde el usuario y seleccionamos **Ver cuenta**



4. Pulsamos en **ACTUALIZAR INFORMACIÓN**, dentro del apartado **Información de Seguridad**.

5. En el apartado Información de seguridad no debería aparecer ningún método de autenticación registrado.
   Para añadir uno pulsamos el botón **Agregar método de inicio de sesión**

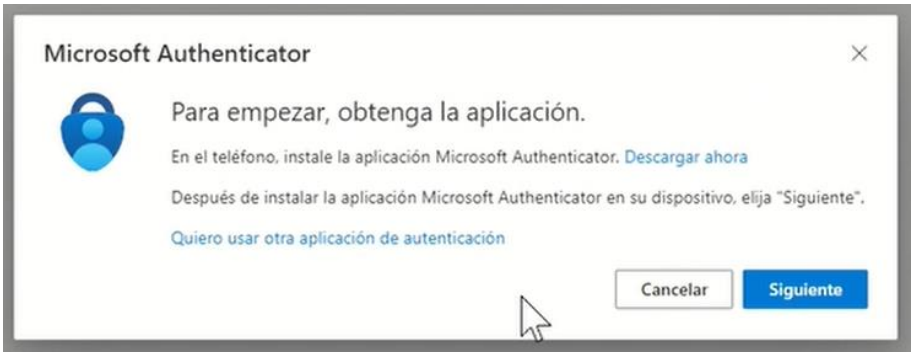
6. Al agregar un método de autenticación aparecen todos los métodos para MFA disponibles.



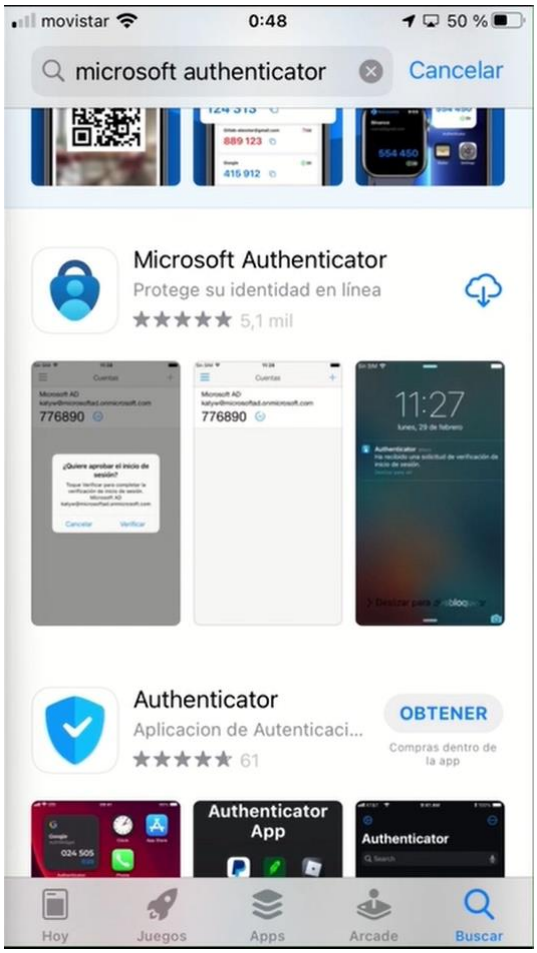
En el apartado "¿De qué métodos de autenticación dispongo?"

7. Como primer método se selecciona la opción "**Aplicación de autenticación**" y se pulsará el botón **Agregar**

8. Aparece la ventana de inicio del asistente:



9. Lo primero que se debe hacer es necesario instalar la aplicación Microsoft Authenticator en el móvil. Nos vamos al App Store (iPhone) o Play Store (Android)



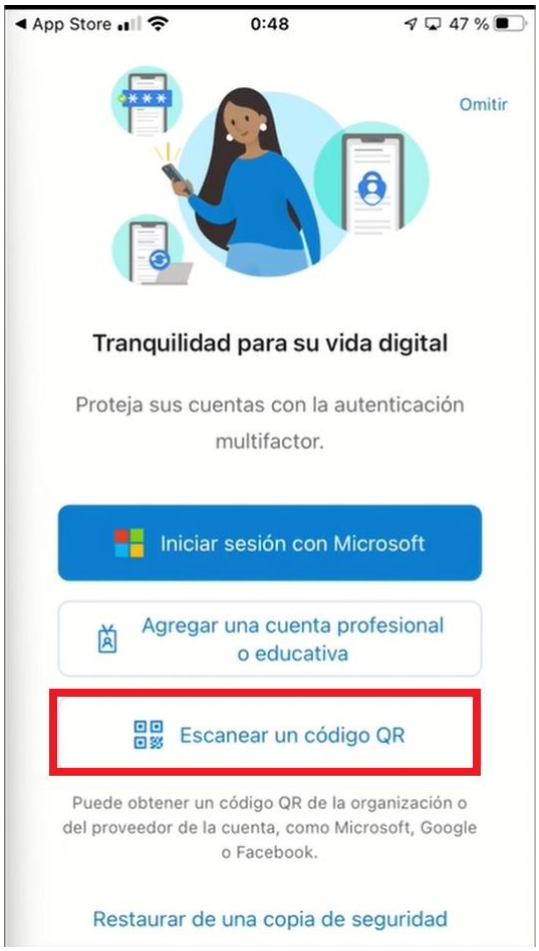
10. Mientras que se termina de instalar las aplicaciones en el móvil, es posible avanzar en el asistente del navegador. En el navegador pulsamos el botón **Siguiente**, con lo que continuará el asistente.

