

Configuración de seguridad 2FA en Office365

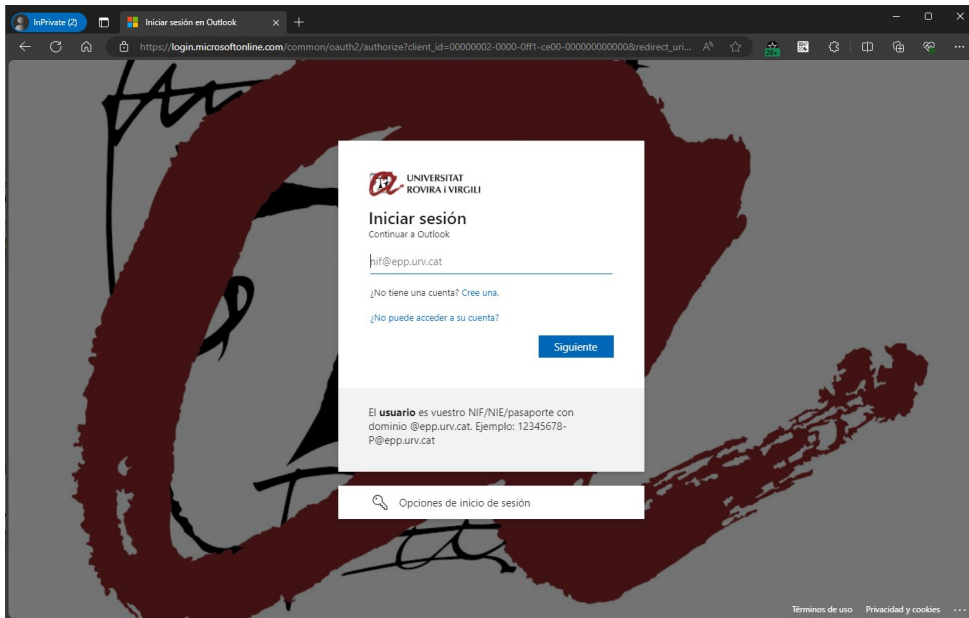
APLICACIÓN ESCRITORIO – 2FAST – WINDOWS
SERVICIO DE RECURSOS INFORMÁTICOS Y TIC v.2

Índice

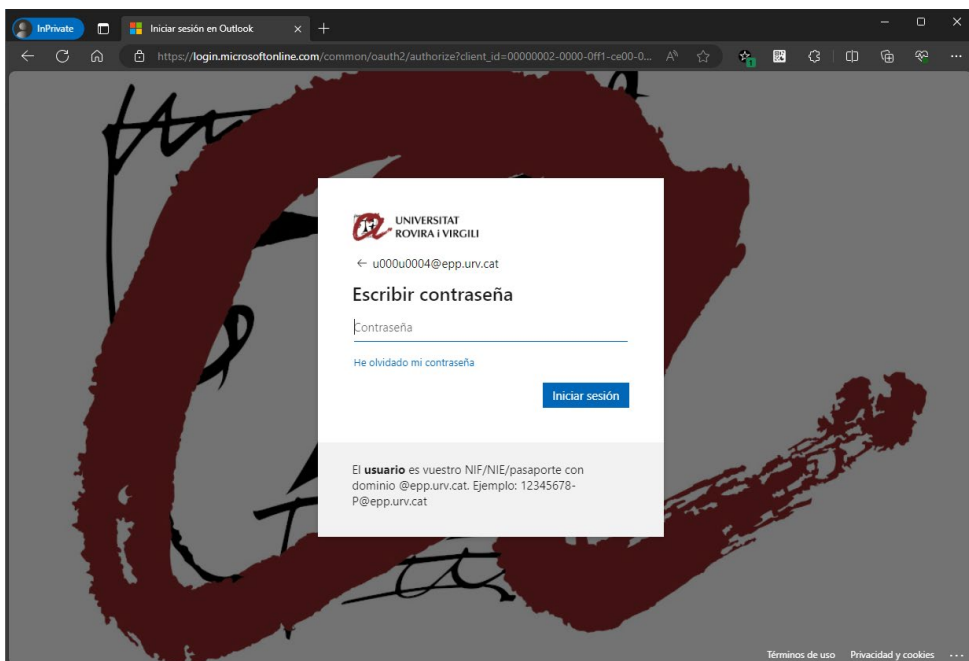
Añadir un método	4
Añadir método «Aplicación escritorio» (generador de TOTP)	5
Instalación en equipos en el dominio Azure (Inicio de sesión con epp.urv.cat)	5
Instalación en equipos en los dominios PAS/PDI o personales.....	7
Configuración de la aplicación	9

