



MFA - Autenticación Multi-factor

Bienvenido

Con este manual queremos ayudarte en la configuración de la aplicación Microsoft Authenticator en tus dispositivos móviles.

1. ¿Qué es MFA?	3
2 . Gestionar nuestros dispositivos (nuevos dispositivos y eliminación de antiguos)	4
2.1 Métodos de autenticación	5
2.1.1 Aplicación de autenticación	6
2.1.2 Teléfono de trabajo	10
2.1.3 Teléfono	12
3. Terminar la configuración	14

1. ¿Qué es MFA?

Habitualmente iniciamos sesión en miles de servicios cloud utilizando un usuario y una contraseña.

- El usuario nos identifica, le dice al sistema o aplicación quienes somos.
- La contraseña nos autentica, es un factor para comprobar que realmente somos quienes decimos ser.

La autenticación Multi-factor(MFA) fortalece la autenticidad al combinar estos dos factores: Lo que sabemos(la contraseña)+ lo que tenemos(nuestro teléfono). Así de simple, ¡y sólo necesitas 5 minutos! Si estás listo, podemos empezar...



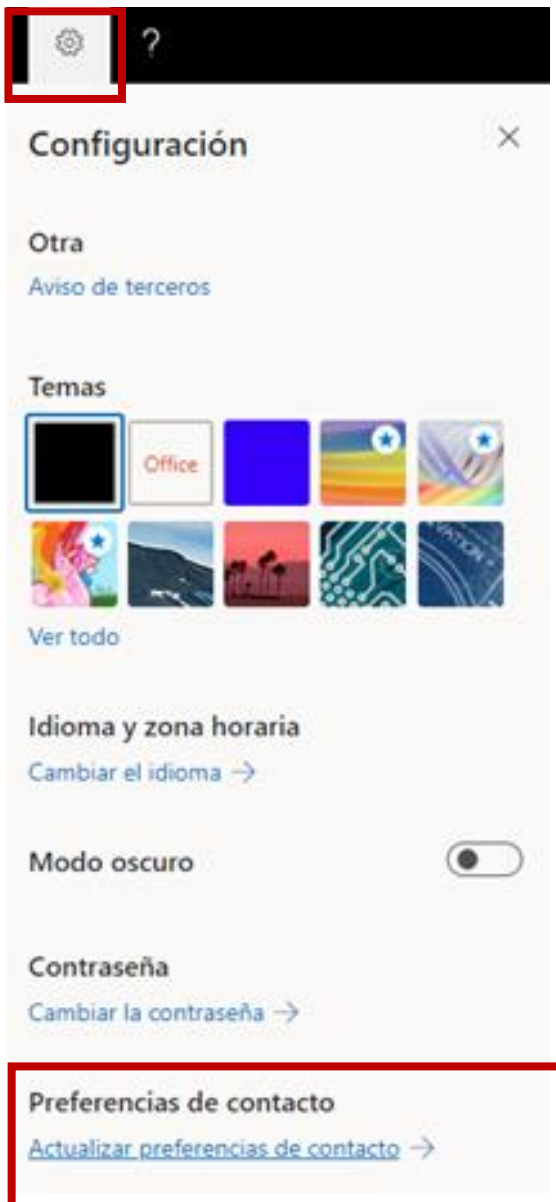
Se recomienda leer todos los pasos previamente, para familiarizarse con el proceso, ya que si se tarda mucho tiempo entre las diversas pantallas, puede darse un timeout y que el proceso no finalice correctamente.

2 . Gestionar nuestros dispositivos (nuevos dispositivos y eliminación de antiguos)

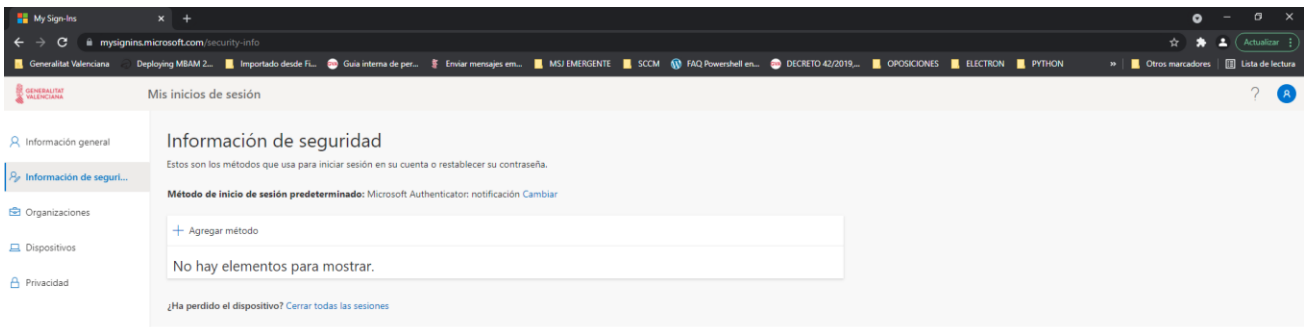
Antes de empezar debemos asegurarnos de **cerrar en el ordenador todas las aplicaciones** que utilizan nuestra cuenta de @gva.es, para que no interfieran en el proceso:

- Word
- Excel
- Outlook
- PowerPoint

Podemos gestionar dispositivos (dar de alta nuevos, eliminar antiguos...) para la activación del MFA desde la web: <https://www.office.com> . Introducimos nuestra cuenta de usuario y después buscaremos el menú de configuración (rueda dentada en el margen superior derecho)

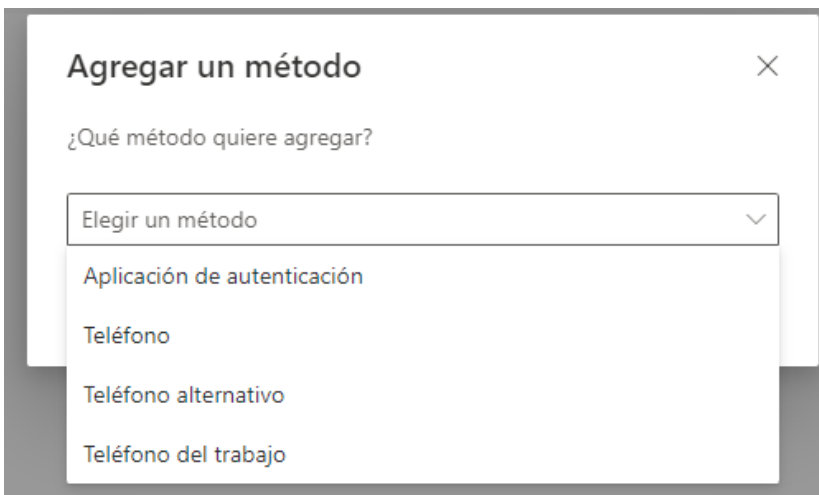


Haremos clic en **Actualizar preferencias de contacto** y después en **Información de seguridad**



2.1 Métodos de autenticación

Necesitaremos definir al menos **DOS MÉTODOS DE AUTENTICACIÓN** (es posible que ya esté definido algún método de inicio)



Aplicación de autenticación: Es una aplicación en la que recibiremos una notificación a través de la aplicación móvil Authenticator para aprobar o rechazar el inicio de sesión.

Teléfono: Realiza una verificación por llamada telefónica de voz automatizada al número de teléfono registrado por el usuario. Para completar el proceso de inicio de sesión, se le pide al usuario que presione # en el teclado.

Teléfono alternativo: Realiza una verificación por llamada telefónica de voz automatizada al número de teléfono registrado por el usuario. Para completar el proceso de inicio de sesión, se le pide al usuario que presione # en el teclado

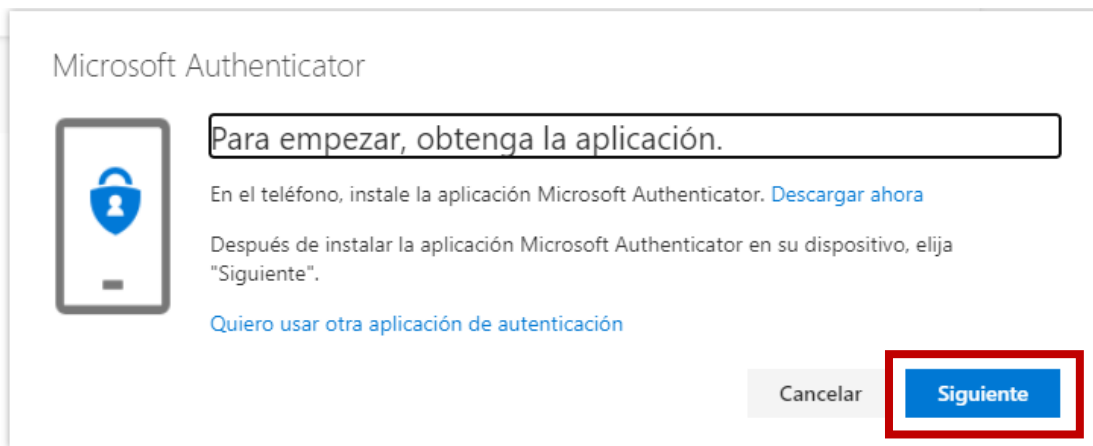
Teléfono de trabajo: Realiza una verificación por llamada telefónica de voz automatizada al número de teléfono de trabajo registrado por el usuario. Para completar el proceso de inicio de sesión, se le pide al usuario que presione # en el teclado.

A continuación explicaremos cómo registrarnos con cada método. Recuerda que hay que registrar mínimo 2 métodos de autenticación.

