CDC - Autenticación con doble factor

Versión 10-04-2024

Anar a la versió en valencià[1]

Índice

1. ¿Qué es la autenticación con doble factor?

La autenticación con doble factor es una medida de seguridad para acceder a servicios y aplicaciones con la identidad digital. Se trata de un método de control donde hay que aportar, además de las credenciales (nombre y contraseña), una verificación extra. Esta verificación es sólo de un uso y puede tener varias representaciones, como por ejemplo un código o una pulsación en la pantalla, y se obtiene mediante:

- Una aplicación de autenticación instalada en el móvil
- Un mensaje de texto (sms) enviado al móvil
- Una llamada de teléfono

Con esta doble autenticación se consigue que la cuenta de una persona esté más segura frente a accesos no deseados, incluso cuando un tercero conozca las credenciales de la identidad digital de esa persona.

[1] https://sway.office.com/qFfQRI4QnCy3JJrF

2. ¿Cómo se configura la autenticación con doble factor?

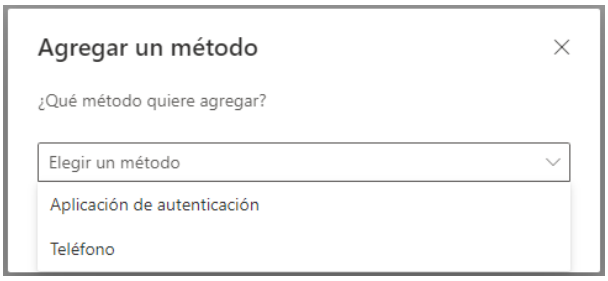
Los dispositivos para obtener el código de autenticación de doble factor se pueden gestionar (dar de alta nuevos, eliminar de antiguos...) vía web. Los pasos para configurar un nuevo dispositivo son estos:

1. Cerrar todas las aplicaciones donde se haya iniciado sesión con la identidad digital @edu.gva.es, con el fin de que todo el proceso de configuración funcione correctamente.
2. Ir a la dirección web: https://www.office.com.
3. Introducir las credenciales (nombre y contraseña) de la identidad digital.
4. Hacer clic sobre la imagen de perfil.
5. Pulsar en *Ver cuenta*.
6. Abrir el apartado *Información de seguridad* del menú lateral.

7. Hacer clic en *Agregar método de inicio de sesión*. En la ventana emergente, hay que elegir uno de los métodos de autenticación de doble factor.

Es conveniente definir dos métodos de autenticación:

- Aplicación de autenticación. El código de acceso se recibe en una aplicación móvil.
- Teléfono. El código de acceso se recibe en un mensaje de texto en el móvil (sms).

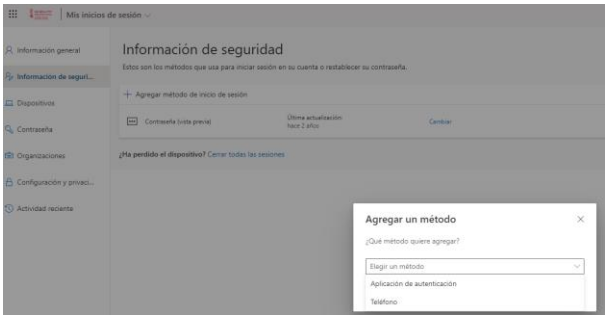


3. ¿Qué métodos de autenticación con doble factor se pueden utilizar?

Cuando se pulsa la opción *Agregar método de inicio de sesión*, aparece una ventana emergente donde se puede elegir:

- Aplicación de autenticación
- Teléfono

A continuación se explica cómo registrarse con cada uno de estos métodos. Recordemos una vez más la recomendación de registrar los dos métodos de autenticación.

