Configuración de la Autenticación Multifactor (MFA)

Versión 2.5 enero 2026

Contenido

Qué es el MFA

La Autenticación Multifactor (**M**ulti**F**actor **A**uthentication, **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, sino que es necesario más cosas.**

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 aplicación del banco", ...etc., pero todos ellos funcionan con el mismo principio, es decir además de nuestra contraseña se nos pide verificar nuestra identidad con un segundo factor, normalmente mediante el móvil.

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 más graves.

El MFA en la UC

El uso de MFA desde fuera de la red institucional además de ser una medida necesaria para proteger nuestra institución, y que ya han adoptado la mayoría de universidades, es una obligación legal de acuerdo al Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Si ya tiene configurado el MFA porque usa la VPN, no es necesario reconfigurarlo. No obstante, compruebe que tiene más de un método configurado para así evitar posibles problemas en el futuro.

Desde agosto de 2023 el uso de MFA es obligatorio para la utilización de la VPN de la UC. Esta obligación se extendió[1] al Correo Electrónico, Teams, OneDrive UNICAN y en general a todos los servicios en la nube de la institución **siempre y cuando se utilicen fuera de la Red UNICAN**.

Posteriormente su uso se extenderá a otras aplicaciones y servicios

Si ya tiene configurada una aplicación, por ejemplo, el correo electrónico, en un ordenador o móvil, a partir de la fecha de activación, si se encuentra fuera de la UC, la aplicación le pedirá hacer la verificación MFA.

Tenga en cuenta que algunas aplicaciones pueden que no lo hagan correctamente y sea necesario reconfigurarlas desde el principio.
Si tiene problemas con la aplicación de correo de su móvil le recomendados usar Outlook Mobile. Más información en
https://sdei.unican.es/Paginas/servicios/correo/correopdipas.aspx

A diferencia de la VPN, el uso de MFA no será necesario en cada consulta al correo electrónico, por ejemplo. **Podremos decir que nos lo pida cada 60 días si es que estamos en un dispositivo de confianza.** Si estamos configurando una aplicación (como el Correo o Teams) la petición de MFA solo se realizará cada 60 días. Es decir, con un cliente de correo configurado, por ejemplo, en el móvil, nos pedirá el segundo factor una vez cada dos meses, pero debemos estar listos para usarlo.

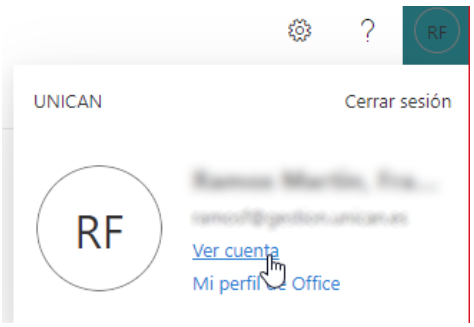
Configurar métodos para el MFA

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 en la nube (formato *usuario*@gestion.unican.es o *usuario*@unican.es o *usuario@alumnos.unican.es*) en:

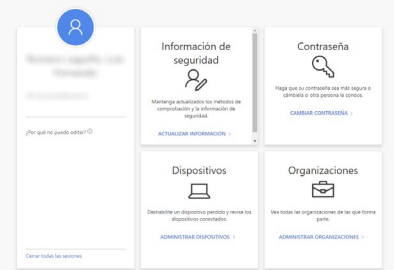
https://myaccount.microsoft.com/

o si ya estamos validados, por ejemplo, en el correo web, pulsamos sobre nuestro icono y elegimos la opción ‘Ver cuenta’.



[1] Desde el 21/10/2025 en el caso de lso empleados y desde el 16/2/2026 en el caos del estudiantado.

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



A la pantalla de configuración de MFA también se puede llegar directamente desde **https://aka.ms/mfasetup**

Lo recomendable es registrar varios métodos MFA. Veamos cómo registrar la App Microsoft Authenticator y un número de teléfono. Podemos registrar la App, un número de móvil (para recibir SMS) o, tal y como recomendamos, ambos.