2.1.1 Aplicación de autenticación

En nuestro caso queremos añadir un nuevo dispositivo. Para ello hay que seleccionar '**Aplicación de autenticación**' -> **Agregar**

Instalaremos la aplicación en nuestro nuevo dispositivo y le daremos a Siguiente



Descargar la app Authenticator

Esta app se vinculará a nuestra cuenta corporativa de Office 365 y nos notificará cada vez que vayamos a iniciar sesión en algún dispositivo desconocido.

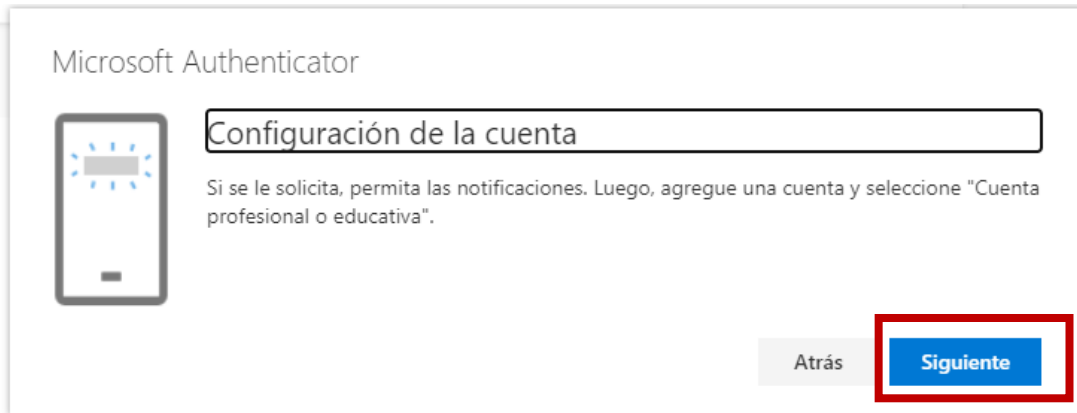
¿Qué smartphone tienes?

Puedes buscarla directamente desde la store de tu smartphone e instalarla. Sino la encuentras también puedes acceder a la página <https://www.microsoft.com/es-es/security/mobile-authenticator-app> .

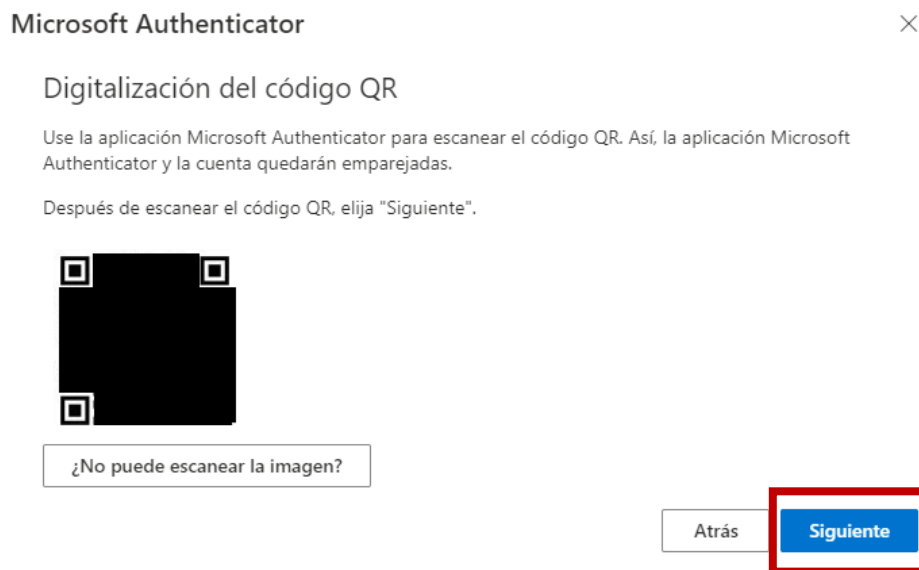
Por favor, comprueba que has instalado correctamente la aplicación de Authenticator en tu smartphone. Deberás ver este icono:



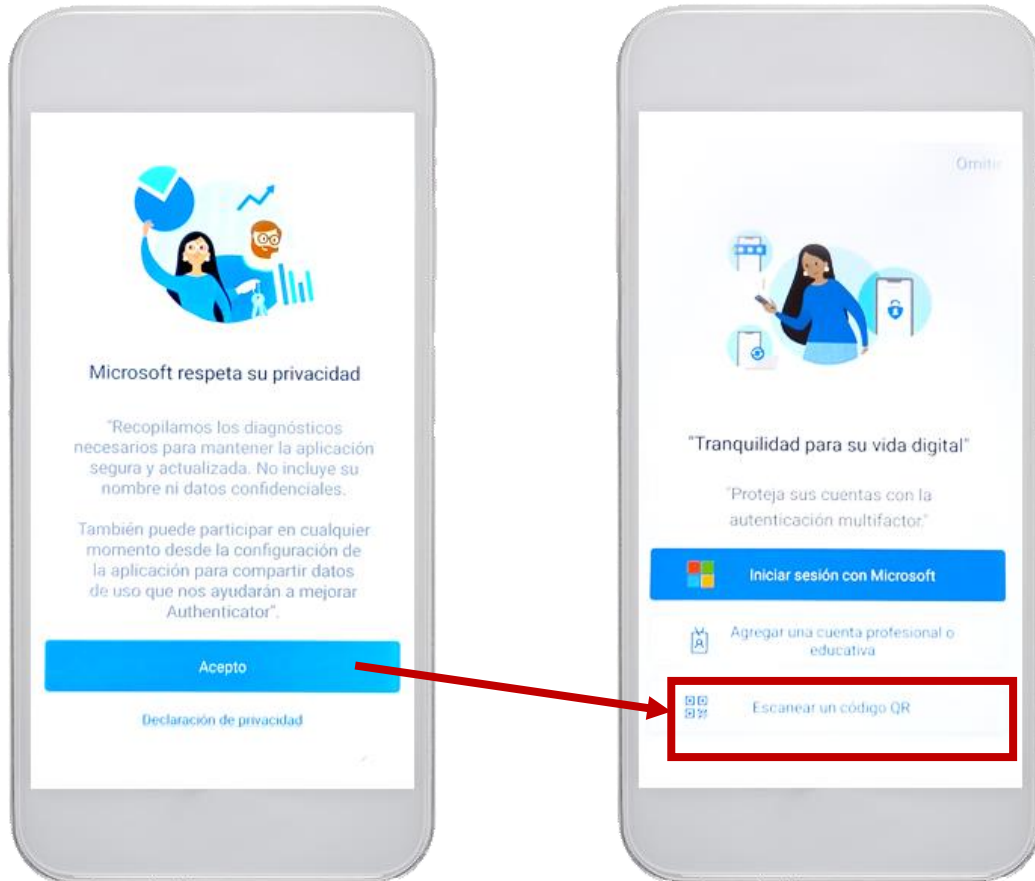
Siguiendo desde nuestro ordenador, nos aparecerá la siguiente pantalla y le daremos a Siguiente



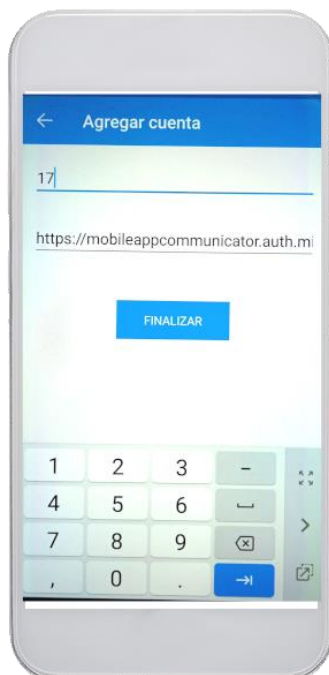
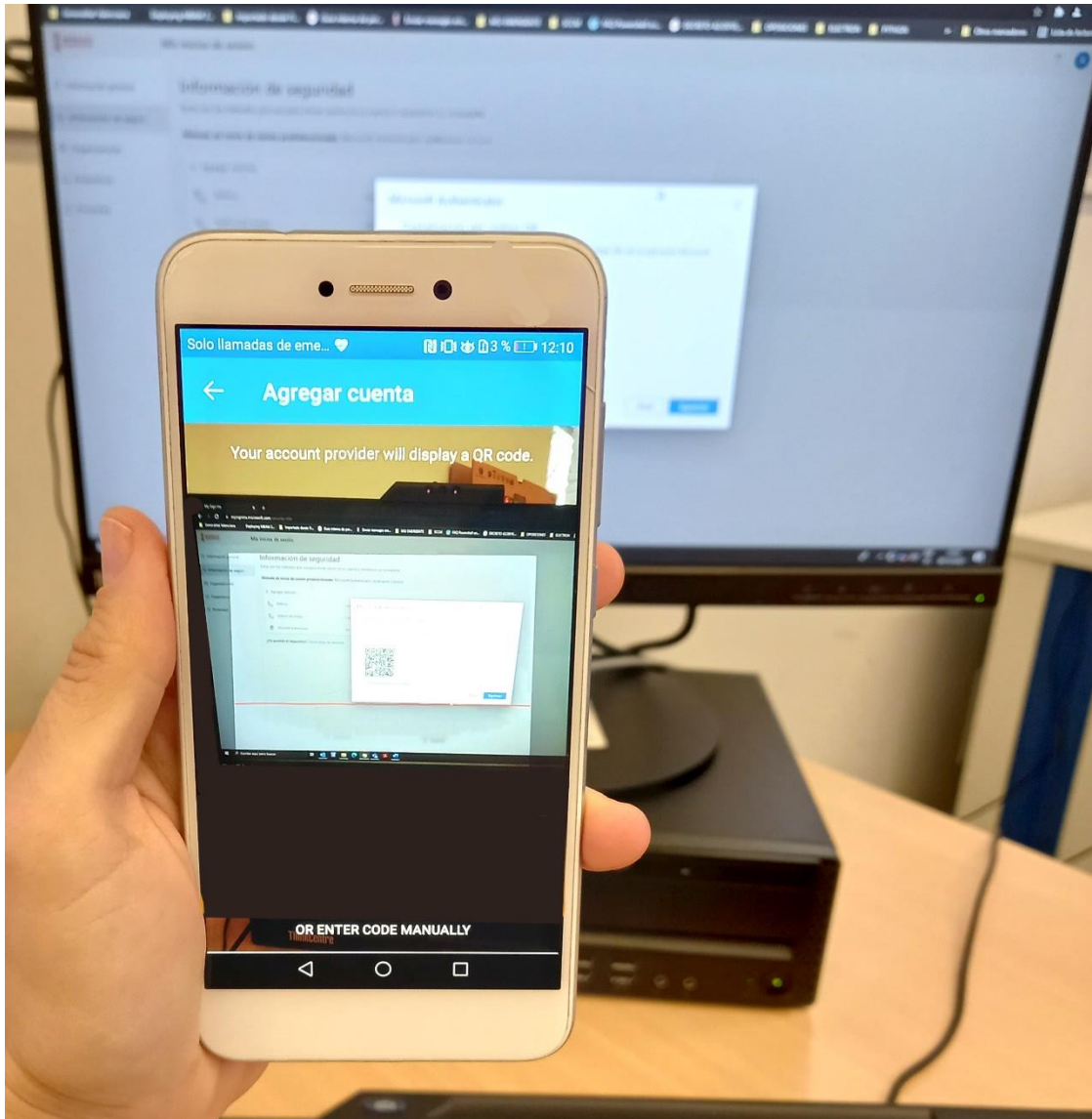
Nos aparecerá una pantalla con un código QR que hay que escanear con la aplicación y nuestro dispositivo.