Volvemos a pulsar el botón **Siguiente**

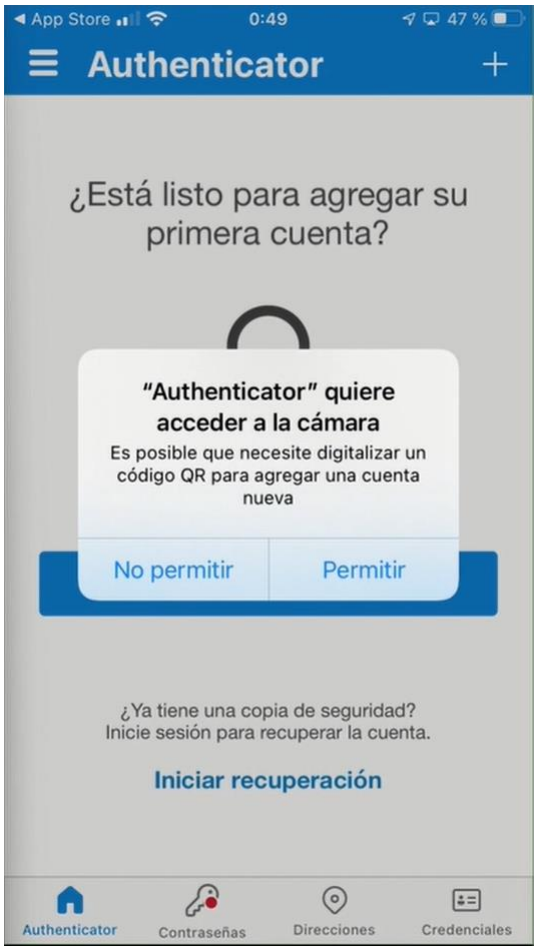
11. El último paso del asistente para el doble factor, consiste en un código QR, de tal menra que facilita la gestión.

12. ahora es necesario volver al móvil y abrir la aplicación recién instalada. Al abrir la aplicación lo primero que hay que hacer es, aceptar las condiciones de uso.

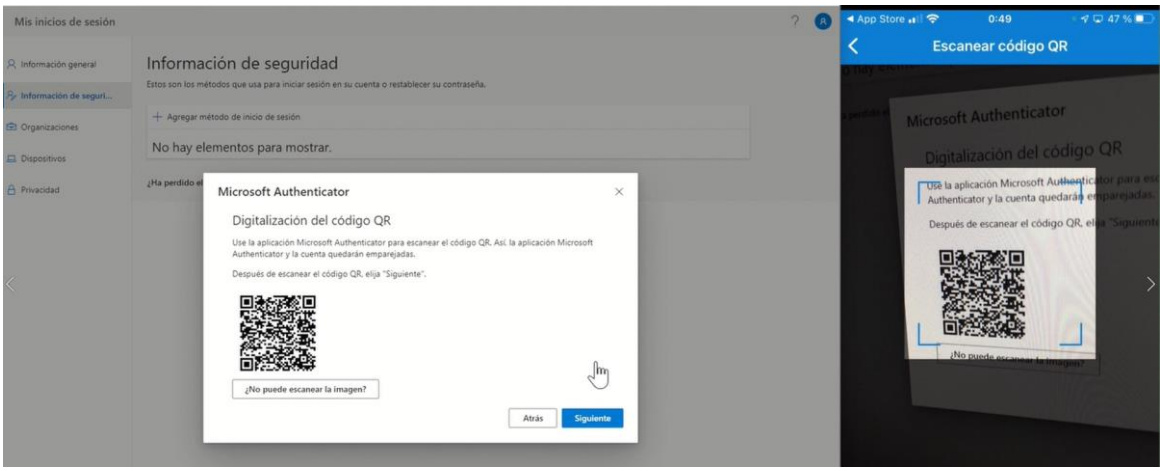
13. En el navegado tenemos un código QR, por lo que Microsft Authenticator tiene la opción **Escanear un código QR**.



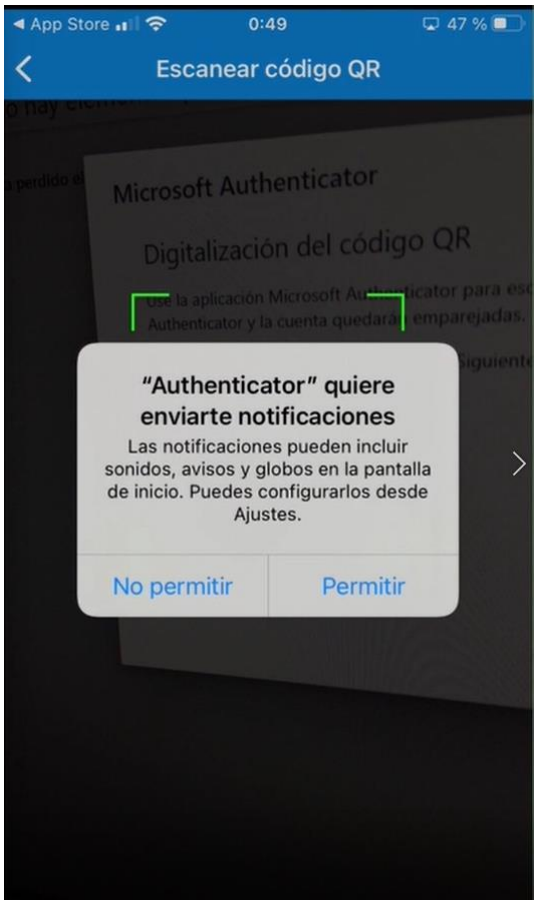
14. Desde la aplicación del móvil, se debe permitir el acceso a la cámara.