Registro de la aplicación de autenticación Microsoft Authenticator

Nuestro método principal debería ser la App Microsoft Authenticator, 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 autentificación **resulta mucho más cómodo y es el método recomendado para usar habitualmente**.

Además de la app, recomendamos, como método alternativo, registrar un número de teléfono, pero en ese caso recomendamos registrar la app en dos dispositivos distintos. Ver más adelante "Preguntas más frecuentes". Si no queremos usar la app, podemos únicamente registrar el número de teléfono para recibir SMS.

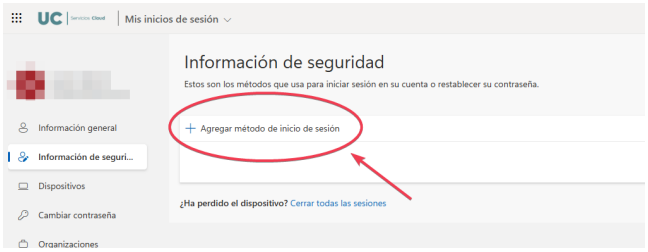
La aplicación se llama **Microsoft Authenticator** y estos son los enlaces de descarga:

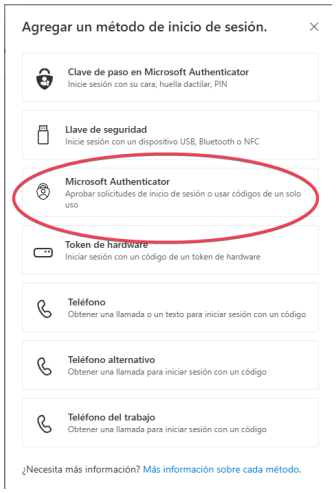
Android: https://play.google.com/store/apps/details?id=com.azure.authenticator

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

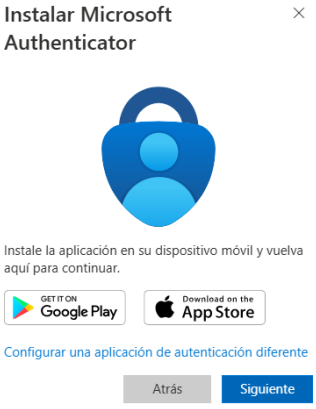
Para registrar una aplicación, lo añadimos, desde https://myaccount.microsoft.com/ y la opción de Actualizar información en 'Información de seguridad'. También se puede acceder directamente desde https://aka.ms/mfasetup

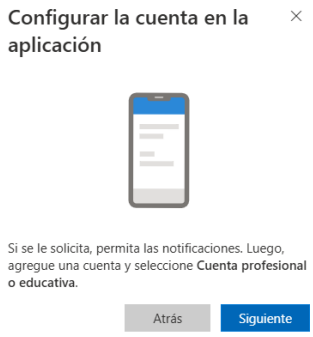
Agregamos un método de tipo "Microsoft Authenticator". Pulse "Agregar método de inicio de sesión" y seleccione "Microsoft Authenticator".





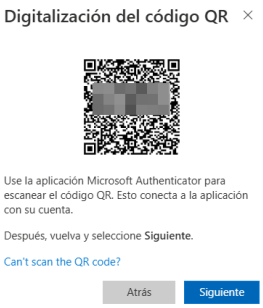
Se nos informa de los detalles de esta aplicación. Se recomienda haberla instalado antes a través de los enlaces en este documento o buscándola en el correspondiente App Store.



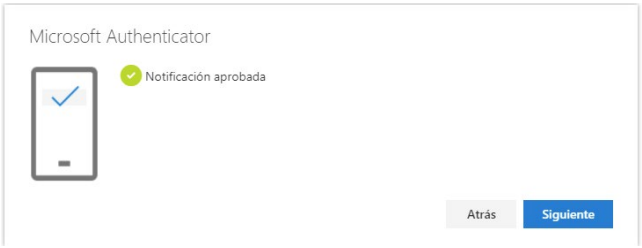


En la aplicación de móvil, **se agrega una cuenta de tipo profesional o educativa, pulsando el +, y eligiendo después la opción de escanear un código QR.** Escaneamos el código QR desde la aplicación del móvil.

