

Configuración de seguridad 2FA en Office365

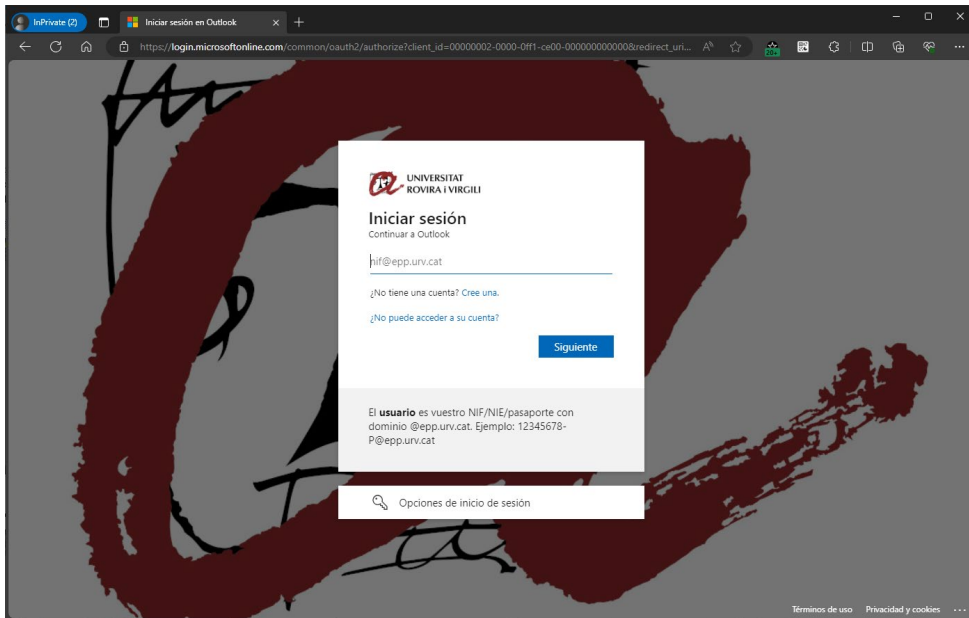
MICROSOFT AUTHENTICATOR
SERVICIO DE RECURSOS INFORMÁTICOS Y TIC v.2

Índice

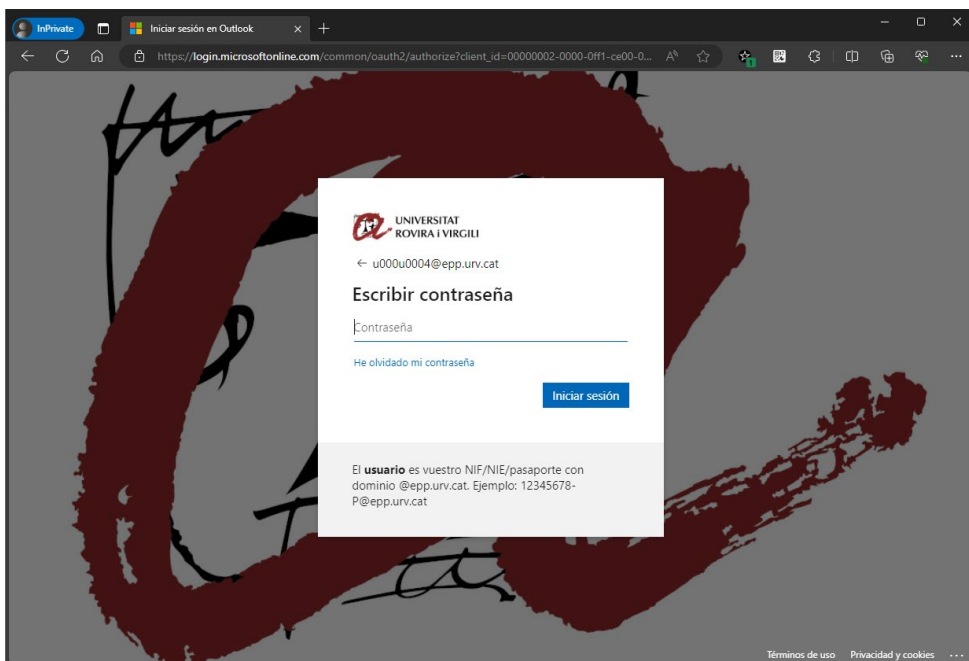
| | |
|--|---|
| Añadir un método | 4 |
| Añadir método «Aplicación de autenticación» en móvil (método preferente) | 5 |
| Instalación Microsoft Authenticator | 5 |
| Configuración Microsoft Authenticator | 6 |

Para configurar el doble factor de autenticación (en adelante, 2FA), tanto si no lo has configurado nunca como si deseas añadir un nuevo método a los existentes, debes entrar en tu cuenta de Office365. Para ello, deberás ir a la página web siguiente:

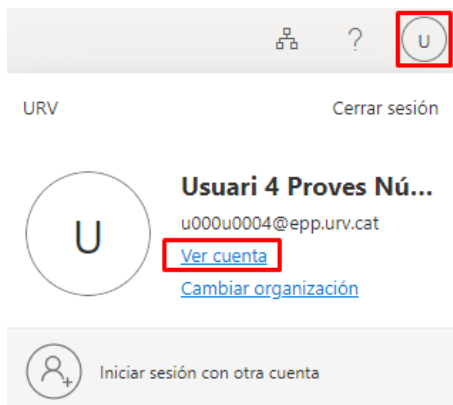
<https://virtual.urv.cat>



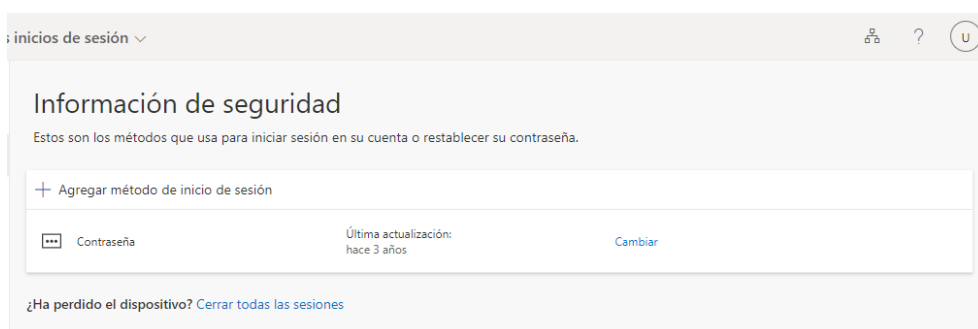
Introduciremos nuestro código de usuario, seguido del dominio @epp.urv.cat, tal y como se nos indica.



Si deseas añadir un nuevo método, o si tu cuenta aún no tiene activado el 2FA, pero quieres tenerlo configurado para cuando se te active, una vez dentro, iremos a la parte derecha superior y sobre el icono seleccionaremos 'Visualiza la cuenta'.



Seleccionamos el apartado 'Información de seguridad'.



Solo os aparecerá un método "Contraseña". Este método representa vuestra clave de acceso.

Nota: A pesar de indicar la opción de "Cambiar", si queréis cambiar la clave de acceso a todos los Servicios Digitales de la Universidad, lo tenéis que hacer dentro del aplicativo de Cambio de Clave: <https://oim.urv.cat/>

IMPORTANTE:

- Si alguna vez has configurado algún método en este punto, te pedirá que utilices el método. Puede que, anteriormente, hayas configurado un número de móvil o teléfono fijo. En este caso, selecciona el método definido y sigue las instrucciones.

Si no reconoce el número de teléfono que aparece, para y abre tique en el SAU, e indica lo que estás haciendo:

- o Acceso al aplicativo: <https://sau.urv.cat/>
 - o Por correo electrónico: cau@urv.cat
- Los teléfonos/ móviles introducidos en este apartado de información de seguridad se usan exclusivamente para la configuración del doble factor de autenticación en la Universidad.

Añadir un método

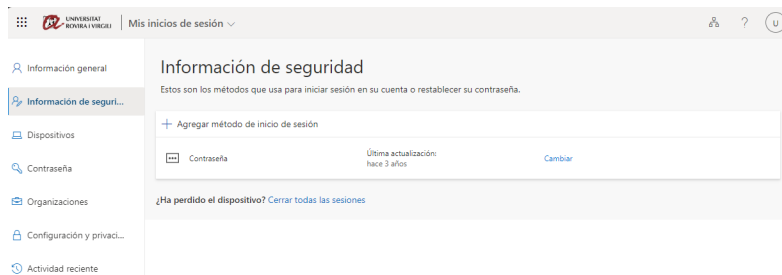
La Universidad recomienda la introducción de más de un método de doble factor y prioriza los siguientes:

- Aplicación de autenticación en móvil (método preferente)
 - Microsoft Authenticator
- Aplicación escritorio (generador de TOTP)
 - 2fast (Windows) / KeePassXC (Mac)
- Número de móvil (SMS) / Teléfono fijo
 - Importante. A partir de octubre de 2023, Microsoft permite la configuración por SMS o teléfono como método secundario y obliga a la configuración de uno de los 2 métodos anteriores.

