

CONFIGURACIÓN DE LA AUTENTICACIÓN MULTIFACTOR (MFA) EN MICROSOFT 365

Guía de usuario v5.11

El siguiente documento le guiará en el proceso de configuración de la autenticación multifactor para su cuenta de la CARM en Office 365 (Correo, Teams, OneDrive,...). Mediante este procedimiento su cuenta estará protegida ante un robo de credenciales, lo que aporta un beneficio directo en su seguridad particularmente y en la del resto de la organización.

Recomendamos usar como primer método de doble factor la aplicación “*Microsoft Authenticator*”. Esta aplicación también se puede usar para securizar el acceso a otras cuentas no corporativas.

Aunque es posible configurar como primera opción la llamada a un número de teléfono fijo o móvil, este documento parte de la premisa de que ha elegido como primera opción la aplicación indicada anteriormente.

INDICE DE CONTENIDOS

| | |
|---|----|
| 1. ACCESO A LAS OPCIONES DE SEGURIDAD DE NUESTRA CUENTA Microsoft 365 | 2 |
| 2. CONFIGURACIÓN MFA PREVIA A SU ACTIVACIÓN..... | 4 |
| 3. AÑADIR UN SEGUNDO MÉTODO DE VERIFICACIÓN | 8 |
| 4. CONFIGURACIÓN MFA TRAS SU ACTIVACIÓN | 9 |
| 5. ELIMINAR O MODIFICAR UN MÉTODO DE INICIO DE SESIÓN..... | 12 |
| 6. INICIO DE SESIÓN CON MFA EN APLICACIONES DE OFFICE 365 | 13 |
| 7. PROBLEMAS FRECUENTES..... | 14 |

1. ACCESO A LAS OPCIONES DE SEGURIDAD DE NUESTRA CUENTA Microsoft 365

Estos son los pasos a seguir para acceder a las opciones de seguridad de su cuenta M365.

1. Desde su ordenador pulse el siguiente enlace <https://mysignins.microsoft.com/security-info>
2. En el cuadro de diálogo siguiente introduciremos nuestro usuario y contraseña corporativos para Office 365 (`<login>@carm.es` o `<login>@ad.sms.carm.es` si usted pertenece al SMS):

Microsoft

Iniciar sesión

pru00a@carm.es

¿No tiene una cuenta? [Cree una.](#)

¿No puede acceder a su cuenta?

Siguiente

Escribir contraseña

.....

He olvidado mi contraseña

Iniciar sesión

Si tiene problemas para acceder, póngase en contacto con el Centro de Atención a Usuarios (279100 para usuarios del SMS // 368900 o GLPI para usuarios de la CARM)

3. Acto seguido se nos preguntará si deseamos mantener la sesión iniciada. Para esta configuración no importa lo que respondamos así que pulsaremos cualquiera de las dos opciones (Sí o No)

Región de Murcia

pru00a@carm.es

¿Quiere mantener la sesión iniciada?

Haga esto para reducir el número de veces que se le solicita que inicie sesión.

No volver a mostrar

No Sí

Si tiene problemas para acceder, póngase en contacto con el Centro de Atención a Usuarios (279100 para usuarios del SMS // 368900 o GLPI para usuarios de la CARM)

4. Finalmente se mostrará el panel con las opciones de seguridad de nuestra cuenta M365

Información de seguridad

Estos son los métodos que usa para iniciar sesión en su cuenta o restablecer su contraseña.

You're using the most advisable sign-in method where it applies.

Sign-in method when most advisable is unavailable: Microsoft Authenticator: notificación

Última actualización: hace 15 días

¿Ha perdido el dispositivo? [Cerrar todas las sesiones](#)

Otras formas de llegar a las opciones de seguridad de su cuenta M365 son:

- 1) Accediendo al panel privado de su cuenta de Office 365 (<https://myaccount.microsoft.com/>) y desde ahí seleccionar la opción “Información de seguridad”

Nombre Apellido

pru00a@carm.es

Información de seguridad

ACTUALIZAR INFORMACIÓN >

Dispositivos

- 2) Usar enlace abreviado <https://aka.ms/MFASetup>

2. CONFIGURACIÓN MFA PREVIA A SU ACTIVACIÓN

1. En primer lugar, instale y ejecute la aplicación “**Microsoft Authenticator**” en su teléfono móvil. Podrá encontrarla en el Apple Store (si tiene un dispositivo Apple iPhone) o Play Store (si tiene un dispositivo Android).