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



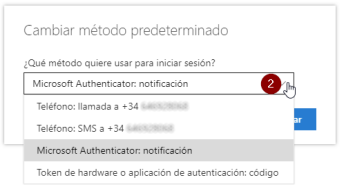
Tras escanearlo y completar los pasos en el móvil, la aplicación queda vinculada a nuestra cuenta.



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

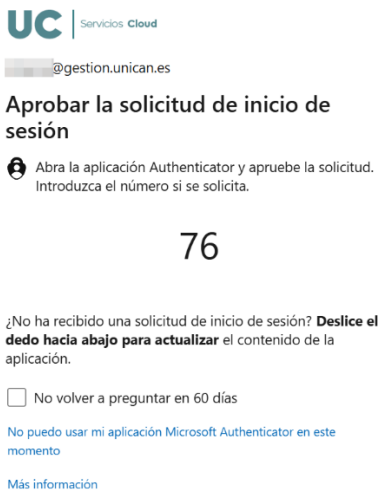
Se recomienda cambiar el método predeterminado a "Microsoft Authenticator, notificación", ya que resulta más cómodo. El método predeterminado es el que nos ofrece por defecto, pero si queremos usar otro de forma puntual, en la ventana de validación podremos pinchar en "Iniciar sesión de otra forma" para usar otro de los métodos MFA que podamos tener configurado (como nuestro número de móvil).

Para ello vamos a la opción de cambiar el método de inicio de sesión predeterminado (1) y luego elegimos el "Microsoft Authenticator, notificación"(2), que es el más cómodo.



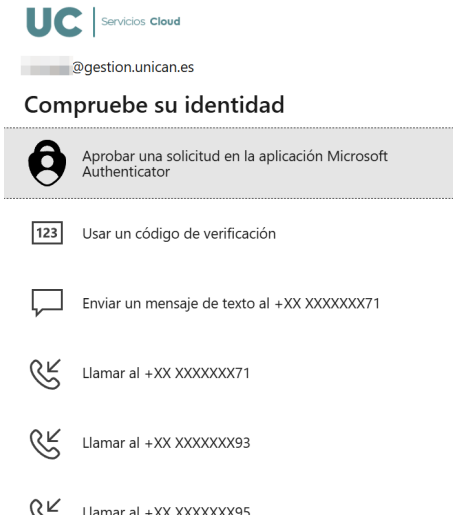
A partir de este momento, cuando inicie sesión, tras introducir usuario y contraseña, se solicitará el segundo factor, que, por defecto, será una notificación a la aplicación Microsoft Authenticator. Es decir, recibiremos una notificación en la app del móvil y deberemos introducir en ella el número de dos cifras que nos aparece en pantalla.

Como se puede observar, podemos indicar que no nos vuelva pedir MFA en 60 días (salvo en la VPN de empleados). Esto se debe hacer únicamente en nuestros dispositivos habituales.



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

En caso de no tener la App disponible, por ejemplo, por haber desinstalado la app, se puede pedir usar otro método, por ejemplo, el envío de un código o llamada al teléfono registrado. Para ello se hace click en “No puedo usar la aplicación Microsoft Authenticator en este momento” y nos mostrará los otros métodos que tengamos registrados.

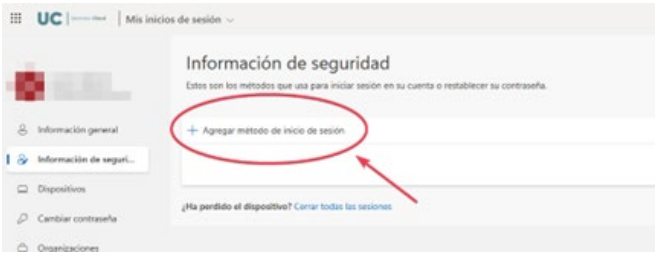


Es por ello por lo que se recomienda agregar más de un método para MFA. En la imagen anterior hay registrados varios. Lo más recomendable son tres: la aplicación Authenticator, el número de móvil habitual y un número de teléfono alternativo por si perdemos el móvil donde tenemos la aplicación y la línea registrada. Ver preguntas más frecuentes.