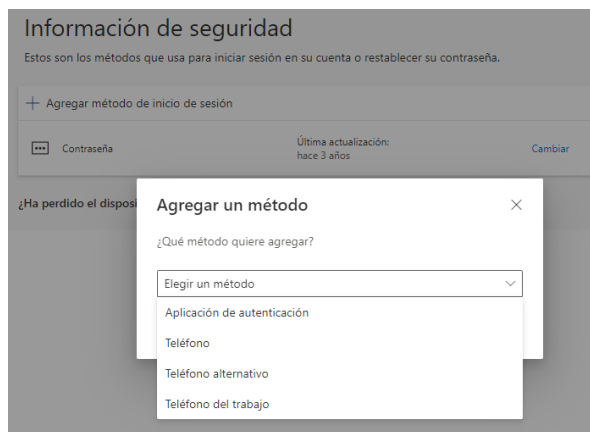
Tal y como indicamos, es importante definir más de un método. De esta forma, si un día no funciona la aplicación del móvil (o nos lo hemos dejado o perdido), podremos aprobar la solicitud mediante una aplicación de escritorio, un SMS o una llamada de teléfono fijo.

Este punto es importante. Recuerda que, si no tienes métodos para aprobar la solicitud, no podrás entrar en la aplicación.

Con el fin de añadir un nuevo método, le damos a 'Añada un método de inicio de sesión'.



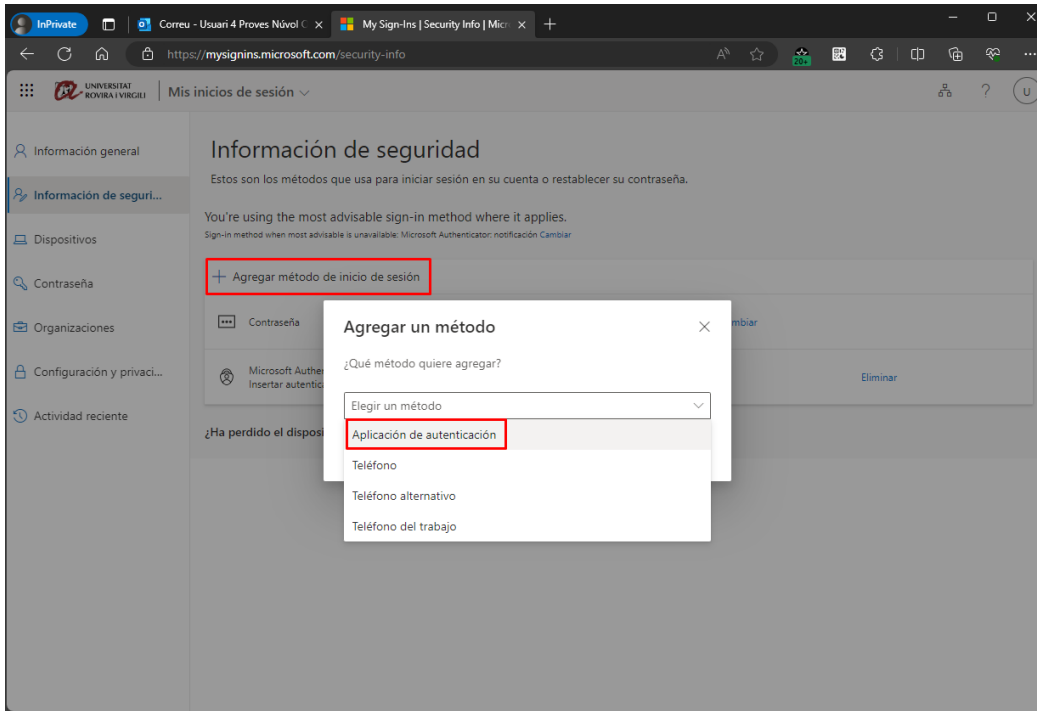
Nos aparece qué método queremos añadir:



Añadir método «Aplicación de autenticación» en móvil (método preferente)

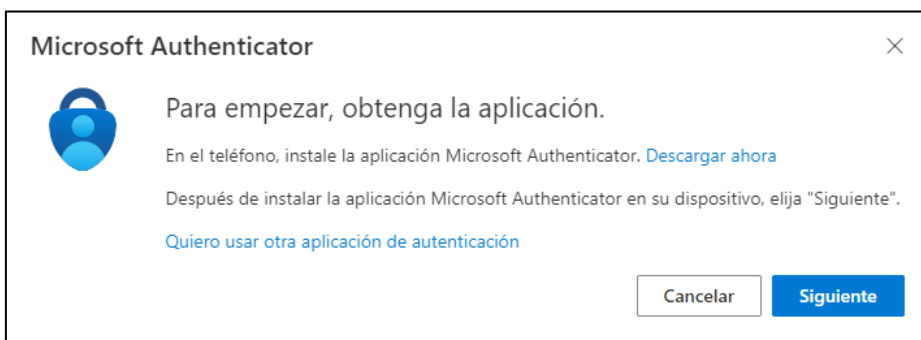
Este método se basa en tener instalado en el móvil una aplicación. Mediante un *push* recibirás el requerimiento de acceso.

