



Configuración de la Autenticación Multifactor (MFA)

Versión 1.3 agosto 2023

Contenido

Qué es el MFA	1
Qué es el acceso VPN	1
El MFA en la VPN UC	2
Configurar métodos para el MFA.....	2
Probar VPN UC con MFA	8
Activar passwordless.....	9
Preguntas frecuentes	11

Qué es el MFA

La autenticación multifactor (MFA) es una forma de seguridad que requiere que los usuarios proporcionen más de una forma de autenticación para verificar su identidad al iniciar sesión en un sistema o servicio. Es decir, no es suficiente con saberse una contraseña.

Casi todos los servicios en línea (bancos, redes sociales, compras, ..etc.) han agregado una forma de MFA para que sus cuentas sean más seguras, ya que usar únicamente una contraseña es arriesgado. Es posible que escuche, o ya use, lo que se denomina "Verificación en dos pasos" o "Autenticación multifactor", "Confirmación con la App", pero todos ellos funcionan con el mismo principio.

Una de las ventajas de MFA es que ayuda a proteger a la institución contra vulnerabilidades causadas por la pérdida o el robo de credenciales, que suelen ser la puerta de entrada de ciberataques. El acceso remoto a la red de la institución es un servicio muy sensible por lo que es el primer candidato a activar esta funcionalidad.

Qué es el acceso VPN

La UC proporciona al PAS y el PDI desde hace décadas un sistema de acceso remoto seguro tipo VPN-SSL a la Red UNICAN cuando se está en el exterior. Previamente hay que estar conectado a Internet.

A través de la VPN únicamente pasa el tráfico dirigido a UNICAN, el resto va por su proveedor de Internet. Este sistema está pensado para el acceso a sistemas y servicios internos de la organización que no están accesibles de forma pública desde Internet. No es necesario para aquellos servicios públicos (Correo. Web, Onedrive, ..) que la UC proporciona a sus usuarios.

Si no sabe lo que es y no lo ha usado nunca, es probable que no necesite utilizarlo y por tanto no es necesario que solicite ahora este servicio.

El MFA en la VPN UC

A partir del **1 de agosto de 2023** se activará obligatoriamente el MFA en la VPN UC. Si quiere usarlo a partir de esa fecha, **deberá prepararse antes, registrando uno o más métodos de autenticación multifactor para su cuenta**. En este mismo documento tiene instrucciones sobre cómo hacerlo.

Por tanto, antes de la fecha indicada le recomendamos que:

- Si es usuario habitual de la VPN, no es necesario solicitar el alta ya que esta se hace de oficio.
- Si no es usuario habitual de la VPN (no la ha usado en abril, mayo o junio de 2023) y necesita usar la VPN, solicite su alta en la VPN-MFA escribiendo a [soporte@unican.es](mailto:suporte@unican.es)
- Configure su cuenta con métodos de autenticación MFA, tal y como se indica en este manual.
- Pruebe la VPN MFA antes de que sea obligatoria, tal y como se indica en este manual.

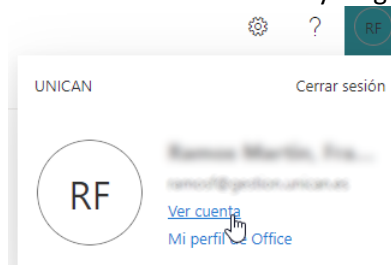
Configurar métodos para el MFA

Para poder usar MFA es necesario primero dar de alta diferentes mecanismos para tener ese segundo factor de autenticación.

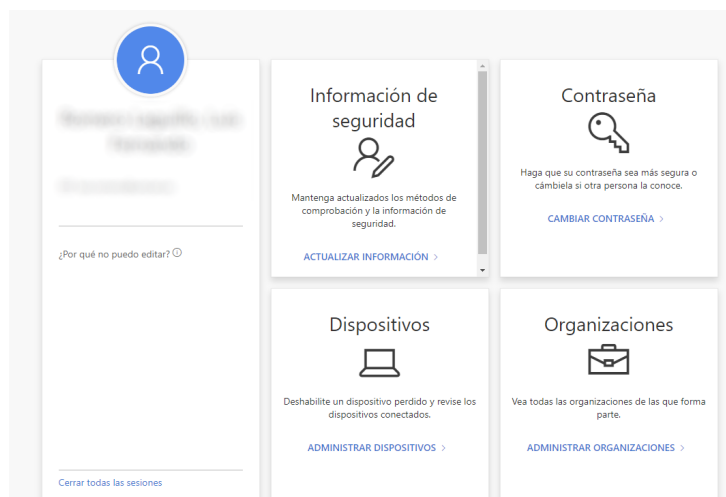
Para ello Iniciamos sesión en la gestión de nuestra cuenta (formato *usuario@gestion.unican.es* o *usuario@unican.es*) en:

<https://myaccount.microsoft.com/>

o si ya estamos validados, pulsamos sobre nuestro icono y elegimos la opción 'Ver cuenta'.