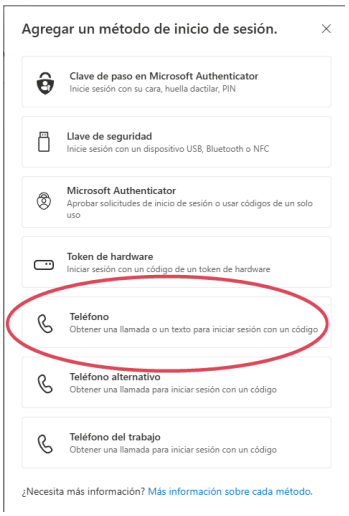
Tal y como se explica más adelante, y **de forma totalmente opcional**, aquellos que se sientan cómodos en su manejo, pueden activar el "password-less sign-in" (inicio de sesión sin contraseña) en la aplicación Authenticator para así no usar la contraseña. El "password-less sign-in" o autenticación sin contraseña solo está aconsejado a personas que entiendan su funcionamiento y estén familiarizas con la tecnología de autenticación sin contraseñas.

Registro de un número de teléfono

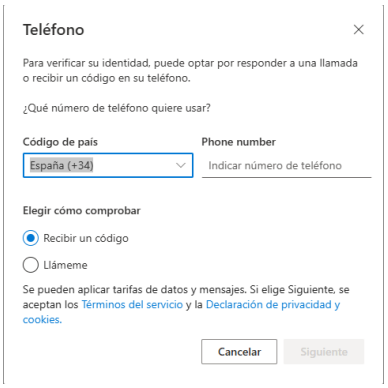
Recomendamos añadir primero un número de teléfono móvil, de esta forma, siempre tendremos la posibilidad de conseguir acceso a nuestra cuenta con un SMS o llamada de teléfono para verificar nuestra identidad. Pulse "Agregar método de inicio de sesión".



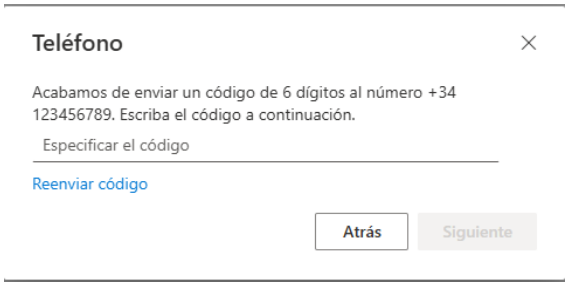
Seleccione Teléfono. Como se ve, posteriormente, se pueden añadir varios teléfonos.



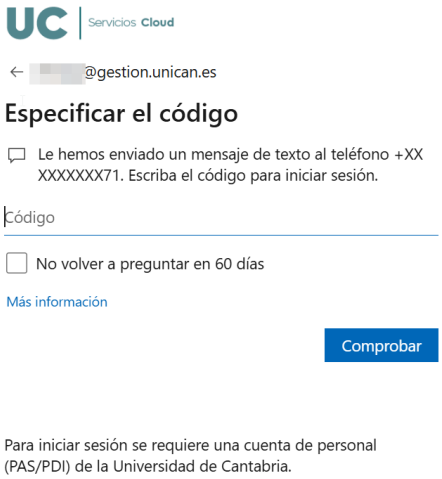
Se indica un número de teléfono (**tenga cuidado e indique el prefijo de España**) y si queremos un SMS (si es un móvil, más cómodo) o llamada para verificar que ese teléfono está bajo nuestro control:



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



Una vez verificado, y partir de este momento, ese número podrá ser usado como nuestro segundo factor de autenticación. Eso quiere decir que cuando se requiera MFA podremos verificar nuestra identidad mediante un número aleatorio que se nos envíe por SMS o mediante una locución de voz. Aquí vemos un ejemplo en el que debemos meter el número recibido por SMS.