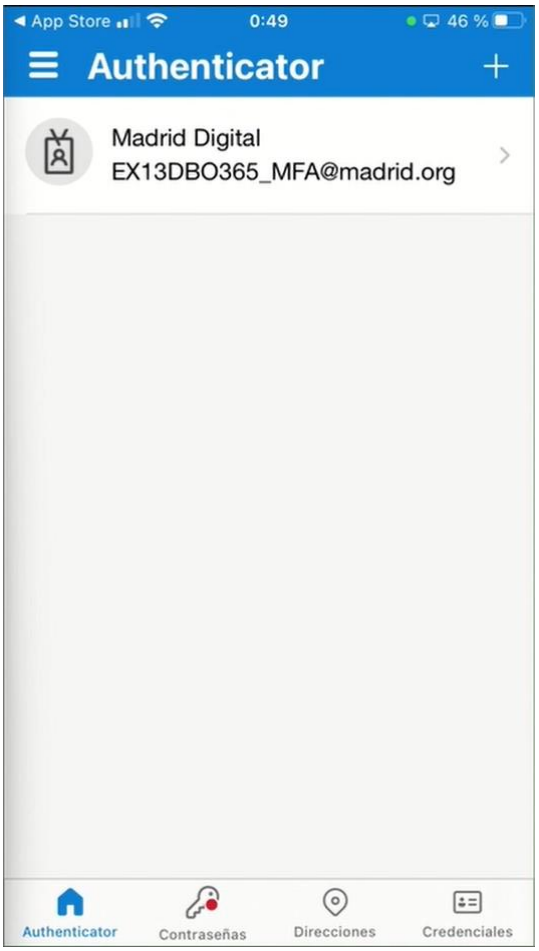
15. Una vez permitida, se debe apuntar con la cámara del móvil a dicho código QR



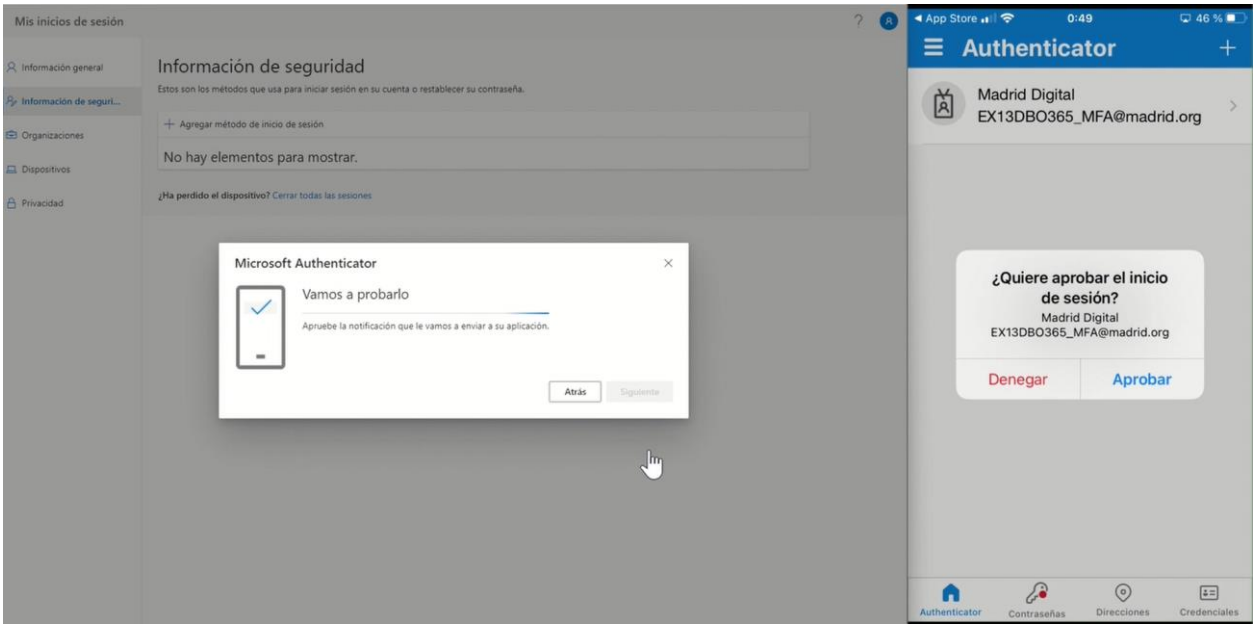
16. Una vez escaneado el código QR, es necesario permitir que la aplicación reciba notificaciones al móvil.



17. En este momento, la aplicación móvil **Microsoft Authenticator** tendrá agregada la cuenta del usuario que ha hecho login.



18. Ahora volvemos al navegador y pulsamos el botón **Siguiente**, por lo que la aplicación enviará una notificación al móvil para que pruebe el acceso.