En el siguiente enlace <https://www.microsoft.com/es-es/security/mobile-authenticator-app?rtc=1> está disponible la descarga segura de la aplicación a través de la tienda oficial de su dispositivo (Apple Store para Iphone o Play Store para Android)

2. Acceda a las opciones de seguridad de su cuenta M365 tal y como se indica en el punto “[1. Acceso a las opciones de seguridad de nuestra cuenta M365](#)”.
3. De esta forma habremos llegado a la pantalla de configuración de métodos Multi Factor. Por defecto tan solo tendremos la contraseña. Pulsamos en “**Agregar método de inicio de sesión**”

Información de seguridad

Estos son los métodos que usa para iniciar sesión en su cuenta o restablecer su contraseña.

+

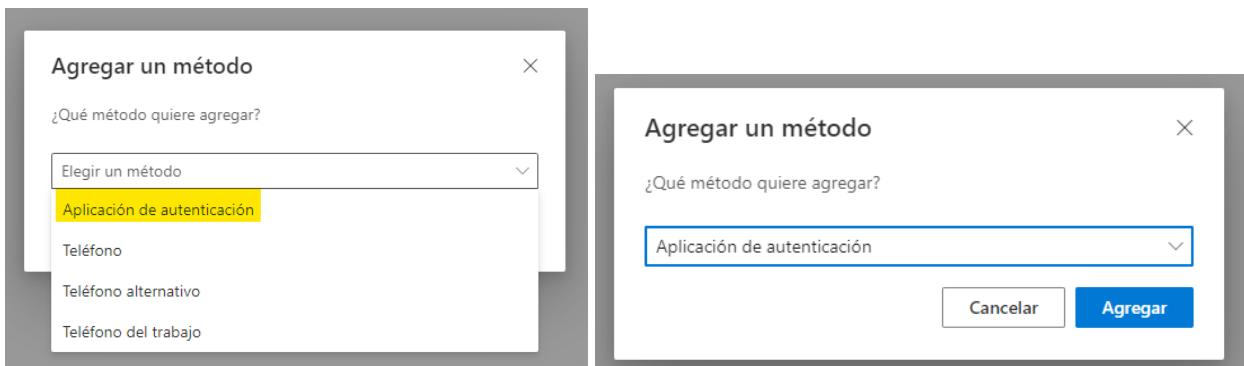
Agregar método de inicio de sesión

Contraseña

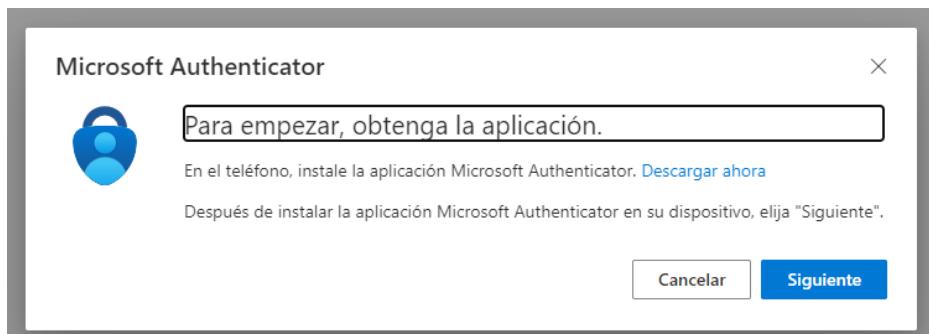
Última actualización: hace 35 minutos

¿Ha perdido el dispositivo? [Cerrar todas las sesiones](#)

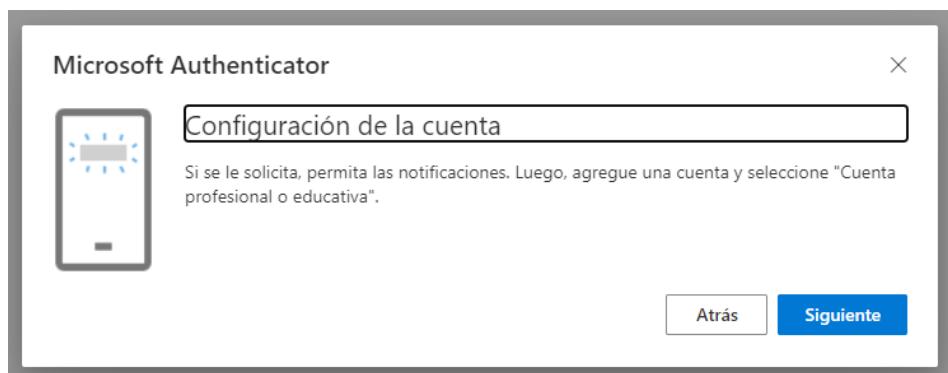
4. En la siguiente ventana nos preguntará sobre el tipo de método que desea agregar. Seleccionamos la opción de “Aplicación de autenticación” y pulsamos “Agregar”.