También se puede hacer el registro sólo con la aplicación de autenticación Microsoft Authenticator, ver más adelante, sin dar un número de teléfono, aunque se recomienda en ese caso tener registrados varios dispositivos en los que tenemos instaladas y configuradas instancias de la app. 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.

Probar MFA

Dado que desde la propia Red UNICAN no se pide normalmente el MFA, una vez que tenga registrados los mecanismos de MFA en su cuenta, puede probarlo usando la antigua página para generar reuniones en Teams. No es necesario crear una reunión, simplemente se trata de comprobar que al iniciar sesión te pide el MFA.

https://campusvirtual.unican.es/teams

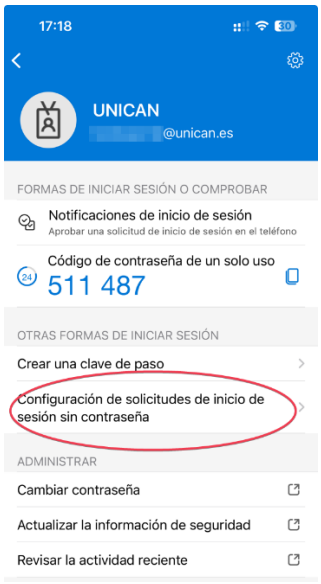
Según los mecanismos que haya registrado y use, durante la validación con MFA necesitará, además de su contraseña, introducir un código de un solo uso de seis cifras que obtendrá por SMS o en la App Microsoft Authenticator o bien confirmar la autenticación en la App Microsoft Authenticator usando el número de dos cifras que se le mostrará en pantalla.

Opcional: Activar passwordless (inicio de sesión sin contraseña)

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. El "password-less sign-in" o autenticación con contraseña **solo está aconsejado a personas que entiendan su funcionamiento y estén familiarizas con la tecnología de autenticación sin contraseñas.**

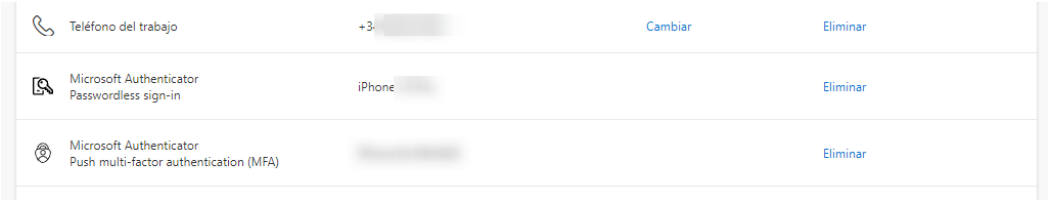
Se trata de un mecanismo seguro, ya que debemos usar el dispositivo y aprobar el inicio de sesión con autenticación biométrica (huella o reconocimiento facial) del dispositivo. El multifactor se logra con nuestra huella/cara (algo que somos) y nuestro dispositivo (algo que tenemos). No usamos la contraseña.

Para activarlo, una vez que tenemos registrada la aplicación Microsoft Authenticator debemos entrar en Microsoft Authenticator, seleccionar la cuenta registrada, seleccionar "Configuración de inicio de sesión sin contraseña"



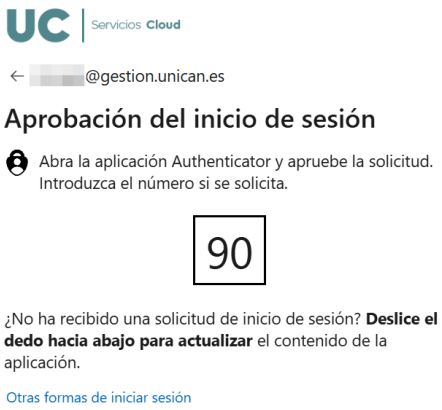
y seguir las instrucciones en pantalla para terminar de registrar la cuenta para el inicio de sesión en el teléfono sin contraseña.

Una vez activado si entramos en https://aka.ms/mfasetup 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 **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 un momento puntual, siempre podemos optar por usar contraseña + desafío MFA.