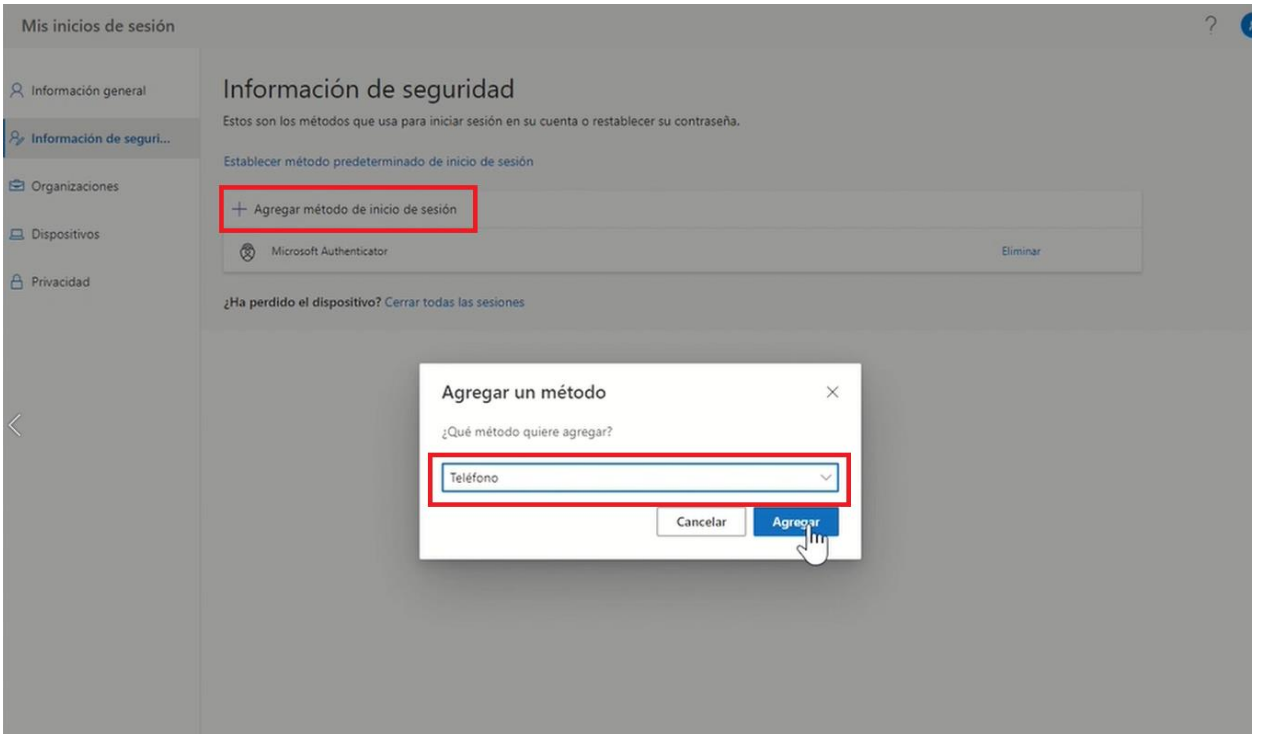


Hay que darle al botón **Aprobar**, en el móvil, para indicar que se aprueba el acceso.

19. En el navegador se podrá comprobar que la notificación ha sido aprobada con éxito.

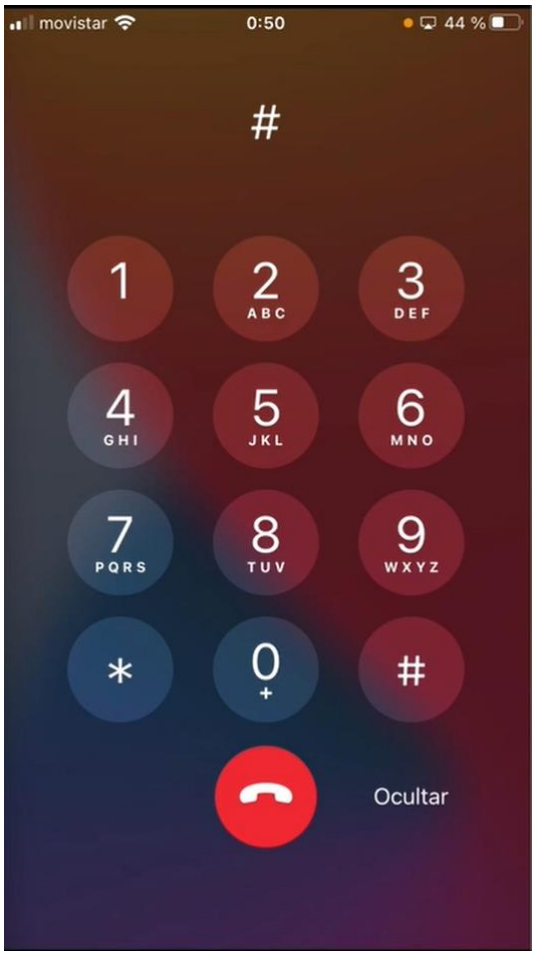
20. Ya estaría agregada la aplicación Microsoft Authenticator como doble factor

21. A continuación, se debe agregar un teléfono móvil, para tener al menos dos métodos y poder accedes sin abrir una incidencia.
    Agregamos un método de inicio de sesión, seleccionamos Teléfono y pulsamos **Agregar**.



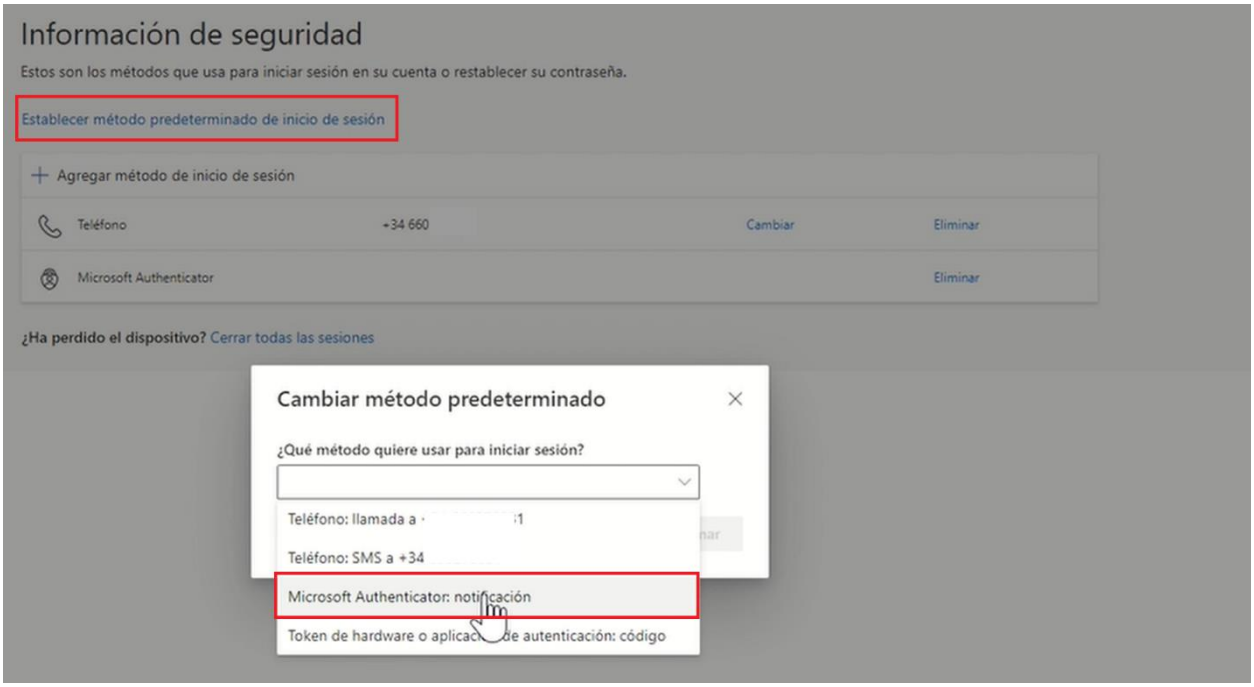
22. Rellenaremos los campos: código del país, número de teléfono móvil, seleccionaremos la opción Llámame y pulsaremos el botón **Siguiente**