Elegimos la opción de Actualizar información en 'Información de seguridad':



Registro de un número de teléfono

Se recomienda añadir primero un número de teléfono móvil, de esta forma, siempre tendremos la posibilidad de conseguir acceso a nuestra cuenta con un SMS o llamada de teléfono para verificar nuestra identidad.

Puede ver un video tutorial de cómo es el proceso en <https://sdei.unican.es/vpn>.

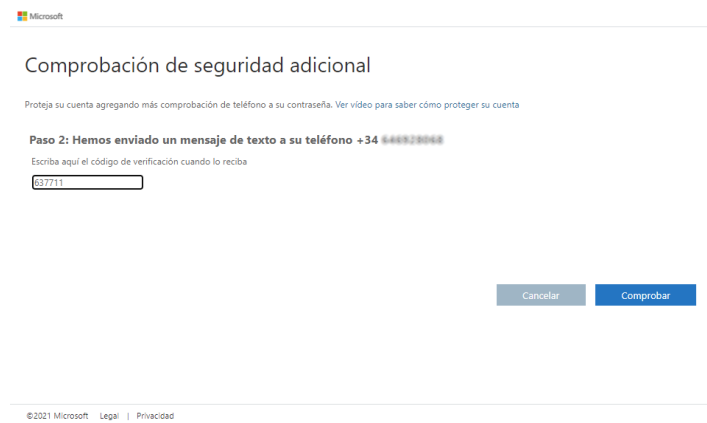


Se puede hacer el registro sólo con la “aplicación de autenticación”, ver más adelante, sin dar un número de teléfono, aunque se recomienda en ese caso tener registrados varios dispositivos. Ver más adelante “Preguntas más frecuentes”.

Por otra parte, al igual que ocurre con los bancos, Microsoft está favoreciendo el uso de la aplicación frente a los SMS ya que estos son más costosos y menos seguros. Es posible que en un futuro el uso de la aplicación sea obligatorio.

Se indica un número de teléfono y si queremos un SMS (si es un móvil) o llamada para verificar que ese teléfono está bajo nuestro control:

Se recibe el SMS de verificación y se valida. También se puede validar mediante una llamada de voz automatizada.



The screenshot shows a Microsoft security verification interface. At the top, it says 'Comprobación de seguridad adicional'. Below that, a message reads: 'Paso 2: Hemos enviado un mensaje de texto a su teléfono +34 646828868'. There is a text input field containing the number '637711'. At the bottom right, there are two buttons: 'Cancelar' and 'Comprobar'. The footer contains '©2021 Microsoft Legal | Privacidad'.

A partir de este momento, ese número será nuestro segundo factor de autenticación.

Registro de la aplicación de autenticación

Recomendamos añadir una aplicación de autenticación, que nos permite completar el proceso de verificación de identidad a través de una notificación que recibimos en el móvil. El uso de la aplicación de autenticación **resulta mucho más cómodo**.

Puede ver un video tutorial de cómo es el proceso en <https://sdei.unican.es/vpn>.



Al igual que ocurre con los bancos, Microsoft está favoreciendo el uso de la aplicación frente a los SMS ya que estos son más costosos y menos seguros. Es posible que en un futuro el uso de la aplicación sea obligatorio.

Con la aplicación nos evitamos dar un número de teléfono, pero en ese caso recomendamos registrarlo en dos dispositivos distintos. Ver más adelante "Preguntas más frecuentes".

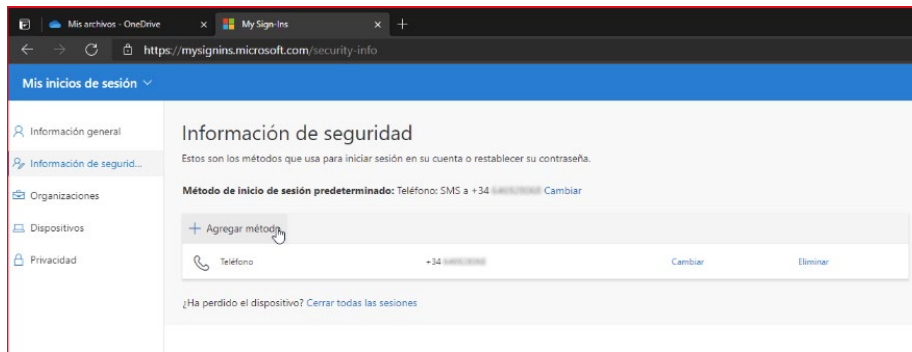
La aplicación se llama **Microsoft Authenticator** y estos son los enlaces de descarga:

Android: <https://play.google.com/store/apps/details?id=com.azure.authenticator>

iOS: <https://apps.apple.com/app/microsoft-authenticator/id983156458>

Para registrar una aplicación, lo añadimos de la misma forma, desde <https://myaccount.microsoft.com/> y la opción de Actualizar información en 'Información de seguridad'.