Abrimos la aplicación Microsoft Authenticator en el smartphone, y lo primero que nos aparecerá será la Declaración de privacidad, le daremos a **Aceptar**.



Elegiremos la opción **“Escanear un código QR”**, y tras escanear el código QR, en el dispositivo indicará: “cuenta creada correctamente.”

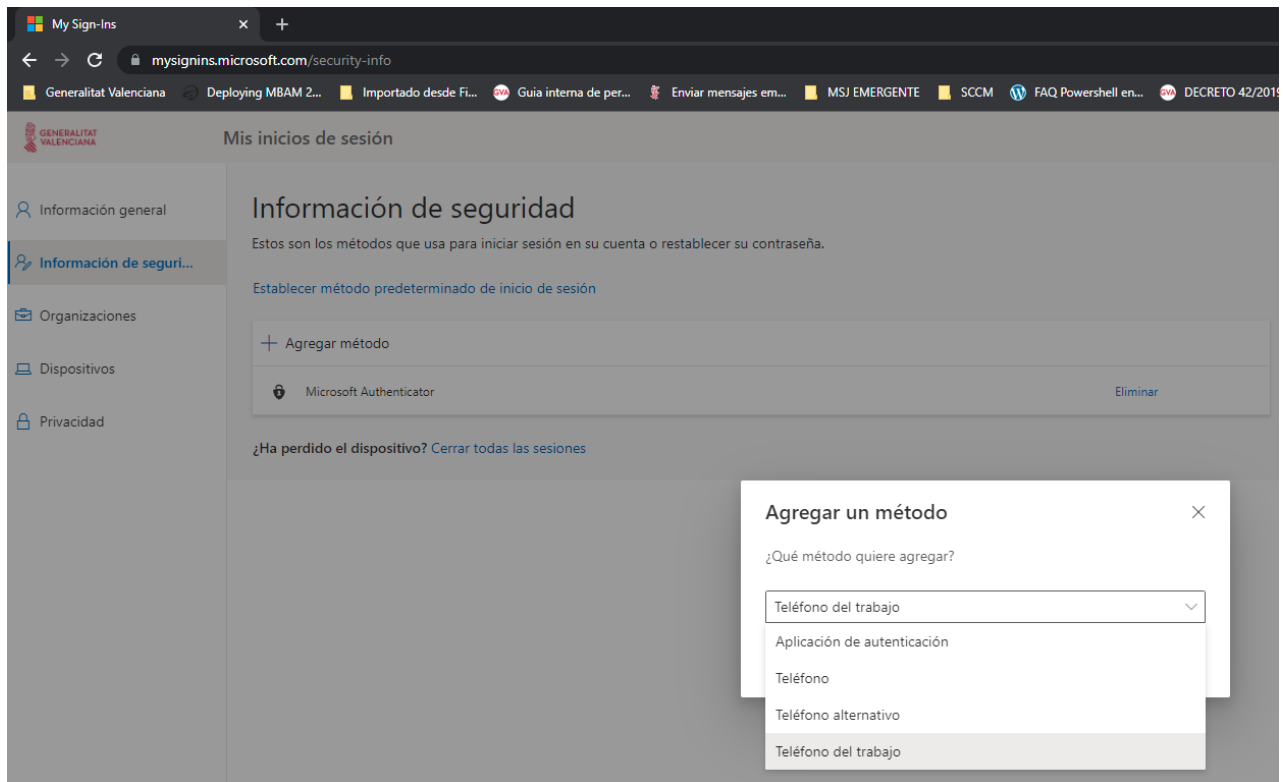


Pulsando sobre Finalizar, habremos agregado la cuenta correctamente.