Pérdida de todos los mecanismos MFA

La pérdida de todos los mecanismos MFA nos impedirá acceder a los servicios que lo requieran, aunque sepamos nuestra contraseña. Por ejemplo, no podremos acceder al correo electrónico desde fuera de la Universidad, aunque sí desde nuestro puesto de trabajo. Es posible que, si hemos indicado que solo nos pida MFA cada 60 días, los accesos en dispositivos existentes sigan funcionando, pero al final dejarán de funcionar.

En caso de que sea empleado y que no dispongamos de un certificado electrónico personal (tipo FNMT o DNIe) deberemos contactar con soporte y personarnos en el Servicio de Informática con nuestra documentación (DNI, Tarjeta Universitaria o Pasaporte) para solicitar el borrado de mecanismos MFA. Este trámite solo se puede hacer personalmente previa cita.

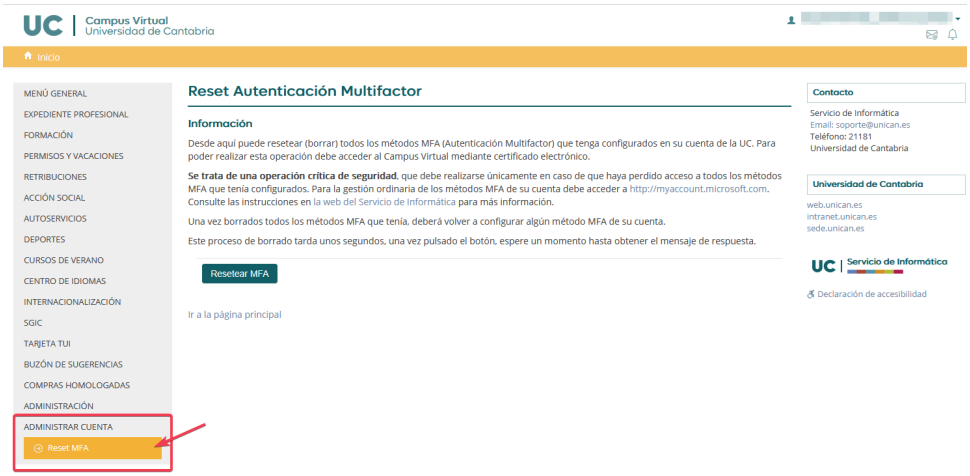
En caso de que sea estudiante y que no dispongamos de un certificado electrónico personal (tipo FNMT o DNIe) puede hacerlo desde Campus Virtual entrando con su usuario y contraseña, pero únicamente si lo hace desde la Red UNICAN (Wifi o equipos de uso para alumnos).

Si disponemos de un certificado electrónico personal podemos hacer este proceso nosotros mismos desde el Campus Virtual desde cualquier sitio.

Para borrar todos los mecanismos existentes deberemos acceder **CON certificado electrónico personal (FNMT o DNIe)** al Campus Virtual de la UC (https://campusvirtual.unican.es) y seleccionar la opción de **Administrar Cuenta -> "Reset MFA".** Para acceder al Campus Virtual con certificado digital, pulse en el botón correspondiente en la página de acceso.

Se trata de una operación crítica de seguridad que no debe realizarse a la ligera. Solo debe realizarse si hemos perdido acceso a todos los métodos MFA que teníamos configurados, ya que **borra todos** los métodos.

Una vez borrados todos los métodos MFA podremos volver a hacer el registro de los mismos.



Para evitar este trastorno, que puede ocurrir en un momento inconveniente, 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.

Recuerde que, si es estudiante, puede hacer este borrado, SIN certificado personal, accediendo al Campus Virtual con nuestro usuario y contraseña, pero solo si se hace desde la Red UNICAN (Wifi o equipos de uso para alumnos).

Para hacerlo desde cualquier sitio es necesario entrar al Campus Virtual con certificado digital (pulsando el botón correspondiente en la página de validación).