Agregamos un método de tipo "Aplicación de autenticación":



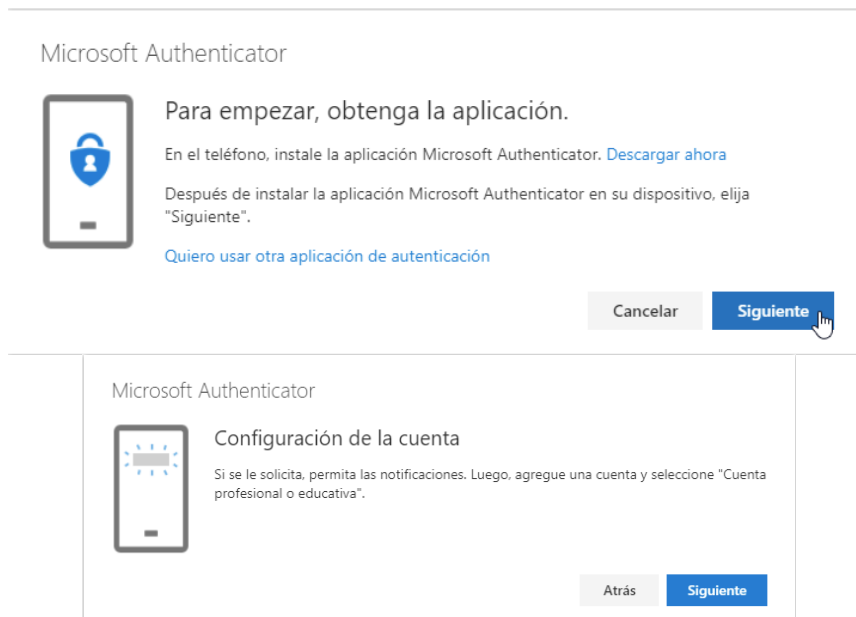
Agregar un método

¿Qué método quiere agregar?

Cancelar

Agregar

Nos informa de los detalles de esta aplicación. Se recomienda haberla instalado a través de los enlaces en este documento.

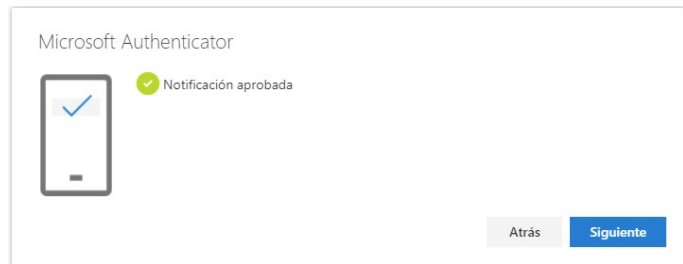


En la aplicación de móvil, se agrega una cuenta de tipo profesional o educativa, eligiendo después la opción de escanear un código QR.

El código QR aparecerá en la pantalla del ordenador en el que comenzamos el proceso:

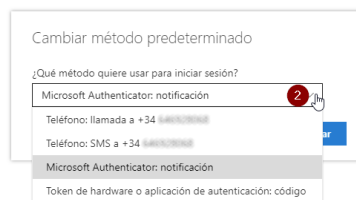


Tras escanearlo y completar los pasos en el móvil, la aplicación queda vinculada a nuestra cuenta.

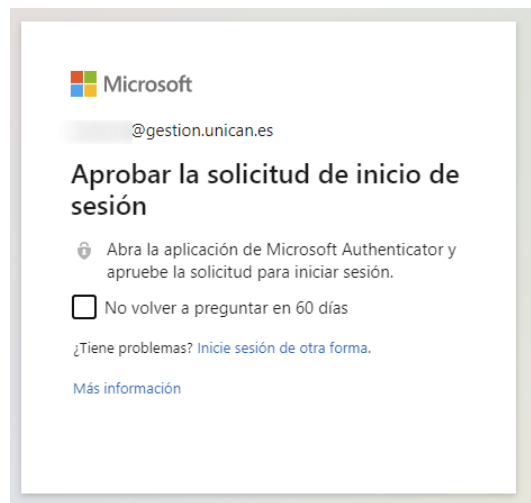


A partir de este momento, en la información de seguridad tenemos dos métodos para verificar nuestra identidad.