23. Nos llamarán al móvil, descolgaremos la llamada, seleccionamos el teclado y pulsaremos almohadilla (#)



24. Si todo ha ido bien, aparecerá un mensaje indicando que todo está correctamente.

25. Por último se debe indicar el método de autenticación predeterminado. Este método es el que se usará cuando se requiera MFA
Pulsamos sobre **Establecer método predeterminado de inicio de sesión** y seleccionaremos **Microsoft Authenticator: notificación**



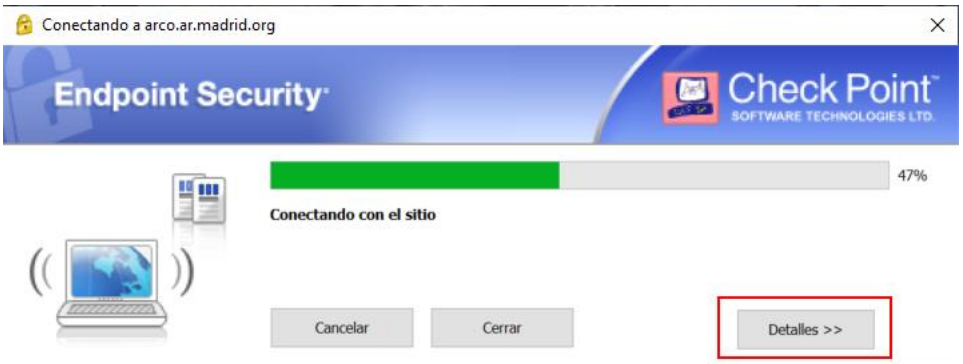
Pulsamos el botón **Confirmar**.

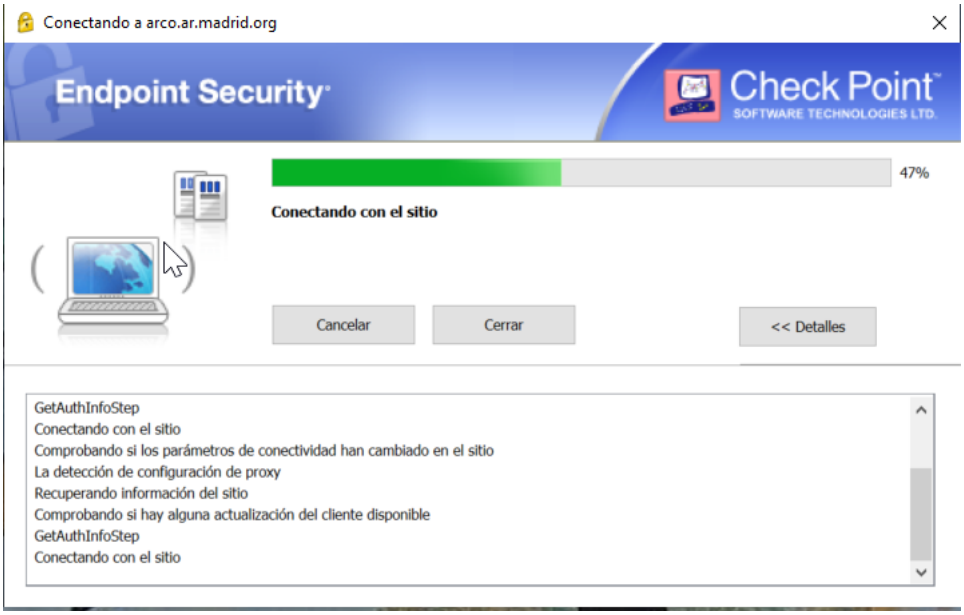
3 Acceso a la VPN con MFA

El acceso a la VPN con MFA se realizará con el cliente de Checkpoint, que deberá estar instalado en nuestro equipo.