Preguntas frecuentes

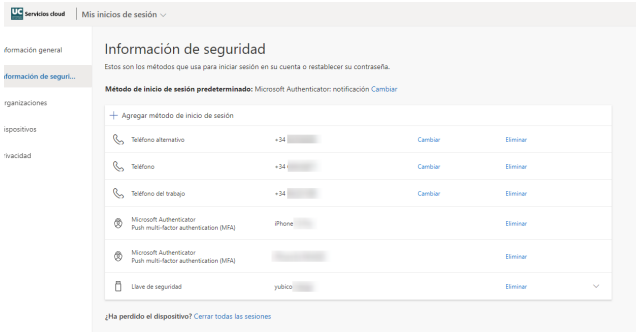
¿Es obligatorio utilizar MFA?

Sí, en caso de querer acceder a determinados servicios desde fuera de la UC.

Si no quiere utilizar MFA o no se siente cómodo usándolo, no podrá acceder remotamente a la Red UNICAN por VPN y no podrá acceder a los servicios que requieran autenticación MFA cuando estamos fuera de la UC, por lo que solo podrá usarlos cuando esté en su puesto de trabajo. Por ejemplo, sin MFA no podrá leer su correo profesional salvo cuando está en la Universidad.

¿Qué métodos para usar 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 códigos temporales por SMS o llamada), llaves de seguridad (tipo Yubico) y aplicaciones de autenticación (Microsoft Authenticator) instaladas en varios dispositivos. Lo importante es que sean dispositivos que están bajo su control personal. Si pierde un dispositivo donde tienen configurado la App para MFA, debe borrar dicho método de la configuración de su cuenta.



¿Por qué me pide MFA para configurar el MFA?

Si al intentar configurarlo le solicita MFA, significa que ya tenía algún método configurado previamente. Por ejemplo, en su día configuró la App Microsoft Authenticator pero posteriormente la borró o cambió de móvil. Si no tiene registrado su número de teléfono (para recibir un SMS) o no se acuerda de nada, tendrá que empezar de cero.

Para borrar todos los mecanismos MFA existentes deberemos acceder con certificado electrónico al Campus Virtual de la UC (https://campusvirtual.unican.es) y seleccionar la opción de Administrar Cuenta > “Reset MFA”. Los estudiantes pueden hacerlo, con certificado, desde cualquier sitio, o accediendo con su usuario y contraseña, pero solo desde la UC.

¿Qué método es mejor?

Sin lugar a dudas, lo mejor es usar habitualmente la aplicación de autenticación **Microsoft Authenticator** mediante notificaciones, 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).

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 Microsoft Authenticator aunque recomendamos en ese caso tener la aplicación registrada en al menos **dos dispositivos distintos** para tener dos alternativas de validación MFA.

¿Y si no tengo móvil (o no quiero usarlo)?

Aunque **el móvil es el mecanismo más natural y cómodo para hacer uso del MFA**, existe como alternativa la posibilidad de utilizar alguna aplicación de escritorio que permite usar MFA. Naturalmente esta aplicación será necesaria configurarla en un ordenador que esté bajo nuestro control exclusivo y al que tengamos acceso cuando nos encontramos fuera de la UC.

Para ello se han de seguir las instrucciones del **Manual de Configuración del MFA si no tengo móvil,** que encontrará en https://sdei.unican.es/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 (RGPDP) 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 limitaciones físicas. Puede ser de utilidad como medio de emergencia alternativo por si pierde/desinstala el Microsoft Authenticator, por ejemplo. Pero su limitación es que **solo podrá usarlo si está físicamente donde está la línea fija,** y si se trata del despacho no tiene sentido como método principal ya que solo le pedirá el MFA cuando esté fuera de la Universidad.

¿Puedo registrar el número de teléfono del mismo 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. O al menos hasta que recupere la línea del número de móvil después de hacer los correspondientes trámites con su compañía telefónica. 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.

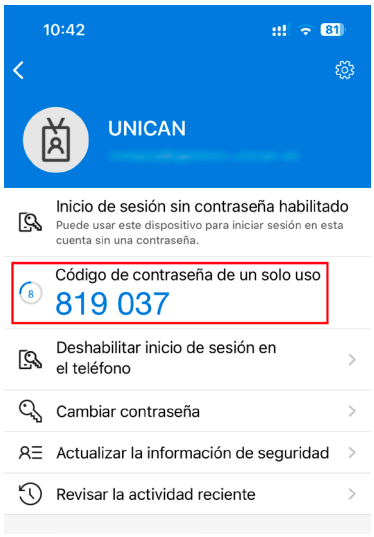
¿Debo proteger el acceso a Microsoft Authenticator y la autorización de validaciones en mi dispositivo?