Se recomienda cambiar el método predeterminado a "Microsoft Authenticator".

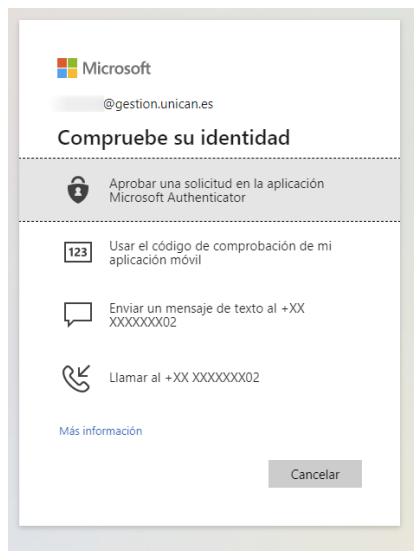


A partir de este momento, cuando inicie sesión en un nuevo dispositivo, tras introducir usuario y contraseña, se solicitará el segundo factor, que, por defecto, será la aplicación de móvil.



¿Qué hago si recibo una solicitud de inicio de sesión que no esperaba? Consulte la sección de preguntas más frecuentes.

En caso de no tenerla disponible, por haber reinstalado el teléfono móvil, se puede pedir el envío de un código o llamada al teléfono registrado.



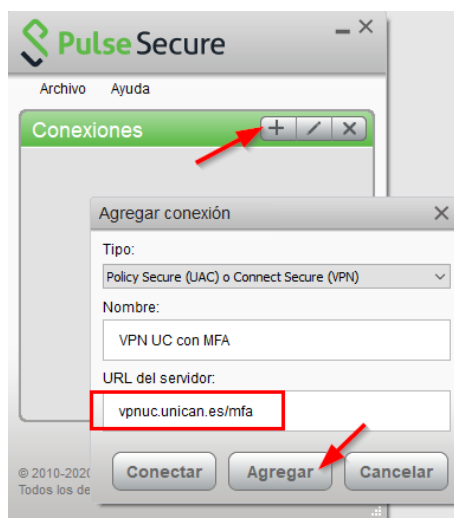
Se recomienda agregar más de un método para MFA. Lo más recomendable son tres: la aplicación Authenticator, el número de móvil habitual y un número de teléfono alternativo por si perdemos el móvil donde tenemos la aplicación y la línea registrada. Ver preguntas más frecuentes.

Probar VPN UC con MFA

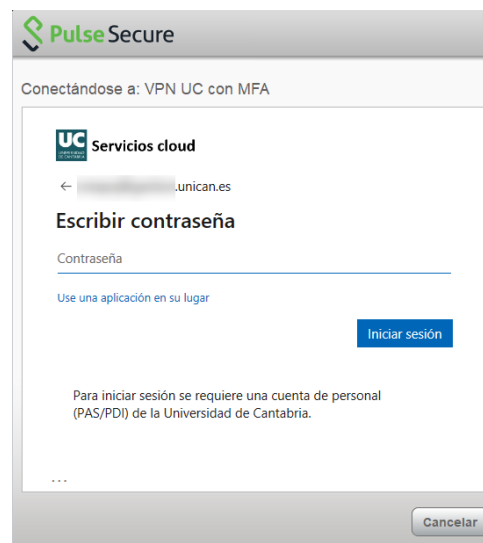
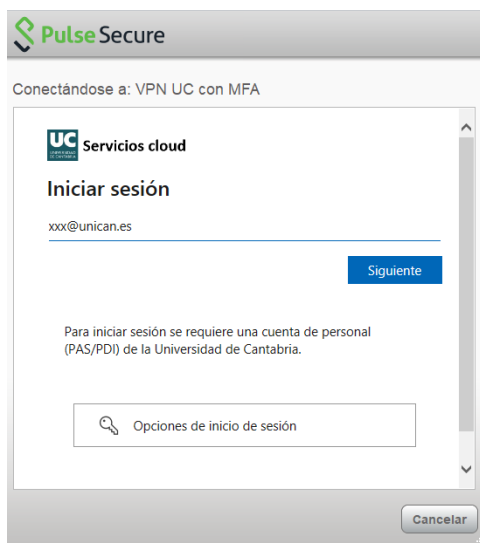
Una vez que tenga registrados los mecanismos de MFA en su cuenta, podrá probarlo añadiendo una nueva entrada en el cliente VPN que tenga como URL de servidor “vpnuc.unican.es/mfa” Para ello deberá seguir las instrucciones de la web sobre la configuración de la VPN UC, pero en vez de vpnuc.unican.es usar vpnuc.unican.es/mfa. También puede entrar directamente en <https://vpnuc.unican.es/mfa>.