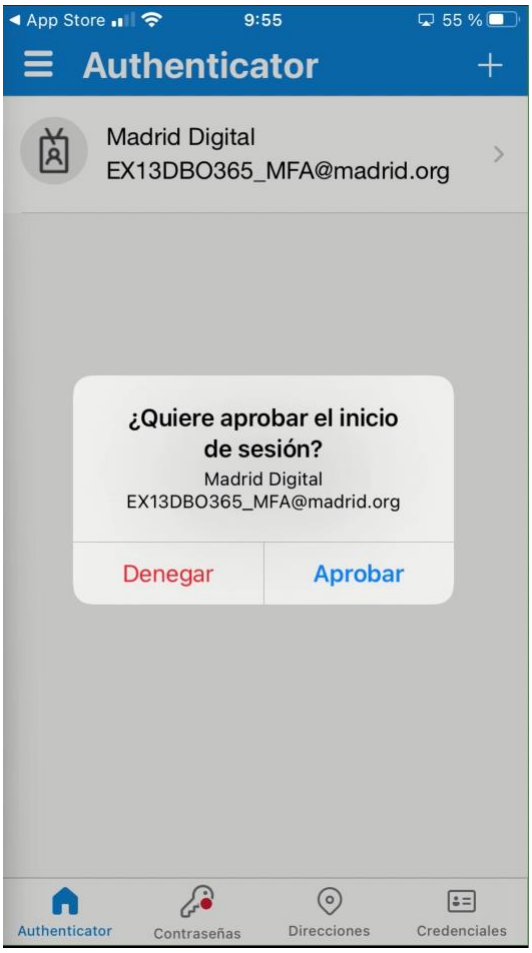
- Abriremos la aplicación cliente de Checkpoint y seleccionaremos el sitio **arco.ar.madrid.org**, que es el sitio donde se requerirá MFA para acceder.
- En este misma pantalla indicaremos el nombre de usuario, se deberá ser el mismo que el usuario usado para acceder a Office 365.

- Durante la conexión podremos ver el progreso de la misma, así como los **Detalles**

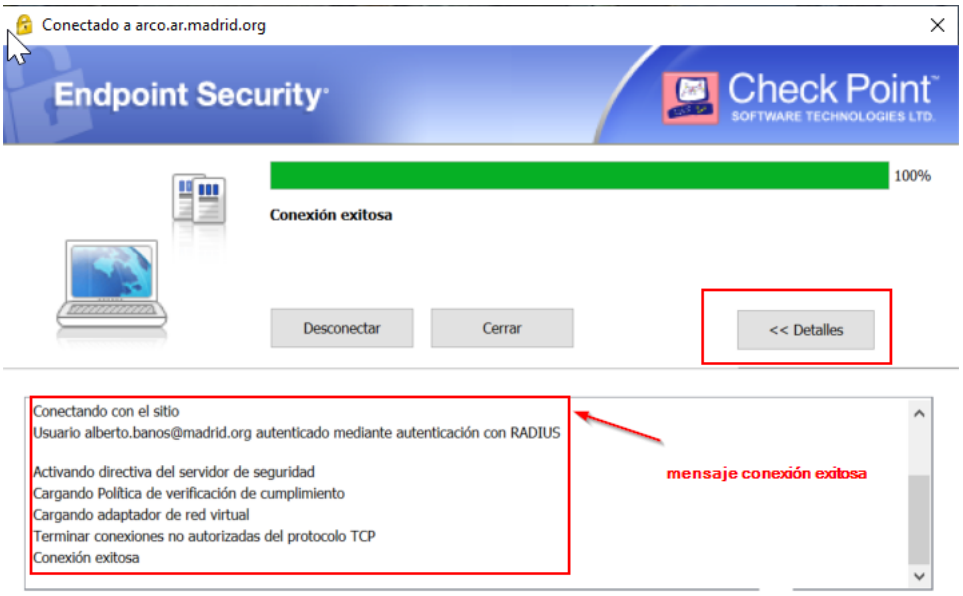




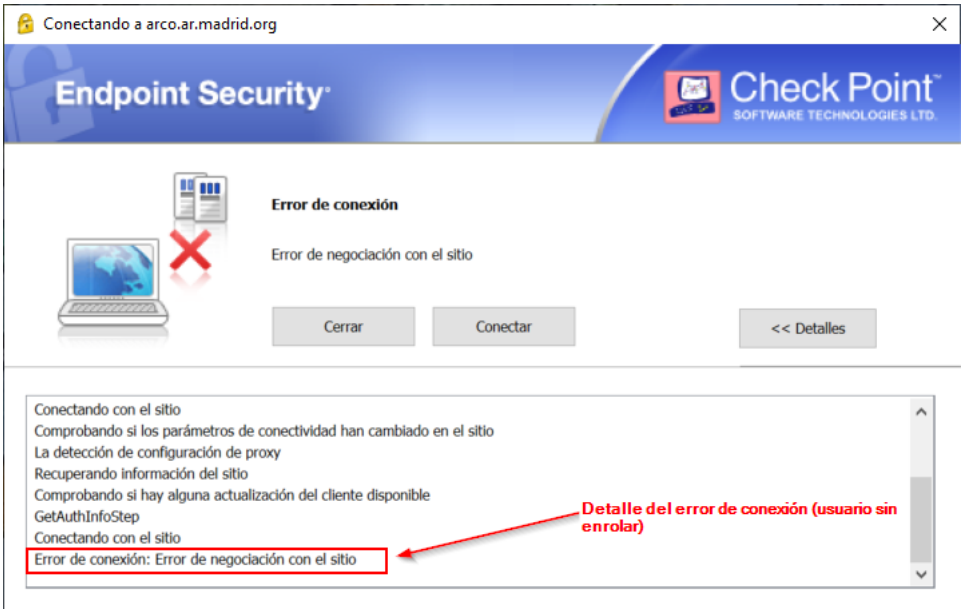
- Durante el proceso de conexión, se solicitará la autenticación con MFA. Dependiendo del método de autenticación predeterminado seleccionado durante el proceso de registro.
  Si es la notificación a la aplicación Microsoft Authenticator, en el móvil recibirá una notificación de este tipo:



- Si la conexión a la VPN se ha realizado con éxito aparece una ventana similar a esta:



Importante: Si no te has registrado/enrolado en MFA, el mensaje que aparecerá durante la conexión a la VPN será similar a este:



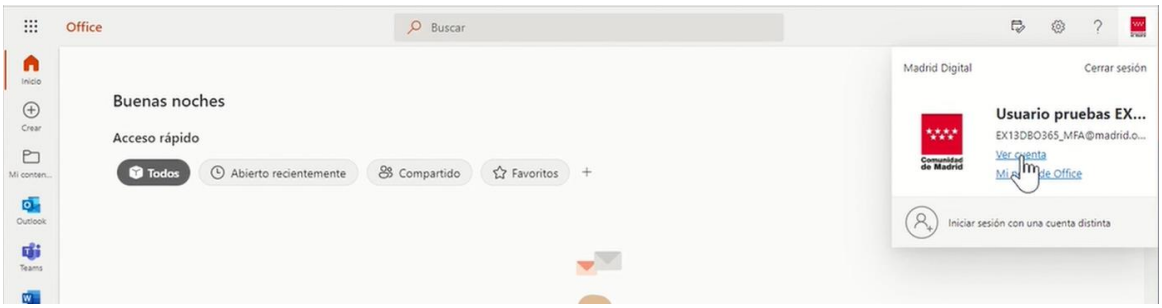
En este caso, deberás seguir los pasos indicados en el apartado “Proceso de Enrolado” de este documento.

4 Gestionar Información de Seguridad

Podemos gestionar qué métodos de autenticación podemos usar, cuál será el predeterminado, o si queremos añadir un nuevo método de autenticación.

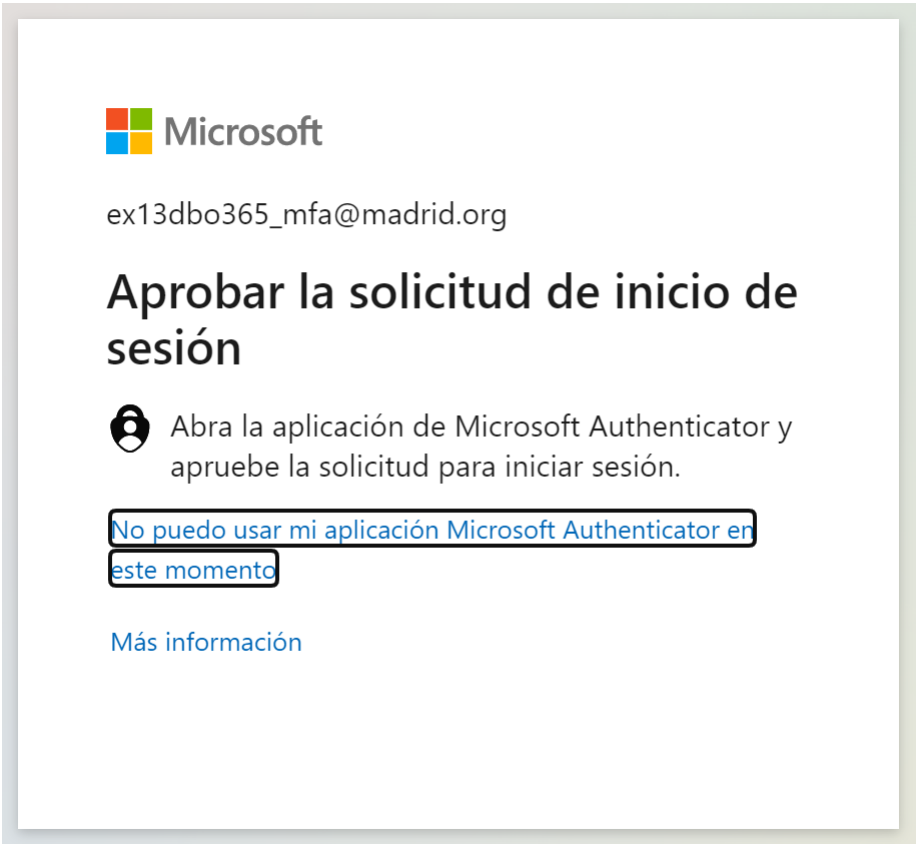
Como se ha visto en el apartado “Proceso de Enrolado”, esta gestión se realiza desde el apartado “Información de Seguridad” de la cuenta del usuario.

A Información de Seguridad se puede acceder desde el portal de office, a la derecha, vamos a donde el usuario y seleccionamos **Ver cuenta**



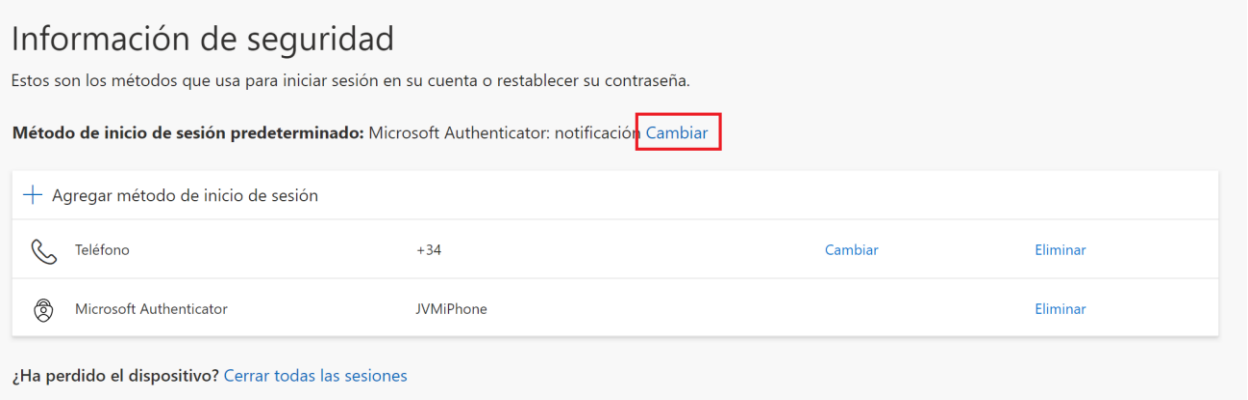
Y aquí estará el acceso a Información de Seguridad.