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 Microsoft Authenticator?

Si se desinstala la aplicación se pierde el vínculo con la cuenta y por tanto ese factor de autenticación. No vale con volverla a instalar. Al reinstalarla deberá vincular de nuevo la aplicación a su cuenta. 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 y deberá resetear todos sus métodos MFA desde Campus Virtual usando su certificado personal.

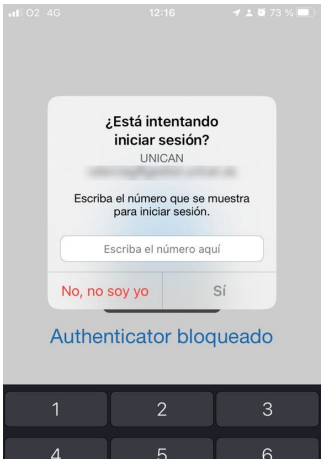
¿Qué pasa si recibo una solicitud de inicio de sesión en la App que no esperaba?

Puede que reciba en la App Microsoft Authenticator una solicitud de inicio de sesión que no esperaba.

Esto puede deberse a:

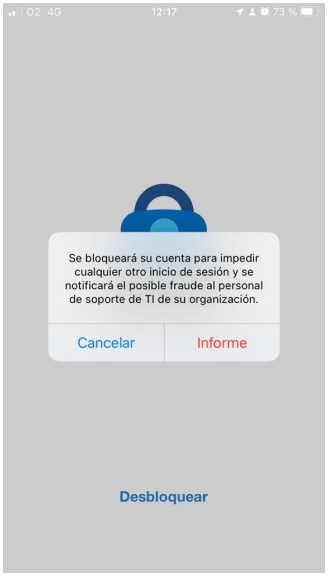
- Una solicitud de renovación del inicio de sesión de un dispositivo en el que tenemos configurado.
- Un intento de **validación fraudulenta.**

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" es posible que el sistema nos ofrezca a continuación **bloquear la autenticación MFA** para nuestra cuenta pulsando "Informar". **Este punto es muy delicado,** ya que **si bloqueamos el MFA de nuestra cuenta bloquearemos la validación en cualquier servicio que use MFA**.

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 los servicios cuando se requiera MFA y deberá abrir un caso con nuestro soporte que se podrá demorar o bien restear todos sus métodos MFA accediendo a Campus Virtual con su certificado electrónico personal. Por ello le recomendamos que active varios métodos MFA. 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://aka.ms/mfasetup y agregar primero 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://aka.ms/mfasetup

Si ya no tiene acceso al antiguo dispositivo (lo ha perdido, se ha roto, ..) 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://aka.ms/mfasetup 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.

¿Será necesario usar MFA en todos los servicios de la UC?

Paulatinamente se irá implementado en todos los servicios en donde sea técnicamente viable. Por otra parte, en esta fase solo se requerirá MFA desde fuera de la Red UNICAN.

¿Me va a pedir siempre autenticación MFA?

En el caso de la VPN UC cada vez que se valida debe usar MFA. Es decir, en la VPN se va pedir siempre, aunque localmente se puede indicar que lo cacheé y lo pida con menos frecuencia.

Pero en el caso de otros servicios podremos decir que solo pida el MFA cada 60 días. Además, solo se solicitará si estamos fuera de la Red UNICAN.

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

¿Por qué tanto lio?

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.** Por eso muchas de las universidades españolas ya obligan a sus empleados a usar MFA y varias lo requieren siempre.

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 de motivación ideológica.

Esto no es algo que "pase a los demás". **Cada año a decenas de empleados de la UC les roban sus contraseñas**, normalmente por usar la misma contraseña que en otros servicios, como correos particulares o redes sociales, por phishing o por otras causas.

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