Utilice el cliente VPN de Pulse/Ivanti que se puede descargar desde la página del Servicio de informática (buscar VPN) y que es el que se usa habitualmente. **El cliente Pulse que hay en la Microsoft Store no funciona con MFA.**



Al conectarse le saldrán las ventanas de validación. En este caso el segundo factor MFA, el primero es nuestra contraseña, es un código que debe escribir en la aplicación MS Authenticator.





La dirección vpnuc.unican.es/mfa es provisional durante el periodo de transición para realizar las pruebas oportunas. A partir del 1 de agosto de 2023 en la URL original vpnuc.unican.es también se pedirá MFA por lo que será indistinto usar una u otra.

Si le resulta más cómodo puede activar el password-less sign-in en la aplicación Authenticator para así no usar la contraseña del móvil, tal y como se explica a continuación.

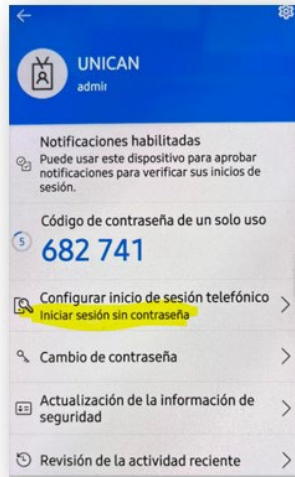
Activar passwordless

El passwordless sign-in (Inicio de sesión sin contraseña) es un mecanismo opcional para autenticarse sin necesidad de escribir nuestra contraseña. Tan solo se responde a un “desafío” (un número aleatorio de dos cifras) desde el móvil autorizado.

Puede ver un video tutorial de cómo es el proceso en <https://sdei.unican.es/vpn>.

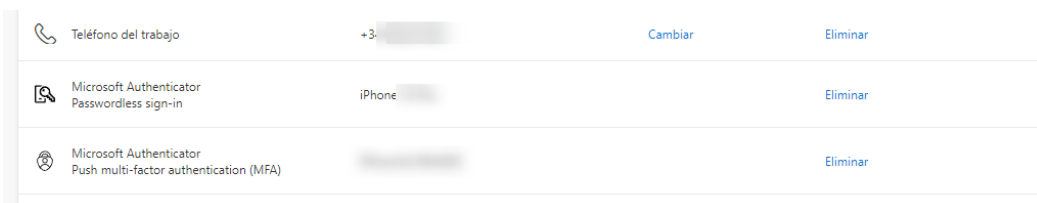
Se trata de un mecanismo seguro, ya que debemos usar el dispositivo y aprobar el inicio de sesión con autenticación biométrica (huella o reconocimiento facial) del dispositivo. El multifactor se logra con nuestra huella/cara (algo que somos) y nuestro dispositivo (algo que tenemos). No usamos la contraseña.

Para activarlo, una vez que tenemos registrada la aplicación Microsoft Authenticator debemos entrar en Microsoft Authenticator, seleccionar la cuenta registrada, seleccionar “Habilitar inicio de sesión en el teléfono”

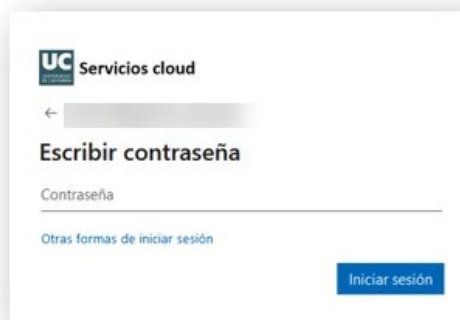


y seguir las instrucciones en pantalla para terminar de registrar la cuenta para el inicio de sesión en el teléfono sin contraseña.

Una vez activado si entramos en <https://myaccount.microsoft.com/> y vamos a la opción de Actualizar información en 'Información de seguridad', vemos el dispositivo que está habilitado para passwordless sign-in



Una vez activado el passwordless cuando tratas de validarte en un servicio protegido por MFA (como la VPN UC) en vez de escribir la contraseña, se puede marcar la opción 'Otras formas de iniciar sesión':



Esto nos dará un número que tenemos que introducir en Microsoft Authenticator, a través de la notificación que nos envía al móvil:



Si ya no queremos usar passwordless sign-in debemos, desde la app Authenticator, hacer el paso inverso y “Deshabilitar el inicio de sesión en el teléfono”.

Si no queremos usar passwordless sign-in en ese momento, siempre podemos optar por usar contraseña + desafío MFA.

Preguntas frecuentes

¿Será obligatorio utilizar MFA para el acceso remoto VPN UC?