Vamos a añadir otro método de autenticación por si perdiéramos o nos cambiáramos el móvil poder recuperar nuestra cuenta.

2.1.2 Teléfono de trabajo

Seguiremos los mismos pasos que antes.



Añadiremos **Teléfono de trabajo** y le daremos a Siguiente.

Teléfono

Para verificar su identidad, puede optar por responder a una llamada en su teléfono.

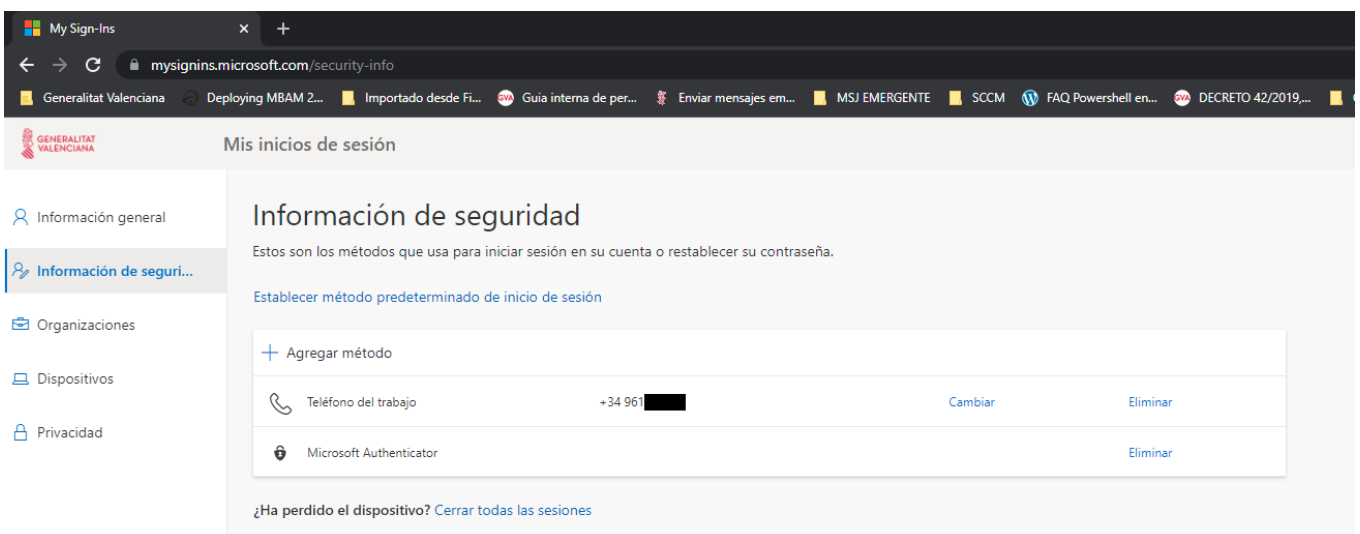
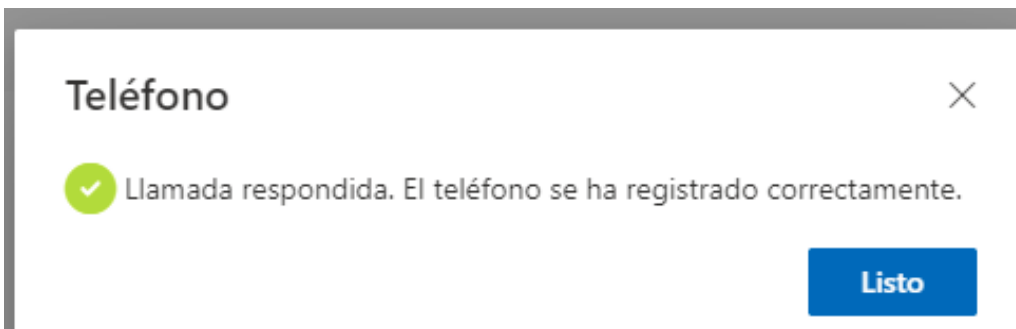
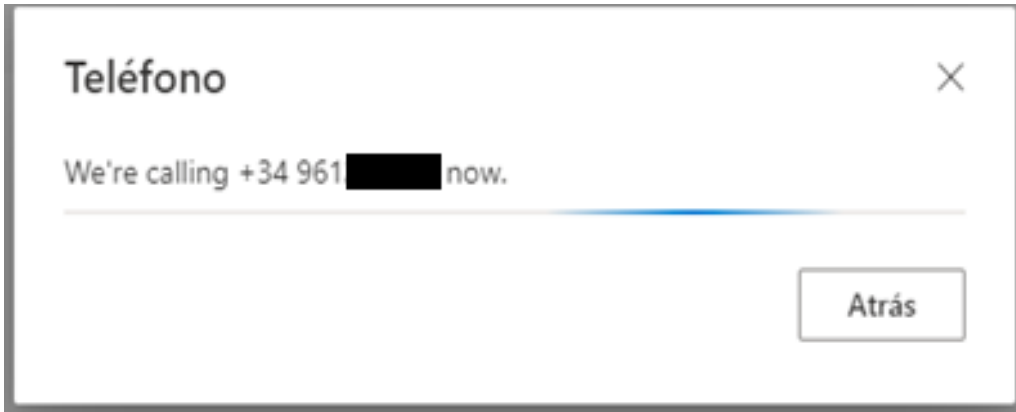
¿Qué número de teléfono quiere usar?