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:

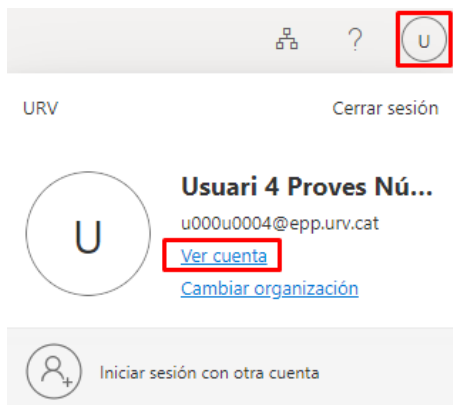
<https://virtual.urv.cat>



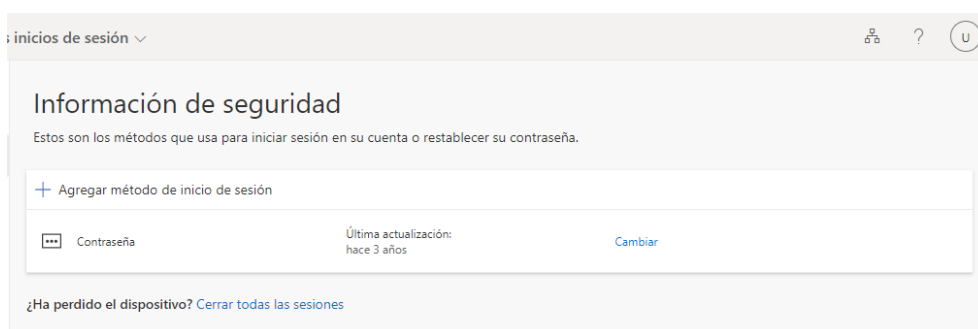
Introduciremos nuestro código de usuario, seguido del dominio @epp.urv.cat, tal y como se nos indica.



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)
 - o Microsoft Authenticator
- Aplicación escritorio (generador de TOTP)
 - o 2fast (Windows) / KeePassXC (Mac)
- Número de móvil (SMS) / Teléfono fijo
 - o 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.

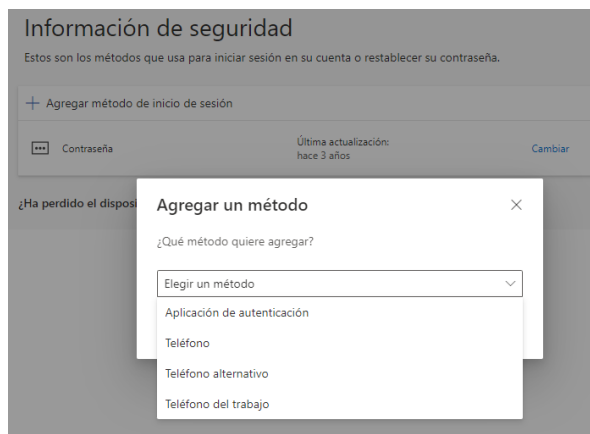
Tal y como indicamos, es importante definir más de un método. De esta forma, si un día no funciona la aplicación del móvil (o nos lo hemos dejado o perdido), podremos aprobar la solicitud mediante una aplicación de escritorio, un SMS o una llamada de teléfono fijo.