Sí. El acceso por VPN será siempre mediante MFA. Si no quiere utilizar MFA o no se siente cómodo usándolo, no podrá acceder remotamente a la Red UNICAN, ya que forma parte de las condiciones del servicio.

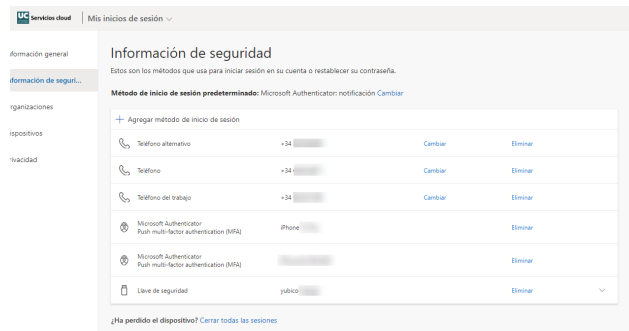
¿Puedo utilizar otro método/programa para acceder remotamente a mis equipos en la Red UNICAN si no quiero usar la VPN UC?

No. El uso de mecanismos alternativos a la VPN UC para acceder remotamente la red corporativa de la Universidad de Cantabria ya **está prohibido por el Reglamento de Uso de recursos TIC** de la UC desde 2008. La vulneración de esta prohibición tiene un carácter **grave** dadas las implicaciones para la institución.

El único mecanismo autorizado para acceder remotamente a la Red UNICAN es mediante la VPN UC. Si cree que tiene algún imperativo técnico para usar otros mecanismos de acceso remoto directo para situaciones específicas, contacte con el Servicio de Informática.

¿Qué métodos para realizar MFA están disponibles?

Puede registrar hasta cinco métodos, que pueden ser: un teléfono fijo (para recibir un código temporal por llamada de voz automatizada), dos números de móvil (para recibir un código temporal por SMS o llamada), llaves de seguridad (tipo Yubico, para passwordless) y aplicaciones de autenticación (Microsoft Authenticator) instaladas en varios dispositivos. Lo importante es que sean dispositivos que están bajo su control personal.



¿Qué método es mejor?

Sin lugar a dudas, lo mejor es usar habitualmente la aplicación de autenticación **Microsoft Authenticator**, pero además registrar al menos otro método alternativo para no quedarse bloqueado. Además, Microsoft Authenticator le permite darse de alta, opcionalmente, en passwordless sign-in (ver instrucciones en este documento).

Por otra parte, al igual que ocurre con los bancos, Microsoft está favoreciendo el uso de la aplicación frente a los SMS ya que estos son más costosos y menos seguros.

No quiero dar mi número de teléfono ¿Necesito obligatoriamente dar mi número de teléfono para usar MFA?

No. No es necesario proporcionar un número de teléfono. Se puede utilizar solo la aplicación (o llaves de seguridad), aunque recomendamos en ese caso tener la aplicación registrada en al menos dos dispositivos distintos para tener dos alternativas de validación MFA.

Si doy mi número de teléfono ¿A quién se lo doy?

Si decide registrar un número de teléfono, se trata de un **acto entre usted y Microsoft** y únicamente a efectos de la prestación del servicio MFA. La Universidad no interviene. No se utiliza para ninguna otra finalidad. Los datos se almacenan en la Unión Europea y Microsoft cumple la legislación española y europea en materia de datos personales (RGPD) y de seguridad para las administraciones públicas (ENS), siendo su representante legal en la Unión Europea Microsoft Ireland Ltd. Para más información consulte la información legal disponible en el sitio de Microsoft.

¿Puedo registrar un número de teléfono fijo, por ejemplo, el del despacho o el de casa?

Sí, pero tengan en cuenta las posibles limitaciones. Puede ser de utilidad como medio de emergencia alternativo por si pierde/desinstala el MS Authenticator, por ejemplo. Pero su limitación es que **solo podrá usarlo si está físicamente donde está la línea fija.**

¿Puedo registrar el número de teléfono del móvil en donde tengo instalada y registrada la aplicación de Microsoft Authenticator?

Sí, pero tenga en cuenta que eso solo le sirve por si hay un problema con la aplicación (por ejemplo, la desinstala por error). **Se recomienda tener registrados otros métodos adicionales** por si pierde el terminal móvil, y con ello el acceso a la aplicación y a la línea móvil, ya que en este escenario al perder el móvil perdería los dos métodos MFA a la vez. Lo mínimo sería tener dos y lo más recomendable para evitar inconvenientes son tres: la aplicación Authenticator, el número de móvil habitual y un número de teléfono alternativo bajo nuestro control o total confianza por si perdemos el móvil donde tenemos la aplicación y la línea registrada.