Extensión:

Llámeme

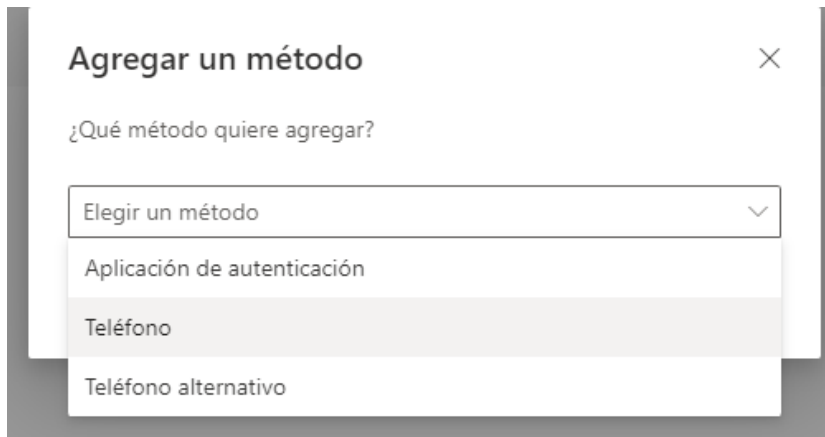
Se pueden aplicar tarifas de datos y mensajes. Si elige Siguiente, se aceptan los [Términos del servicio](#) y la [Declaración de privacidad y cookies](#).

El usuario recibirá una llamada de teléfono del extranjero, suele ser : +1 (855) 330 8653, pero dependiendo del operador es posible que no llegue el identificador de llamada. Hay que seguir las instrucciones de la locución. Normalmente solicita pulsar sobre la tecla #, pero es posible que sea diferente en algunos casos.