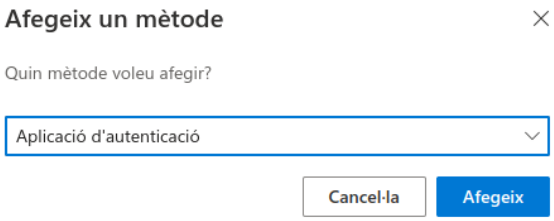


Aplicación de autenticación

Los pasos a seguir con este método son los siguientes:

1. Elegir la opción *Aplicación de autenticación*

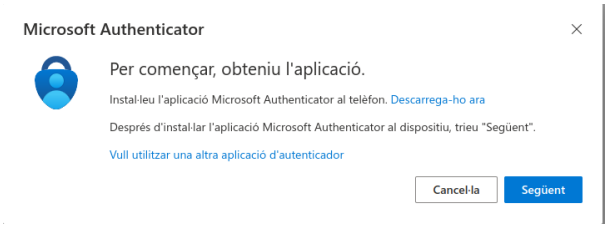
2. Hacer clic en el botón *Agregar*



3. Aparecerá una ventana con las instrucciones paso a paso para instalar la aplicación correspondiente:

- Enlace *Descargar ahora*. Donde se detallan las instrucciones para instalar la aplicación *Microsoft Authenticator*
- Enlace *Quiero usar otra aplicación de autentica*. Donde se detallan las instrucciones para instalar una aplicación diferente a *Microsoft Authenticator*

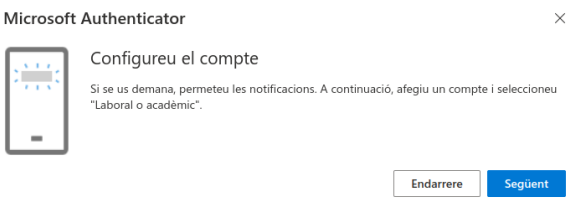
4. Una vez la aplicación esté instalada en el móvil, se debe continuar el proceso de configuración haciendo un clic en *Siguiente*.



Microsoft Authenticator

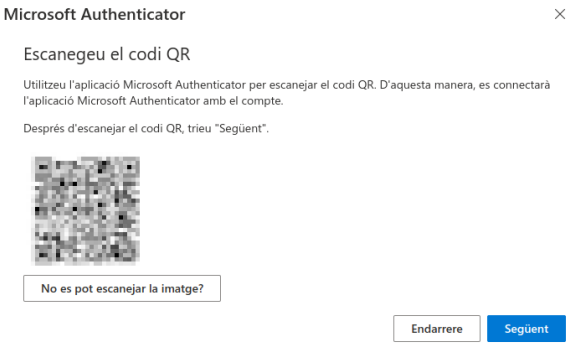
En el caso de haber elegido el enlace *Descargar ahora* (es decir, autenticación con la aplicación *Microsoft Authenticator*), se deben seguir los siguientes pasos:

5a. Aparece la ventana *Configuración de la cuenta*, donde simplemente hay que hacer clic en *Siguiente*

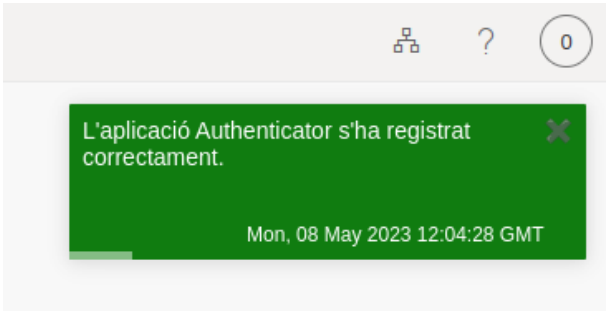


6a. A continuación, aparece una nueva ventana con un código QR que hay que escanear con la aplicación de autenticación que acabamos de instalar en nuestro móvil.

Esto sirve para emparejar la aplicación con la identidad digital. Una vez escaneado el código QR, se continúa el proceso con un clic en *Siguiente*.