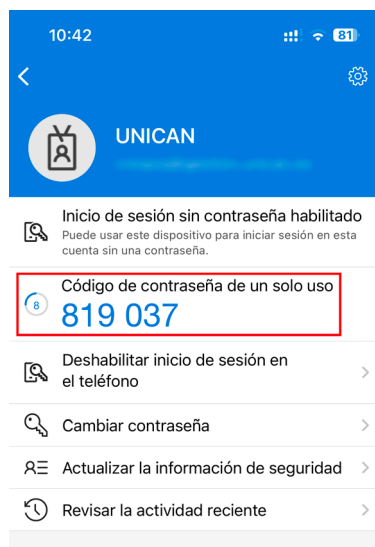
¿Debo proteger el acceso a Microsoft Authenticator y la autorización de validaciones en mi dispositivo?

Sí. Normalmente se protege con autenticación biométrica (huella o reconocimiento facial). Si su dispositivo no lo soporta debe protegerlo con un PIN local.

¿Necesito cobertura de móvil y/o wifi para utilizar Microsoft Authenticator?

No. Solo en la instalación de la aplicación (para “bajársela”) y el registro inicial. Luego funciona de forma autónoma incluso si no hay cobertura o está en modo avión.

Si no tiene datos en el móvil, las notificaciones entrantes (tipo “push”) con los números de dos cifras no funcionan, pero en ese caso basta con marcar, “quiero usar otro método” e indicar que se quiere usar una contraseña de un solo uso. Entonces introducimos el número de seis cifras que aparece en la App para nuestra cuenta y que es aleatorio y cambiante.



¿Qué pasa si desinstalo la aplicación MS Authenticator?

Si se desinstala la aplicación se pierde el vínculo con la cuenta y por tanto ese factor de autenticación. Al reinstalarla deberá vincular de nuevo la aplicación. Tenga en cuenta que necesitará otro sistema de MFA (por ejemplo, un SMS al número de línea móvil) para acceder al portal y realizar todas estas operaciones. Por eso recomendamos tener medios alternativos ya que, si no, no podrá acceder a la VPN UC y deberá abrir un caso con nuestro soporte que se podrá demorar.

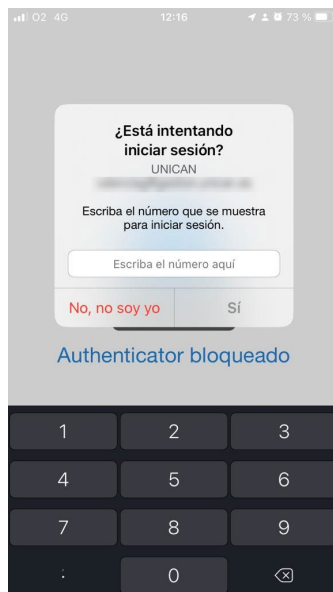
¿Qué pasa si recibo una solicitud de inicio de sesión en la App que no esperaba?

Puede que reciba en la App MS Authenticator una solicitud de inicio de sesión que no esperaba. Esto es poco probable si solamente usamos MFA para la VPN.

Esto puede deberse a:

- Una solicitud de renovación del inicio de sesión de un dispositivo en el que tenemos configurado. Por ejemplo, el correo (si es que tenemos activada la MFA para el correo).
- Un intento de **validación fraudulenta**.

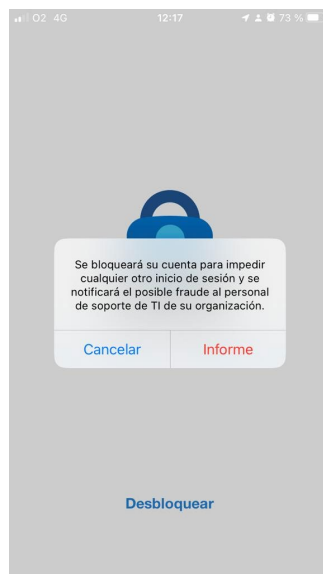
Dado que ante la duda es mejor no aceptar un intento de validación que no reconocemos, es mejor pulsar “No, no soy yo”.



Sin embargo, cuando pulsamos “No, no soy yo” el sistema nos ofrece a continuación **bloquear la autenticación MFA** para nuestra cuenta pulsando “Informar”. **Este punto es delicado**, ya que si bloqueamos el MFA de nuestra cuenta bloquearemos la validación en cualquier servicio que use MFA (como la VPN u otros, si es que lo tenemos activado en otros).