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 escritorio» (generador de TOTP)

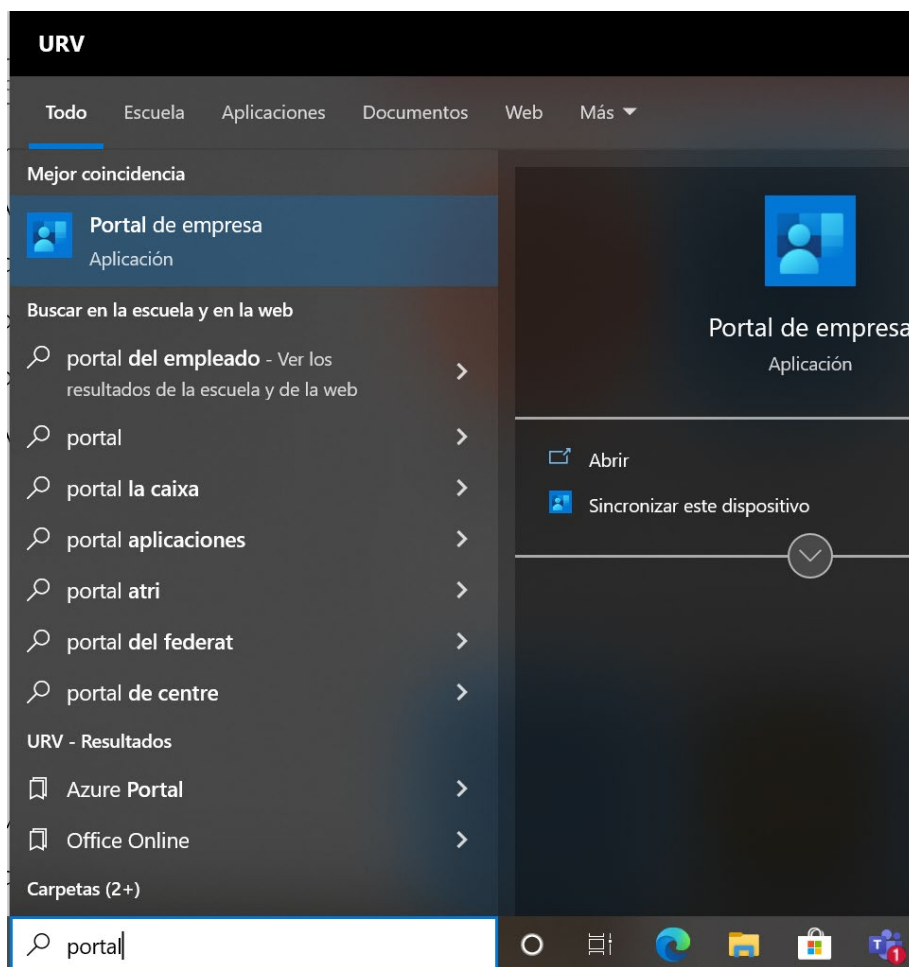
Este método consiste en tener la aplicación que nos permite realizar el doble factor instalado en nuestro ordenador.

Al estar en nuestro ordenador, si no tenemos acceso al ordenador, no podremos realizar el doble factor.

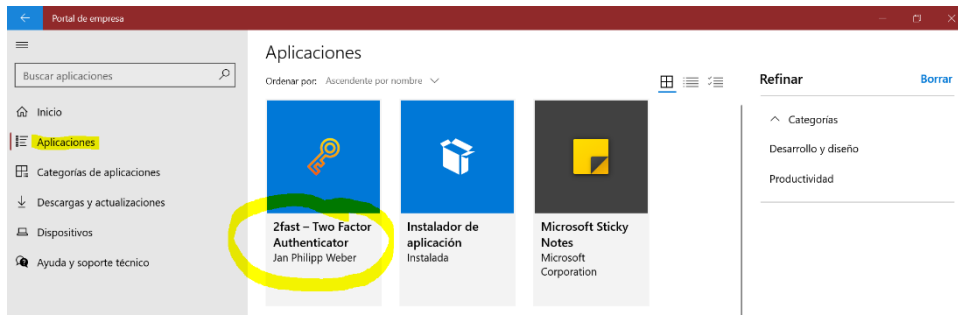
Instalación en equipos en el dominio Azure (Inicio de sesión con epp.urv.cat)

Para instalar la aplicación seguiremos el procedimiento:

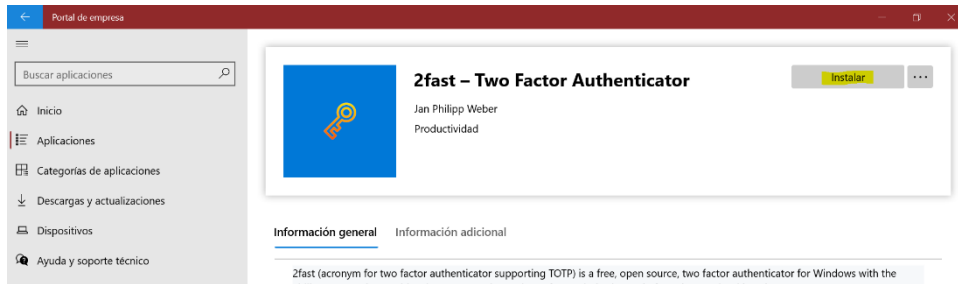
Abriremos la aplicación Menú Inicio -> Portal de empresa/Company portal



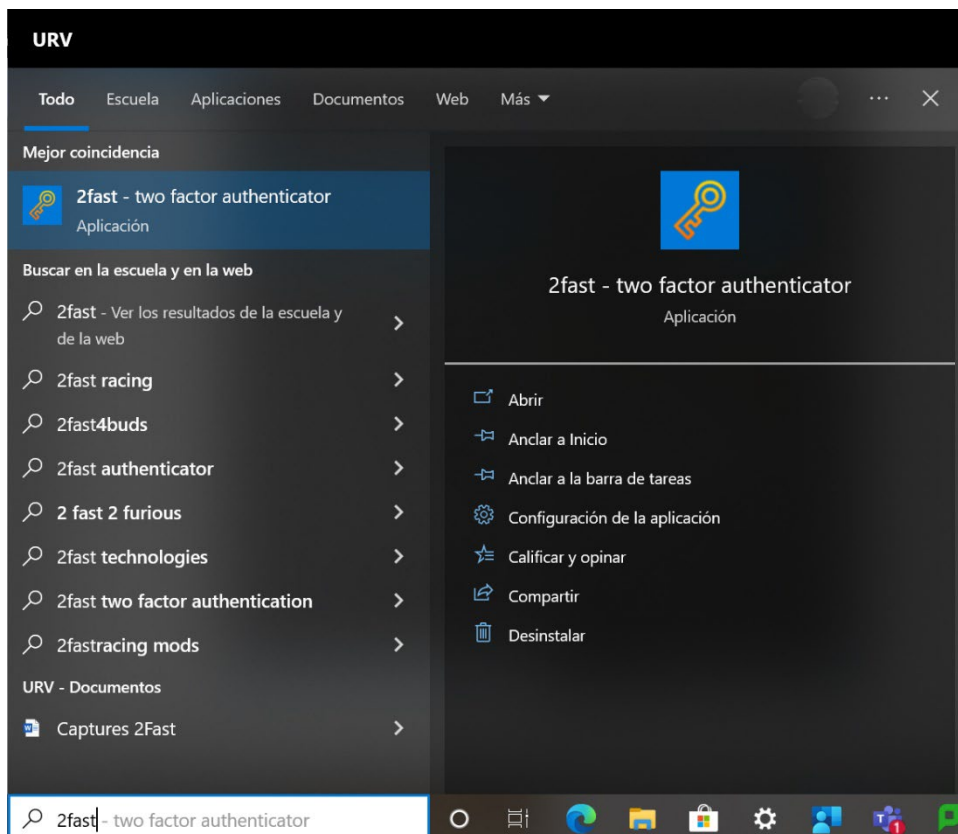
Podemos encontrar la aplicación preparada para instalar en la sección Aplicaciones. Seleccionamos la aplicación *2fast – Two Factor Authenticator*.



Seleccionaremos 'Instalar' para iniciar la instalación.



El software quedará instalado y accesible desde Menú Inicio->2fast - two factor authenticator.