Si previamente no nos hemos autenticado con MFA, al pulsar ACTUALIZAR INFORMACIÓN se requerirá el uso de MFA. Si el método de autenticación predeterminado es Microsoft Authenticator, aparecerá una ventana similar a esta en el navegador:



4.1 Cambiar método predeterminado

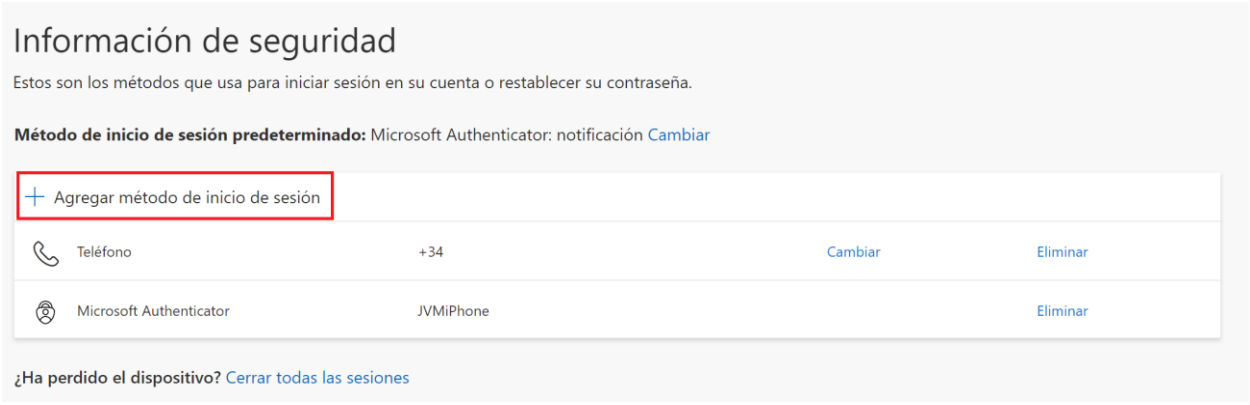
Una vez en la pantalla de Información de Seguridad es posible modificar el método de autenticación predeterminado.



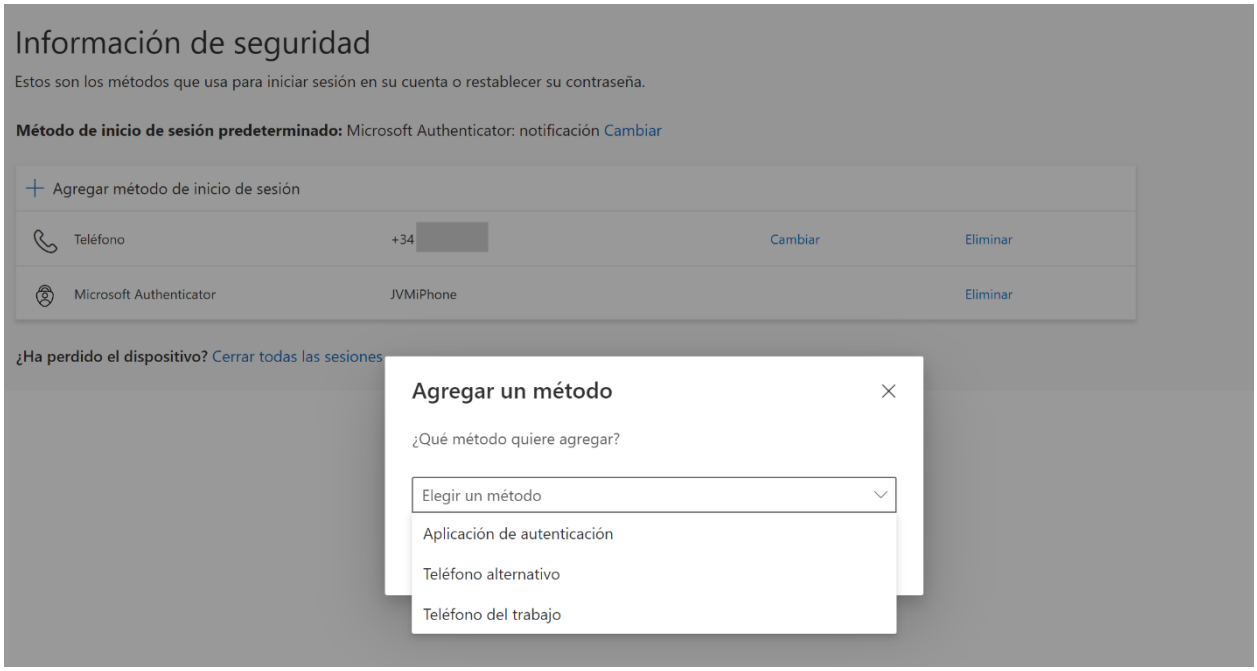
Al pulsar cambiar aparece la lista de métodos de autenticación indicados.

4.2 Añadir método de autenticación

Para añadir un número método de autenticación pulsamos sobre **Agregar método de inicio de sesión**



Aparecerá la lista de métodos que tendríamos disponibles.



5 ¿Qué hacer en caso de problemas?

SI tienes algún problema puedes acudir según tu perfil

- **Consejera Delegada:** SIAC – 914205500 - siac@madrid.org
- **Directores y Subdirectores:** UNIR – 914936800 - unir@madrid.org
- **Resto de plantilla:** Servicio de soporte al puesto digital - 628457156 / 803924 - MD_SERVICIO_SOPORTEPUESTO@madrid.org