Si seleccionamos el método 'Aplicación de autenticación':



Instalación Microsoft Authenticator

Nos aparece el menú para descargar la aplicación del móvil. Si no tenemos la aplicación de Microsoft Authenticator en el teléfono móvil, le damos a 'Descargarlo ahora'.



En la página que se nos abre, tenemos los códigos QR de descarga



Google Play



App Store

Google Play:

<<https://go.microsoft.com/fwlink/p/?LinkID=2168850&clid=0x409&culture=en-us&country=US>>

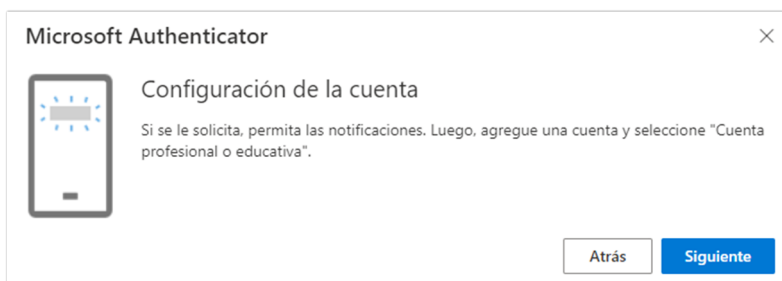
App Store:

<<https://go.microsoft.com/fwlink/p/?LinkID=2168643&clid=0x409&culture=en-us&country=US>>

Nota: Si quisiéramos utilizar Google Authenticator, deberíamos seleccionar 'Quiero utilizar otra aplicación de authenticator' y seguir las instrucciones que se indican.

Configuración Microsoft Authenticator

Cuando tengamos la aplicación en el móvil, le damos a 'Siguiente'



Nos aparecerá la pantalla con un código QR.

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".



¿No puede escanear la imagen?

Atrás

Siguiente

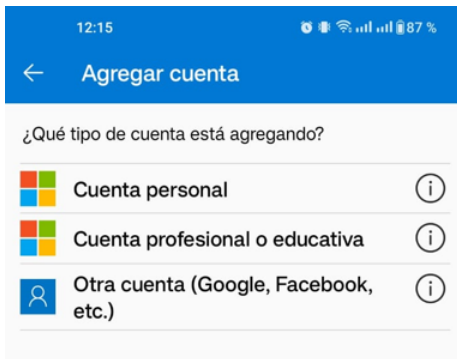
Este código QR es el que deberemos escanear con la aplicación de Microsoft Authenticator de nuestro móvil.

Abrimos la aplicación en el móvil:

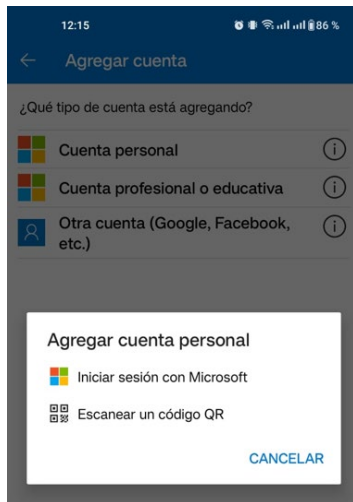
- Le damos al símbolo '+'



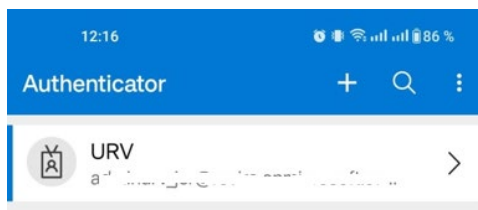
- Seleccionamos 'Cuenta laboral o académica'



- Seleccionamos 'Escanea código QR'



Y, a continuación, escaneamos el código QR de nuestra pantalla del ordenador. Una vez escaneado, ya tenemos este método configurado. En el móvil veremos la cuenta configurada.



A continuación, nos pide probarlo. Muy importante. Debemos dar este paso, si no el método no estará configurado en su totalidad y no podrá utilizarse.

Microsoft Authenticator



Vamos a probarlo

Para aprobar la notificación que enviamos a la aplicación, escriba el número que se muestra a continuación.

17

Atrás

Siguiente

En el móvil debería aparecer la acción de aprobar la solicitud, donde deberemos introducir el número indicado.

Cuando la apruebes, te aparecerá que el proceso se ha realizado correctamente.

Microsoft Authenticator



✔ Notificación aprobada

Atrás

Siguiente

Para finalizar le daremos al botón 'Siguiente'.