5. Nos aparecerá una ventana invitándonos a instalar la aplicación *Microsoft Authenticator*, cosa que ya habremos hecho en el paso 1. Pulse “Siguiente”.



6. La siguiente pantalla es informativa, pulse “Siguiente”.



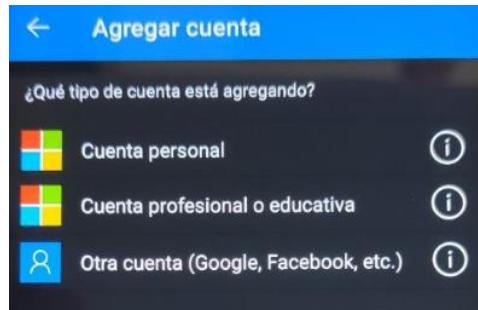
7. Finalmente llegaremos a una pantalla con un código QR que escanearemos desde el móvil en los siguientes pasos:



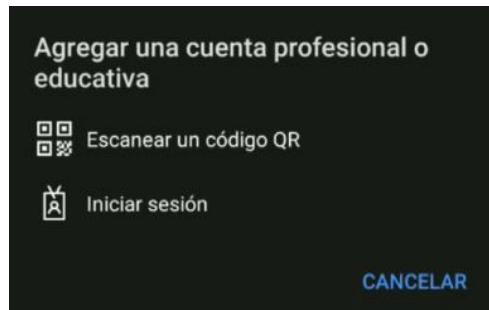
- a) En este momento abriremos la aplicación móvil “Microsoft Authenticator” en nuestro Smartphone:
- En la parte superior pulsaremos en el ícono (+) para agregar una nueva cuenta



- Seleccionaremos la opción “Cuenta profesional o educativa”

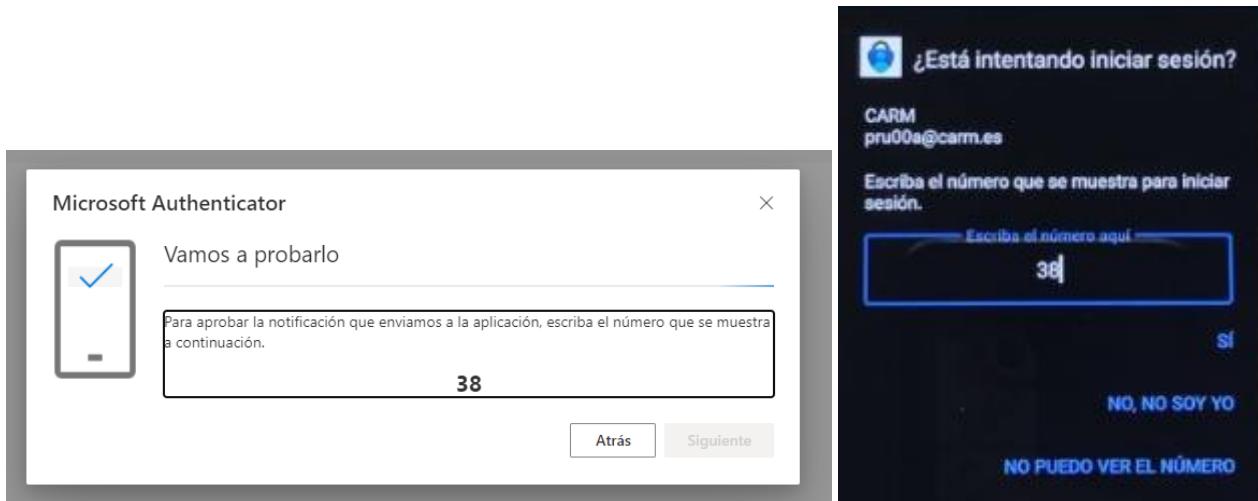


- Elegiremos la opción de “Escanear un código QR”



- Apuntaremos con el visor de la cámara hacia el código QR que nos han facilitado en el paso anterior. Nuestra cuenta quedará añadida en la aplicación.

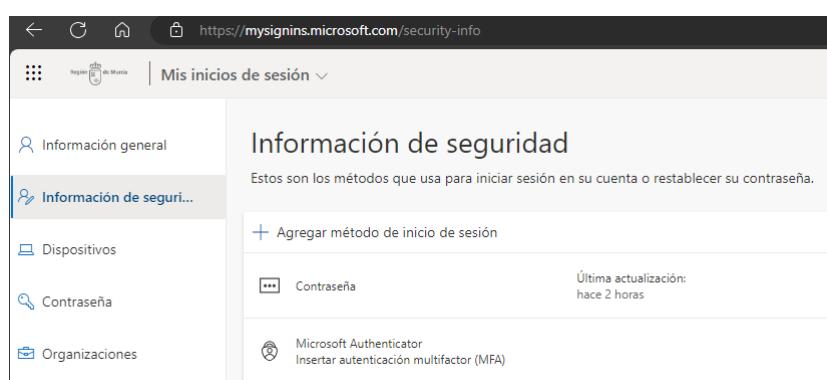
8. De vuelta a la pantalla del ordenador, pulsamos “**Siguiente**” en la ventana que nos muestra el código QR.
9. A continuación se nos propone hacer una prueba de funcionamiento. Recibiremos una notificación en el móvil y al abrirla se nos solicitará un código. Debemos introducir el que se muestra en la pantalla del ordenador y pulsar en “**Sí**”