7a. Si todo el proceso se realiza correctamente, aparecerá un mensaje de confirmación



Otras aplicaciones de autenticación

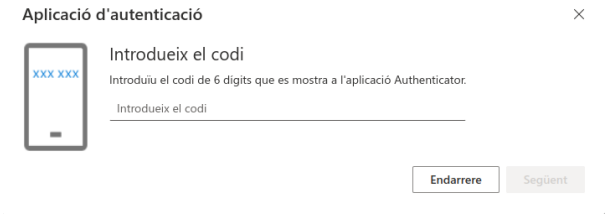
En caso de haber elegido el enlace *Quiero utilizar otra aplicación de autenticador*, (es decir, autenticación con una aplicación diferente a Microsoft Authenticator), deberemos seguir los siguientes pasos:

5b. Aparece la ventana *Configuración de la cuenta*, donde simplemente hay que hacer clic en *Siguiente*

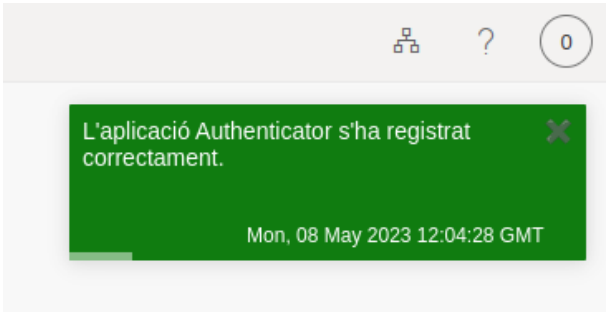
6b. A continuación, aparece una nueva ventana con un código QR que hay que escanear con la aplicación de autenticación que acabamos de instalar en nuestro móvil.

Esto sirve para emparejar la aplicación con la identidad digital. Una vez escaneado el código QR, se continúa el proceso con un clic en *Siguiente*.

7b. En la aplicación de autenticación se recibirá un código de 6 dígitos, que hay que introducir correctamente. Para finalizar, simplemente hay que hacer clic en *Siguiente*



8b. Si todo el proceso se realiza correctamente, aparecerá un mensaje de confirmación

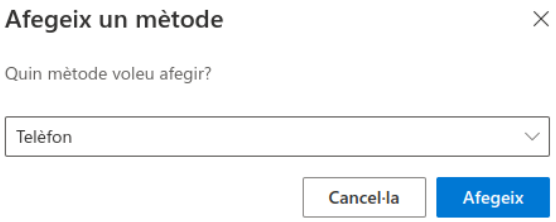


Teléfono

Los pasos a seguir con este método son los siguientes:

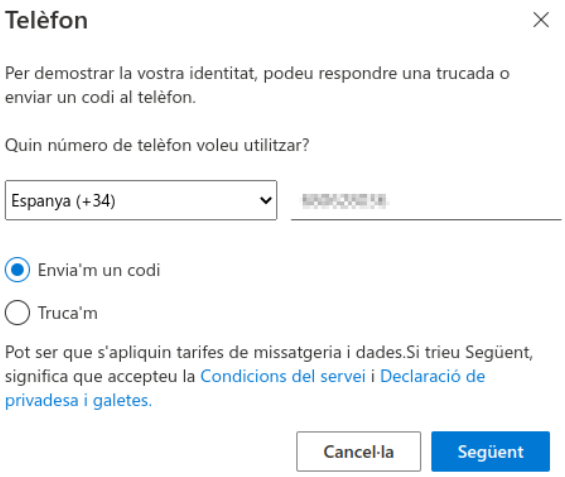
1. Escoger la opción *Teléfono*

2. Hacer clic en el botón *Agregar*



3. Aparecerá una ventana donde hay que introducir el país y el número de teléfono donde se quiere recibir el mensaje de texto (sms) con el código o la llamada