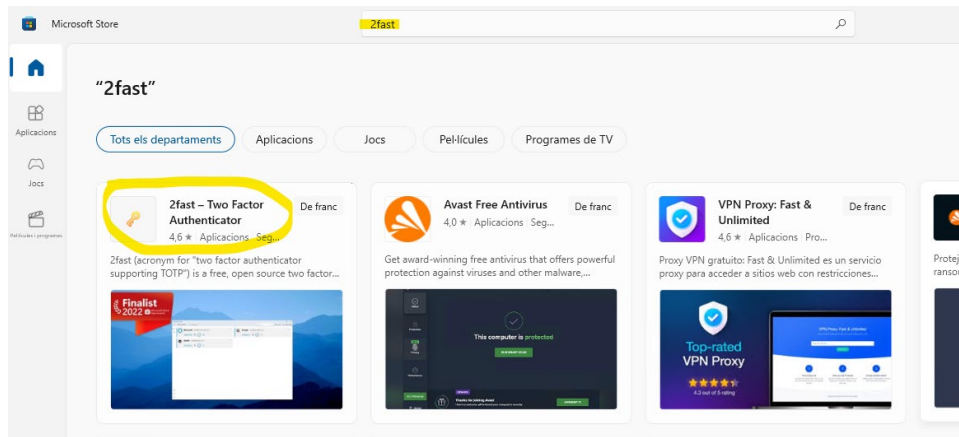


Instalación en equipos en los dominios PAS/PDI o personales

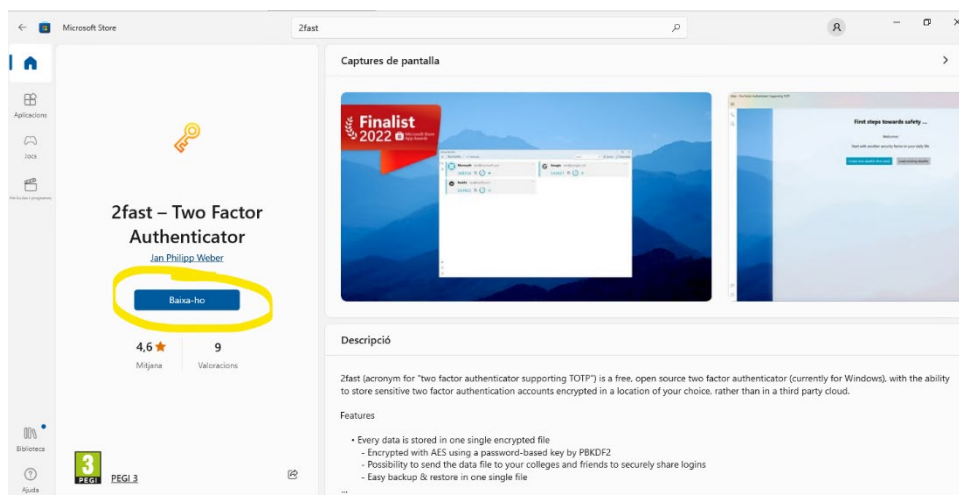
Para instalar la aplicación seguiremos el procedimiento:

Abrimos la aplicación Microsoft Store en Menú Inicio-> Microsoft Store hacemos una búsqueda de *2fast*

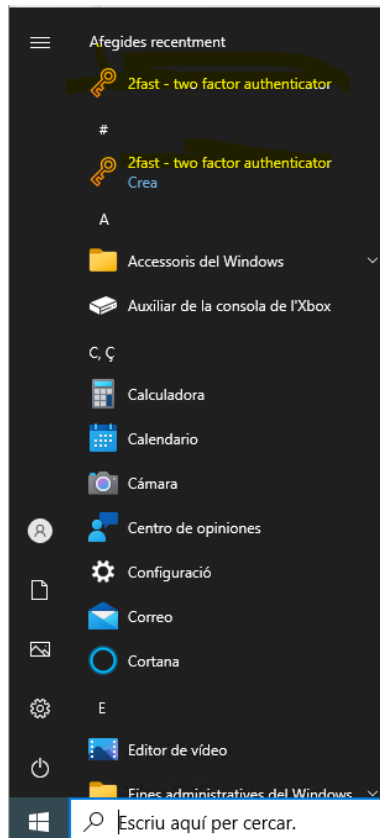
Seleccionamos en la aplicación *2fast – Two Factor Authenticator*



Seleccionamos 'Descargar' para iniciar la instalación.