10. Acto seguido se mostrará en el ordenador una notificación verificando que ha aprobado correctamente el inicio de sesión en el móvil. Pulsamos “**Siguiente**”.



11. Finalmente volveremos a la pantalla inicial, y ahora además de la contraseña como método de inicio de sesión, también tendremos “*Microsoft Authenticator*”.



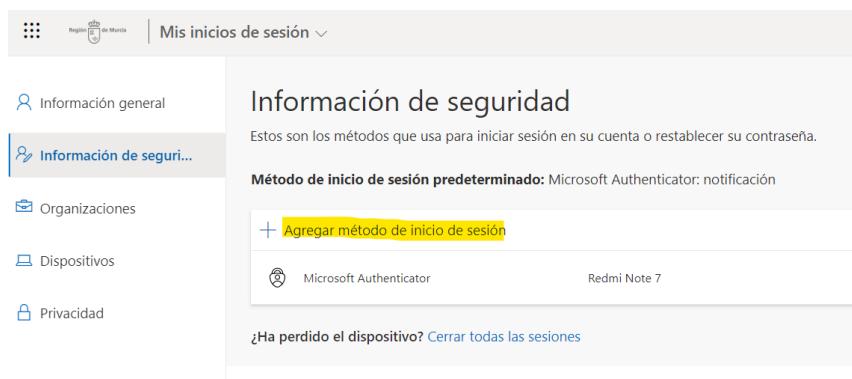
NOTA: Se recomienda encarecidamente la configuración de un segundo método de verificación, ya que en caso de imposibilidad de usar el primero (aplicación Microsoft Authenticator), tengamos otra opción para validar nuestro inicio de sesión.

12. Si desea configurar un segundo método de validación consulte el punto “[3. Añadir un segundo método de verificación](#)”

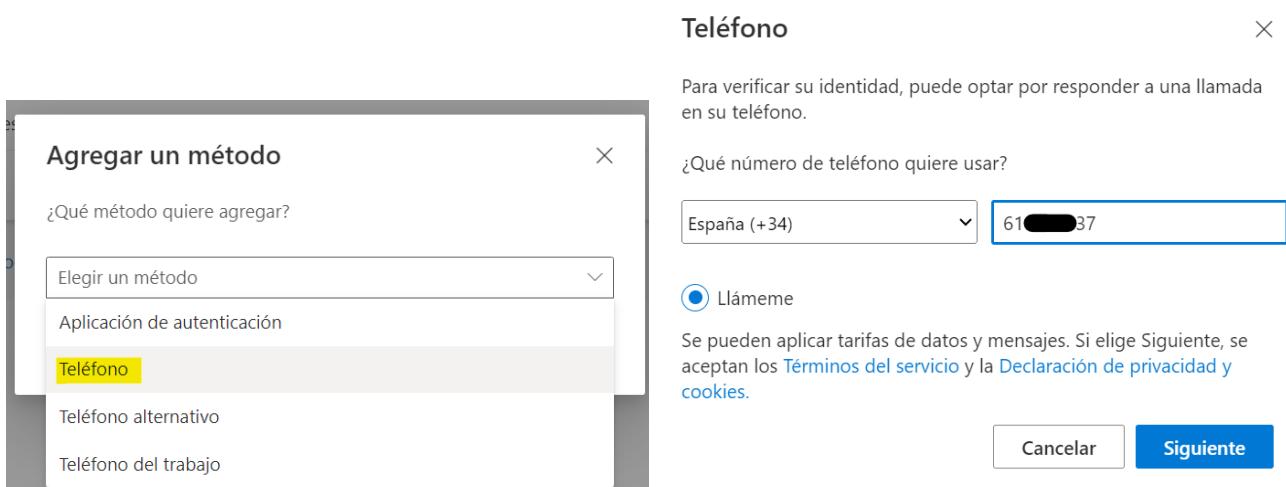
3. AÑADIR UN SEGUNDO MÉTODO DE VERIFICACIÓN

Siga estos pasos para añadir un segundo método de verificación a su cuenta M365.