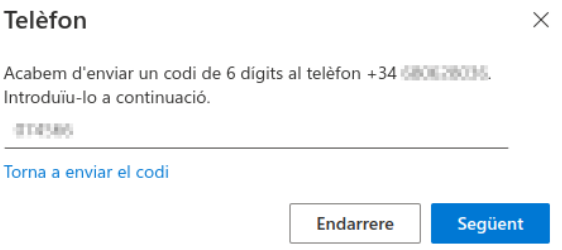
4. Hacer clic en *Siguiente*



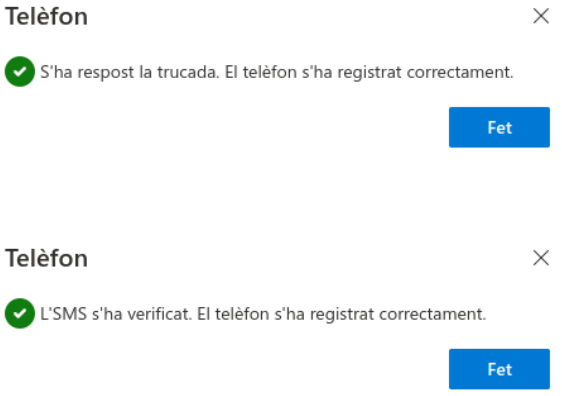
Si se ha elegido la opción *Llámeme,* se recibirá una llamada desde el extranjero (suele ser +1 855-330-8653) y hay que seguir las instrucciones de la locución (normalmente se solicita apretar la tecla #).

AVISO IMPORTANTE > Si se está utilizando una línea IP, como en el caso de los teléfonos en centros educativos, antes de marcar # hay que activar la **marcación por tonos** pulsando ***90**. Por tanto, tras recibir la llamada y escuchar la locución con las instrucciones, hay que pulsar ***90** y después **#**.

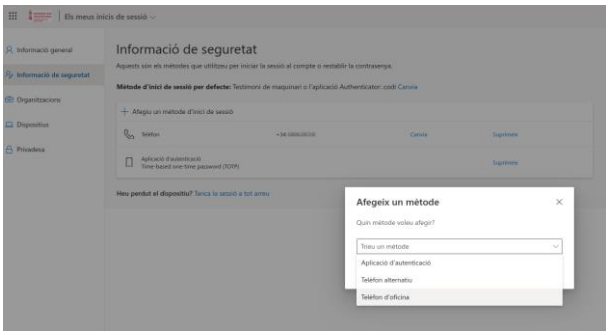
Si se ha elegido la opción *Envíeme un código*, en la nueva ventana, se debe introducir el código de 6 dígitos que se recibe en el mensaje de texto (sms).



Si todo el proceso se realiza correctamente, aparecerá un mensaje de confirmación.



Y, además, en la pantalla de *información de seguridad* ya aparecerá el nuevo método de autenticación.



4. Nuestra recomendación de uso del doble factor de autenticación

Existe un límite en la cantidad de dispositivos que se pueden utilizar para cada método en el doble factor de autenticación. Son éstos:

- Número máximo de teléfonos: 3 (1 teléfono + 1 teléfono alternativo + 1 teléfono de oficina)
- Número máximo de dispositivos con la aplicación de autenticación: 5

Dado este límite, os presentamos nuestra recomendación de uso del doble factor, simplemente como guía por si os sirve de ayuda para planificar vuestra labor diaria.

Doble autenticación en la identidad digital de centro (IDC)

Cada miembro del equipo directivo que quisiera hacer uso de la IDC fuera de la red del centro, debe instalar la aplicación de autenticación en su móvil y configurar el acceso con la IDC (ver apartado 4).

Y, además, se configura el teléfono del centro para recibir el código de verificación mediante una llamada, como sistema secundario (para los casos en que, en algún momento determinado, ninguno de los miembros del equipo directivo tenga la posibilidad de acceder a la aplicación de autenticación de su teléfono móvil).

5. En caso de tener alguna duda sobre la autenticación con doble factor, ¿dónde hay que dirigirse?

Para cualquier duda o incidencia, contactar con el SAI bien a través de la aplicación de incidencias gvaSAI: https://gvasai.edu.gva.es/ en la categoría *Nuevo tique sobre otros servicios o aplicaciones educativas > Incidencia > Centro Digital Colaborativo > Consultas/Incidencias técnicas*, o bien a través del teléfono 961207685 de lunes a viernes de 8h a 20h.