El *software* quedará instalado y accesible desde *Menú Inicio->2fast – two factor authenticator*

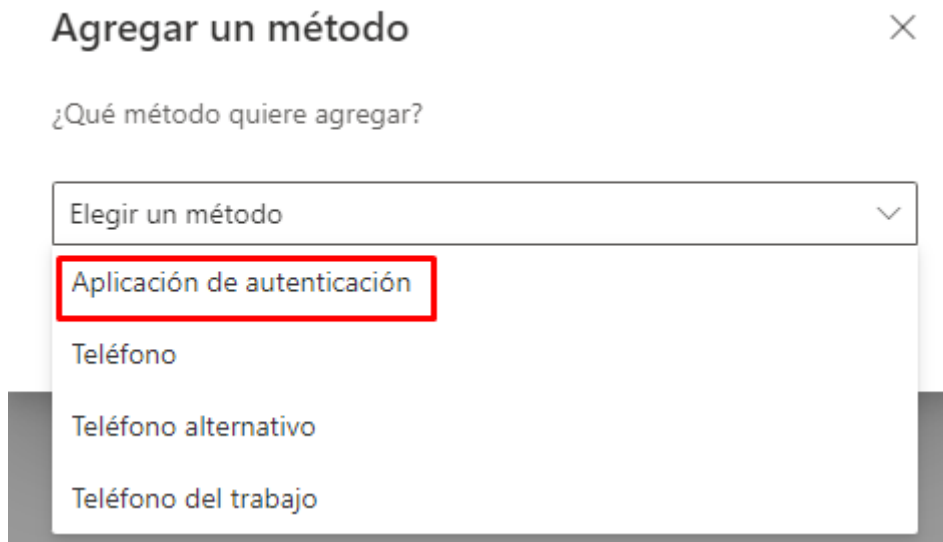


Configuración de la aplicación

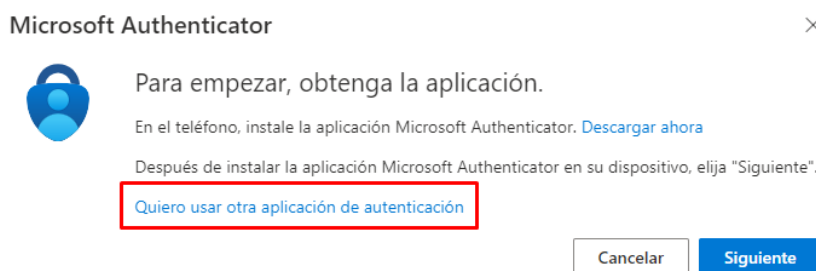
Una vez instalada la aplicación, la abrimos.

Si es la primera vez, nos pedirá crear un archivo de datos y deberemos protegerlo con una contraseña.

Una vez dado el paso anterior, vamos a nuestra cuenta de Office365 (ver 'Añadir método') y vía web seleccionamos la opción 'Aplicación de autenticación'.



Este método es similar al que hemos hecho para añadir Microsoft Authenticator, pero en este caso en lugar de darle a 'Siguiente' le daremos a 'Quiero utilizar otra aplicación de autenticador'.



Una vez le damos a siguiente, se nos muestra el código QR que debemos escanear en la aplicación de escritorio.

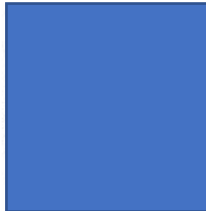
Microsoft Authenticator



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

A continuación, abrimos la aplicación de escritorio que acabamos de instalar:

- Seleccionaremos 'Add account'
- Dentro del menú de *Input type*, seleccionaremos 'Scan Key -QR- code'.
- Nos indicará que en 5 segundos seleccionemos (con el ratón) el área del código QR.
- Lo seleccionamos, y si todo ha ido bien, añadirá la cuenta a nuestro aplicativo.

Una vez dado este paso, ya lo tendremos configurado.

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 [Cambiar](#)

+ Agregar método de inicio de sesión

	Contraseña	Última actualización: hace 3 años	Cambiar
	Aplicación de autenticación Contraseña de un solo uso basada en el tiempo (TC)		Eliminar
	Microsoft Authenticator Insertar autenticación multifactor (MFA)	SM-A505FN	Eliminar

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