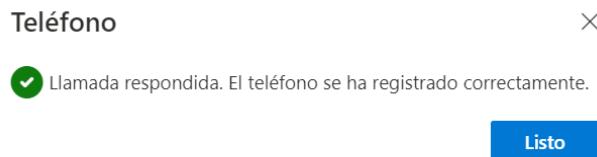
1. Acceda a las opciones de seguridad de su cuenta M365 tal y como se indica en el punto “[1. Acceso a las opciones de seguridad de nuestra cuenta M365](#)”.
2. Pulse la opción “**Agregar método de inicio de sesión**”.



3. Si anteriormente ha configurado “*Microsoft Authenticator*” como método de verificación, en este caso recomendamos seleccionar la opción “Teléfono”, a través de la cual recibirá una llamada de voz en el número indicado. Se recomienda utilizar un número de teléfono móvil, ya que, si configura un teléfono fijo y no se encuentra en la ubicación del mismo, no podrá autenticarse por este medio.



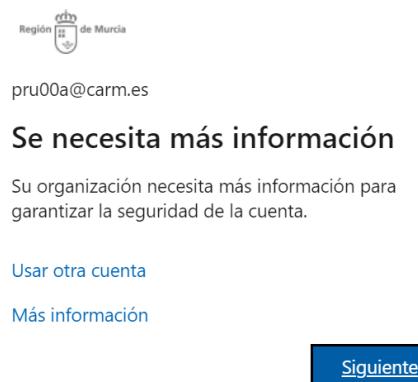
4. Tras pulsar “Siguiente” recibirá una llamada de voz desde un número desconocido o extraño. No se preocupe, puede atenderla. Nos hablará una grabación instándonos a pulsar la tecla almohadilla (#) para confirmar el inicio de sesión. Tras esto, en el navegador nos confirmarán que se ha verificado correctamente el inicio de sesión.



4. CONFIGURACIÓN MFA TRAS SU ACTIVACIÓN

Esta parte del procedimiento muestra los pasos a seguir en el caso de que ya esté habilitado el uso de MFA para su usuario pero no haya realizado la configuración de los métodos previamente. En este caso, el sistema le obligará a configurarlo tras introducir la contraseña.

1. Al acceder a cualquier aplicación de Office365, ya sea correo electrónico, Teams, OneDrive... , tras introducir nuestras credenciales nos aparecerá un mensaje indicando que se necesita más información para garantizar la seguridad de la cuenta:



2. Nos aparecerá una pantalla recomendando la descarga de la aplicación móvil “Microsoft Authenticator”. Si no lo tuviéramos instalado en nuestro dispositivo móvil, deberíamos instalarlo antes de continuar. Pulsamos “Siguiente” hasta que aparezca un código QR.

Garantizar la seguridad de la cuenta

Su organización requiere que configure los siguientes métodos para verificar su identidad.

Microsoft Authenticator

Para comenzar, obtenga la aplicación.



En el teléfono, instale la aplicación Microsoft Authenticator. [Descargar ahora](#)

Después de instalar la aplicación Microsoft Authenticator en su dispositivo, elija "Siguiente".

[Siguiente](#)

Garantizar la seguridad de la cuenta

Su organización requiere que configure los siguientes métodos para verificar su identidad.

Microsoft Authenticator

Digitalización del código QR



Use la aplicación Microsoft Authenticator para escanear el código QR. Así, la aplicación Microsoft Authenticator y la cuenta quedarán emparejadas.

Después de escanear el código QR, elija "Siguiente".

[Siguiente](#)

Garantizar la seguridad de la cuenta

Su organización requiere que configure los siguientes métodos para verificar su identidad.

Microsoft Authenticator

Configuración de la cuenta



Si se le solicita, permita las notificaciones. Luego, agregue una cuenta y seleccione "Cuenta profesional o educativa".

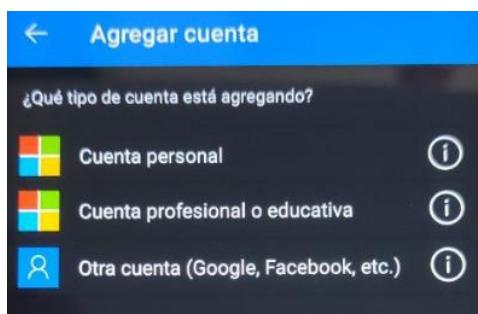
[Atrás](#) [Siguiente](#)