Si bloqueamos el MFA de nuestra cuenta pulsando “Informar” la única forma de desbloquearlo es contactar con el soporte del Servicio de Informática



Por tanto, si se trata de una solicitud puntual que no reconocemos lo mejor es pulsar “No, no soy yo” pero no “informar”, es decir pulsar “cancelar”. Lo más probable es que se deba a algún

dispositivo propio que se nos ha olvidado que lo teníamos configurado. Cuando vayamos a usarlo veremos que la autenticación MFA ha caducado y volvemos a activarla y ya está. **Pero por si acaso se trata de un fraude es mejor decir que no se reconoce** ese intento de inicio de sesión.

Únicamente tiene sentido bloquear en MFA (pulsando “informar”) si recibimos muchas notificaciones que no reconocemos y queremos evitarlas. En ese caso al bloquear el MFA de nuestra cuenta, se bloquearán los servicios que requieren MFA y debemos contactar con el soporte del Servicio de Informática.

¿Qué pasa si pierdo el móvil?

Si pierde el móvil y es el único dispositivo de doble autenticación que tiene registrado no podrá acceder a la VPN UC y deberá abrir un caso con nuestro soporte que se podrá demorar. Por ello le recomendamos que active varios métodos de autenticación secundaria. Por ejemplo, un número de móvil distinto de el del dispositivo donde tiene instalado Microsoft Authenticator. Teniendo un método alternativo puede proceder como se indica más adelante.

He cambiado de móvil ¿Qué hago?

Debe acceder al portal de <https://myaccount.microsoft.com> y desde información de seguridad agregar el Authenticator del nuevo dispositivo. Al agregar el Authenticator del nuevo dispositivo no se elimina automáticamente la aplicación del antiguo. Desinstale la aplicación de su antiguo dispositivo y a continuación elimine la instancia de Microsoft Authenticator referida al antiguo dispositivo de la configuración de su cuenta en <https://myaccount.microsoft.com>. Si ya no tiene acceso al antiguo dispositivo tenga en cuenta que necesitará otro sistema de MFA (por ejemplo, un SMS al número de línea móvil) para acceder al portal y realizar todas estas operaciones.

He perdido el móvil ¿Qué hago?

Debe acceder a <https://myaccount.microsoft.com/> y en información de seguridad “cerrar todas las sesiones”. A continuación, elimine la instancia de Microsoft Authenticator referida al dispositivo perdido. Tenga en cuenta que necesitará otro sistema de MFA (por ejemplo, un SMS a otro número de teléfono o la aplicación en otro dispositivo que sigue en su poder) para acceder al portal y realizar todas estas operaciones.

¿Puedo usar el MFA en más servicios de la UC?

Sí. Más adelante anunciaremos la posibilidad de solicitar de forma voluntaria la activación del MFA en más servicios, como por ejemplo el correo electrónico de la UC. Si quiere participar en un grupo piloto puede solicitarlo ya al Servicio de Informática. Un usuario puede incluso que no utilice la VPN pero puede configurar el MFA y pedir el alta para otros servicios para estos otros servicios.

¿Me va a pedir siempre autenticación MFA?

En el caso de la VPN UC cada vez que requiera autenticarse deberá usar MFA. Es decir, en la VPN se va a pedir siempre, aunque localmente se puede indicar que lo cacheé y lo pida con menos frecuencia. En el caso de otros servicios se podrán establecer medidas para no aplicar MFA en determinadas circunstancias.

Adicionalmente, algunos usuarios encuentran el password-less sign-in más cómodo que la combinación contraseña + MFA.

¿Por qué tanto lío?

Al igual que ocurre desde hace años con su banco, o más recientemente con sus redes sociales o sitios de compras, los servicios online protegidos únicamente con una contraseña se han

demostrado que son muy débiles frente ataques, ya que los robos de contraseña por descuidos o malware son habituales. Con el MFA ponemos otra barrera más para **intentar** parar estos ataques basados en el robo de contraseñas.

¿Quién va a intentar robar mi contraseña? No soy tan importante.

Cada cuenta de empleado de la UC es **una puerta** que permite, mediante el uso de diferentes técnicas, desarrollar ataques más complejos y graves que pueden llegar a **paralizar a toda la institución**. Esto no es una posibilidad teórica o algo lejano. Es algo que **ya ha ocurrido en universidades españolas análogas a la nuestra, y que puede ocurrir aquí**.

Las contraseñas de los empleados de las universidades que se han filtrado, por phishing, malware o porque usan la misma contraseña para otros servicios online, se **venden en el mercado negro** (Dark Web), y son una herramienta muy útil para realizar ataques a personas o instituciones para extorsionarlas o por ciberterrorismo.

No ser cuidadoso con nuestras credenciales de empleado, por ejemplo, usar la misma contraseña para otros servicios fuera de la UC o no prestar atención al phishing, pueden causar un **grave daño social, económico y reputacional tanto a la Universidad como a nivel personal**.

Consulte: <https://sdei.unican.es/nopiques>