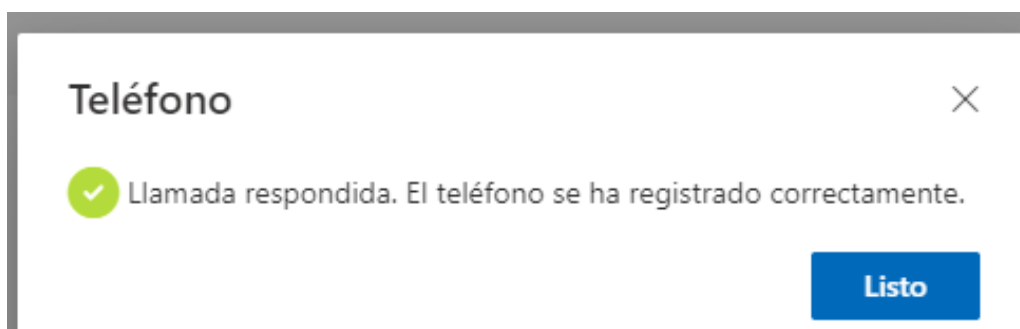


2.1.3 Teléfono

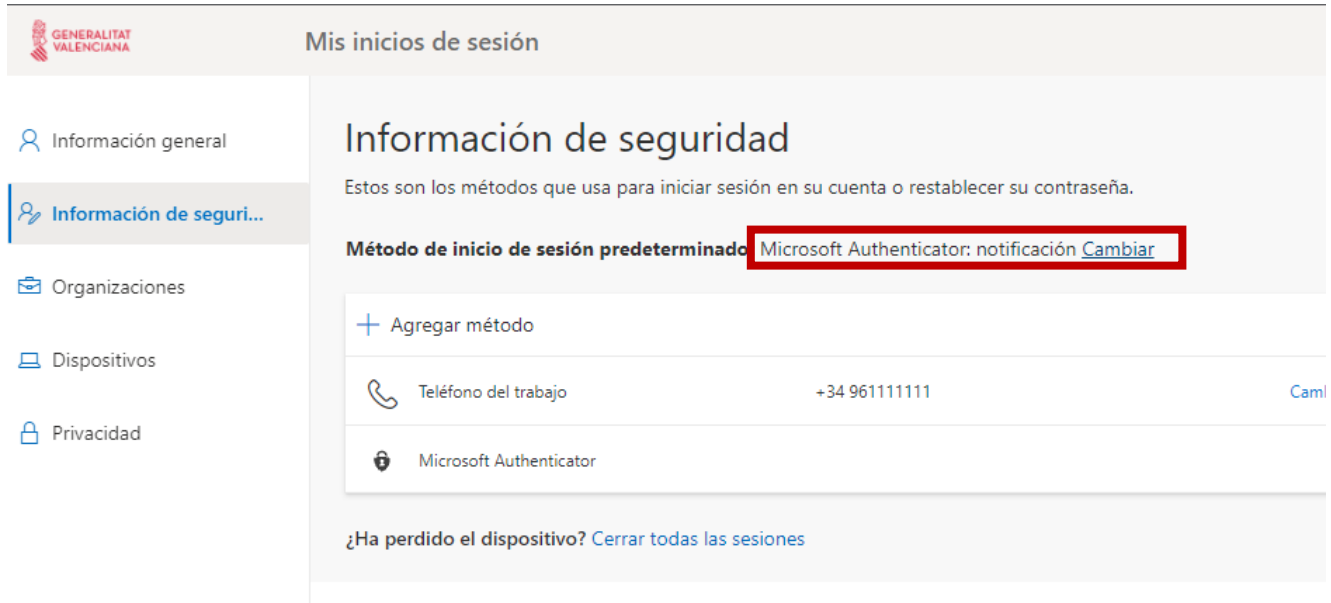
Vamos a añadir un teléfono personal por si queremos acceder desde fuera de la oficina y no disponemos del teléfono de trabajo.



Añadimos el prefijo España y nuestro número telefónico.

Términos del servicio y la [Declaración de privacidad y cookies](#).' At the bottom, there are two buttons: 'Cancelar' and 'Siguiente'." data-bbox="86 419 589 704"/>

Es importante definir el método predeterminado para realizar la doble autenticación, la recomendada por la GVA va a ser la Microsoft Authenticator: notificación.



Mis inicios de sesión

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

Teléfono del trabajo	+34 961111111	Cambiar
Microsoft Authenticator		

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

Cambiar método predeterminado



¿Qué método quiere usar para iniciar sesión?

Microsoft Authenticator: notificación

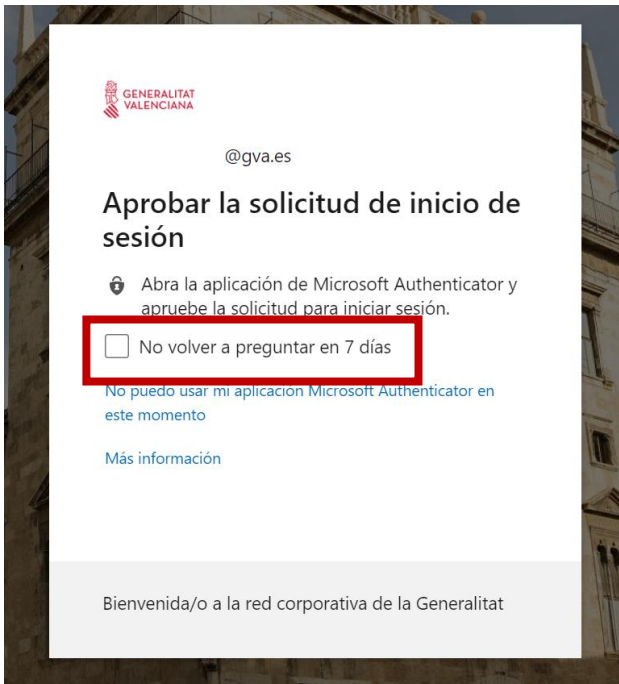
Atrás

Confirmar

3. Terminar la configuración

Para mayor comodidad, recordará los dispositivos de confianza durante 7 días, de ese modo no nos pedirá el multifactor cada vez. Además, si nos conectamos desde **las sedes dentro de la Red Corporativa de la Generalitat Valenciana** tampoco nos pedirá autenticación multi-factor.

Al acceder al portal <https://www.office.com/> desde el exterior, dependiendo del método de inicio de sesión predeterminado que haya elegido el usuario, aparecerá una pantalla como la mostrada. En nuestro caso hemos “Microsoft Authenticator: notificación”,



Nos llegará una notificación que deberemos APROBAR desde la aplicación Microsoft Authenticator.