3. En este momento abriremos la aplicación móvil “*Microsoft Authenticator*” en nuestro Smartphone:

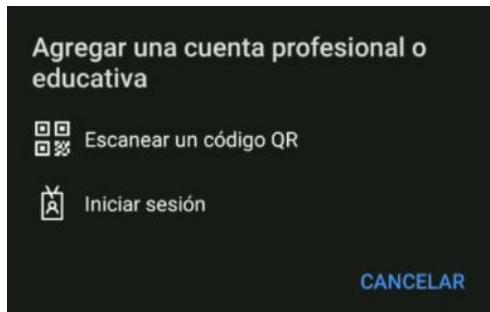
a. En la parte superior pulsaremos en el icono (+) para agregar una nueva cuenta



b. Seleccionaremos la opción “Cuenta profesional o educativa”

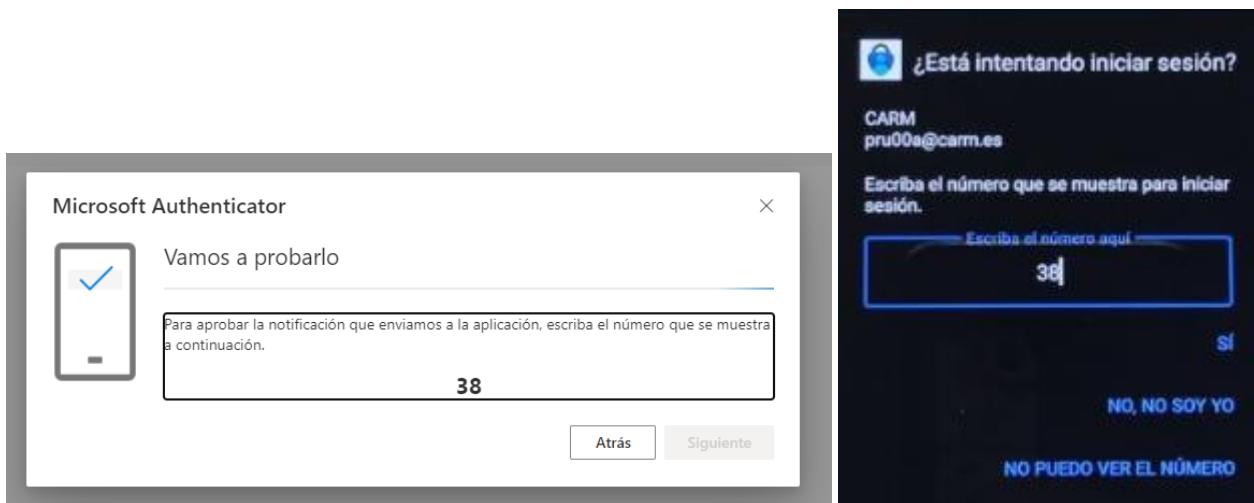


c. Elegiremos la opción de “Escanear un código QR”



d. Apuntaremos con el visor de la cámara hacia el código QR que nos han facilitado en el paso anterior. Nuestra cuenta quedará añadida en la aplicación.

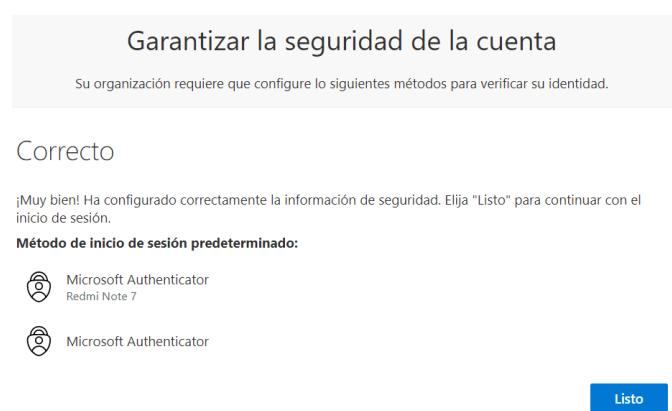
4. De vuelta a la pantalla del ordenador, pulsamos “**Siguiente**” en la ventana que nos muestra el código QR. Se nos propone ahora hacer una prueba de funcionamiento. Recibiremos una notificación en el móvil y al abrirla se nos solicitará un código. Debemos introducir el que se muestra en la pantalla del ordenador y pulsar en “**Sí**”



5. Acto seguido se mostrará en el ordenador una notificación verificando que ha aprobado correctamente el inicio de sesión en el móvil. Pulsamos “**Siguiente**”.



6. Finalmente nos mostrará un mensaje de confirmación acerca de la configuración que acabamos de realizar. Pulsaremos en “**Listo**” para finalizar.



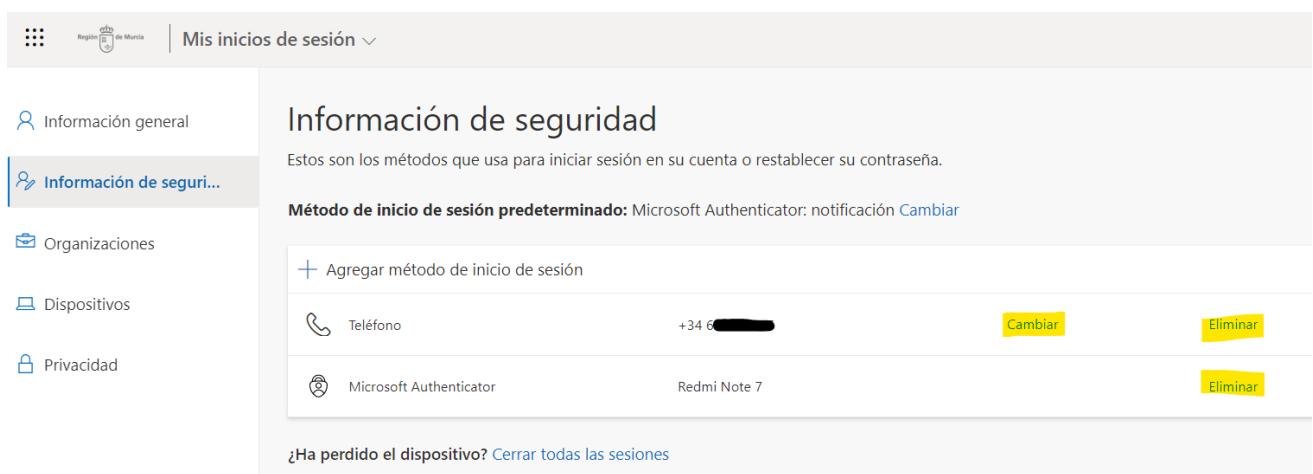
NOTA: Se recomienda encarecidamente la configuración de un segundo método de verificación, ya que en caso de imposibilidad de usar el primero, tengamos otra opción para validar nuestro inicio de sesión.

7. Si desea configurar un segundo método de validación consulte el punto "[3. Añadir un segundo método de verificación](#)"

5. ELIMINAR O MODIFICAR UN MÉTODO DE INICIO DE SESIÓN

En caso de que cambiemos de dispositivo móvil o de número de teléfono, deberemos acceder las opciones de seguridad de nuestra cuenta M365 para modificar o eliminar los métodos que teníamos configurados.

Siga los pasos indicados en el punto "[1. Acceso a las opciones de seguridad de nuestra cuenta M365](#)" y para modificar o eliminar los métodos que tenía configurados.



Información de seguridad

Estos son los métodos que usa para iniciar sesión en su cuenta o restablecer su contraseña.

Método de inicio de sesión predeterminado: Microsoft Authenticator: notificación [Cambiar](#)

[Agregar método de inicio de sesión](#)

| Método | Detalles | Opciones |
|-------------------------|------------------|--|
| Teléfono | +34 6 [REDACTED] | Cambiar Eliminar |
| Microsoft Authenticator | Redmi Note 7 | Eliminar |

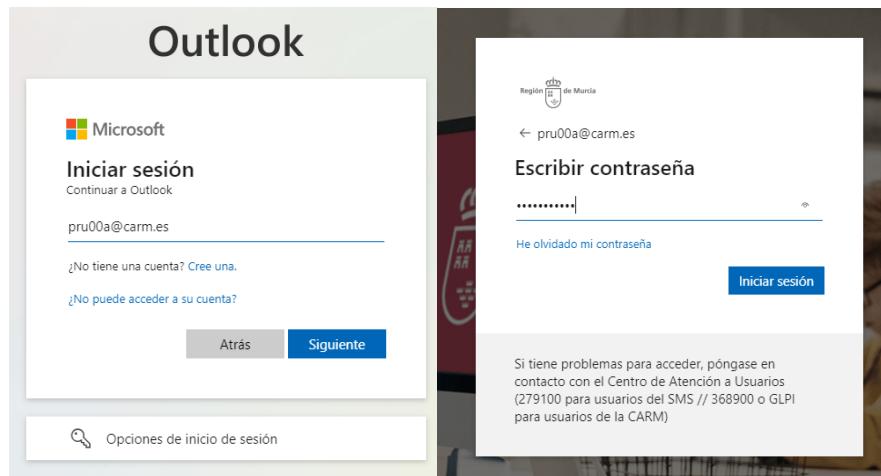
¿Ha perdido el dispositivo? [Cerrar todas las sesiones](#)

Recuerde que se recomienda encarecidamente la configuración de un segundo método de verificación, ya que en caso de imposibilidad de usar el primero, tengamos otra opción para validar nuestro inicio de sesión. En caso de que eliminan un método, asegúrese de introducir otro alternativo.

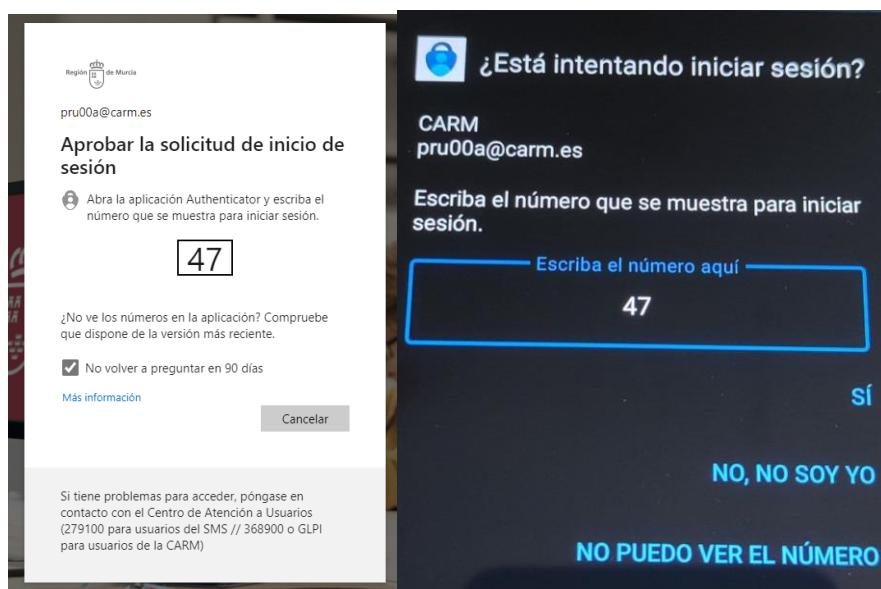
6. INICIO DE SESIÓN CON MFA EN APLICACIONES DE OFFICE 365

Cuando intentemos acceder a un servicio de Office 365 (correo, Teams, One Drive...) desde fuera de la red corporativa se nos solicitará a partir de ahora, además de nuestro usuario y contraseña, confirmación mediante el método MFA configurado previamente.

1. En primer lugar se solicitará usuario y contraseña.



2. En la siguiente pantalla nos indicarán un código de 2 dígitos y al mismo tiempo recibiremos una notificación en el móvil.
3. Al abrir la notificación nos solicitará un código. Deberemos escribir el mismo código que se nos muestra en la pantalla del equipo y pulsaremos "Sí"



4. Acto seguido se iniciará sesión correctamente en la aplicación, en el dispositivo donde intentamos acceder.

7. PROBLEMAS FRECUENTES

Estos son algunos problemas que podrían ocurrir tras activar la autenticación Multifactor.

A) He perdido el acceso al móvil y número de teléfono que tengo configurados y no puedo verificar mi identidad

CAUSA:

Ya sea por extravío, robo, avería, podría haber quedado sin acceso a su dispositivo y/o número móvil.

SOLUCIÓN:

Si es usuario de la CARM contacte con el CAU (968 368900) o si es usuario del SMS, contacte con el Centro de Soporte (968 279100) para que pongan una incidencia en su nombre, solicitando que le reseteen los métodos MFA. Cuando se haya realizado, al acceder, volverá a solicitarle de nuevo la configuración de métodos, y deberá seguir los pasos indicados en este manual, sección "[4. CONFIGURACIÓN MFA TRAS SU ACTIVACIÓN](#)".

B) Tengo instaladas aplicaciones de Office 365 en mi dispositivo móvil y han dejado de funcionar.

CAUSA:

La versión de su aplicación móvil no soporta autenticación MFA.

SOLUCIÓN:

Actualice la aplicación, quizás haya una nueva versión que sí sea compatible con MFA.

C) Al aprobar la solicitud de validación de MFA, me indica que no tienen noticias mías

CAUSA:

Ha tardado demasiado tiempo en validar su identidad o no ha recibido la notificación de aprobación

SOLUCIÓN:

Cuando se nos envía la notificación para aprobar el inicio de sesión tenemos un pequeño espacio de tiempo, cercano a un minuto, para valídalos. Si pasa más tiempo, o si no ha recibido la notificación por cualquier motivo, se mostrará ese mensaje. Si pulsa en la opción "**Enviar otra solicitud a la aplicación Microsoft Authenticator**" se reiniciará el proceso, enviando una nueva notificación al móvil y mostrando un código distinto para validar.



pru00a@carm.es

No tenemos noticias suyas

Hemos enviado una solicitud de verificación de la identidad a tu aplicación Microsoft Authenticator, pero no hemos recibido la aprobación a tiempo.
[Ver detalles](#)

[Enviar otra solicitud a la aplicación Microsoft Authenticator](#)