

# CDC - Autenticació amb doble factor

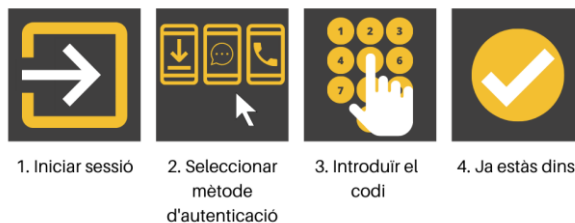
Versió 10-04-2024

[Ir a la versión en castellano](#)

## Índex

1. Què és l'autenticació amb doble factor?
2. Com es configura l'autenticació amb doble factor?
3. Quins mètodes d'autenticació amb doble factor es poden fer servir?
4. La nostra recomanació d'ús del doble factor d'autenticació
5. En cas de tenir algun dubte sobre l'autenticació amb doble factor, on cal adreçar-se?

## 1. Què és l'autenticació amb doble factor?



L'autenticació amb doble factor és una mesura de seguretat per accedir a serveis i aplicacions amb la identitat digital. Es tracta d'un mètode de control on cal aportar, a més de les credencials (nom i contrasenya), una verificació extra. Aquesta verificació és només d'un ús i pot tenir diverses representacions, com per exemple un codi o una pulsació a la pantalla, i s'obté mitjançant:

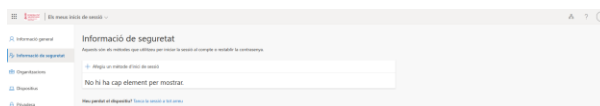
- Una aplicació d'autenticació instal·lada al mòbil
- Un missatge de text (sms) enviat al mòbil
- Una trucada de telèfon

Amb aquesta doble autenticació s'aconsegueix que el compte d'una persona estiga més segur front accessos no desitjats, inclús quan un tercer conega les credencials de la identitat digital d'eixa persona.

## 2. Com es configura l'autenticació amb doble factor?

Els dispositius per obtenir el codi d'autenticació de doble factor es poden gestionar (donar d'alta nous, eliminar d'antics...) via web. Els passos per configurar un nou dispositiu són aquests:

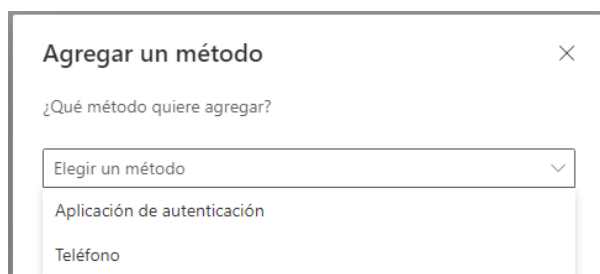
1. Tancar totes les aplicacions on s'haja iniciat sessió amb la identitat digital @edu.gva.es, per tal de què tot el procés de configuració funcione correctament.
2. Anar a l'adreça web: <https://www.office.com>.
3. Introdur les credencials (nom i contrasenya) de la identitat digital.
4. Fer clic sobre la imatge de perfil.
5. Pulsar a *Mostra el compte*.
6. Obrir l'apartat *Informació de seguretat* del menú lateral.



7. Fer clic a *Afegiu un mètode d'inici de sessió*. En la finestra emergent, cal triar un dels mètodes d'autenticació de doble factor.

És convenient definir dos mètodes d'autenticació:

- Aplicació d'autenticació. El codi d'accés es rep en una aplicació mòbil.
- Telèfon. El codi d'accés es rep en un missatge de text al mòbil (sms).

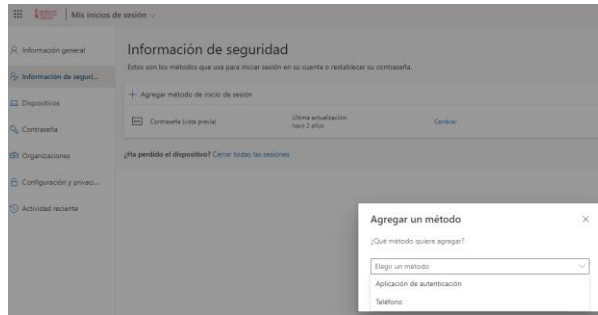


## 3. Quins mètodes d'autenticació amb doble factor es poden fer servir?

Quan es prem l'opció *Afegiu un mètode d'inici de sessió*, apareix una finestra emergent on es pot triar:

- Aplicació d'autenticació
- Telèfon

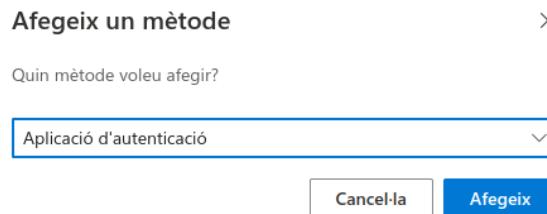
A continuació s'explica com registrar-se amb cadascun d'aquests mètodes. Recordem una vegada més la recomanació de registrar els dos mètodes d'autenticació.



## Aplicació d'autenticació

Els passos a seguir amb aquest mètode son els següents:

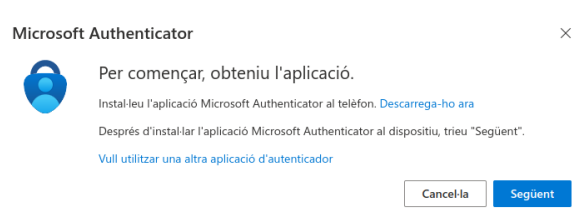
1. Triar l'opció *Aplicació d'autenticació*
2. Fer clic en el botó *Afegeix*



3. Apareixerà una finestra amb les instruccions pas a pas per instal·lar l'aplicació corresponent:

- Enllaç *Descarrega-ho ara*. On es detallen les instruccions per instal·lar l'aplicació *Microsoft Authenticator*
- Enllaç *Vull utilitzar una altra aplicació d'autenticador*. On es detallen les instruccions per instal·lar una aplicació diferent a *Microsoft Authenticator*

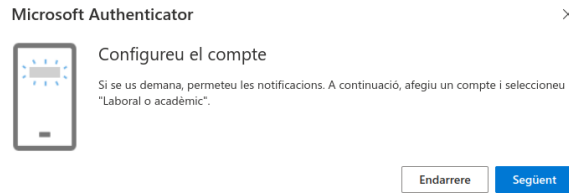
4. Una vegada l'aplicació estiga instal·lada en el mòbil, s'ha de continuar el procés de configuració fent un clic en *Següent*.



## Microsoft Authenticator

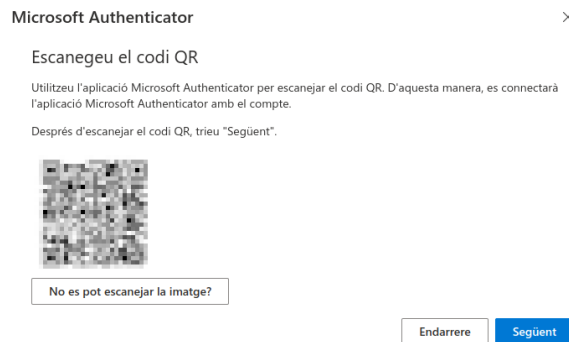
En cas d'haver triat l'enllaç *Descarrega-ho ara* (és a dir, autenticació amb l'aplicació *Microsoft Authenticator*), cal seguir els següents passos:

5a. Apareix la finestra *Configureu el compte*, on simplement cal fer clic en *Següent*

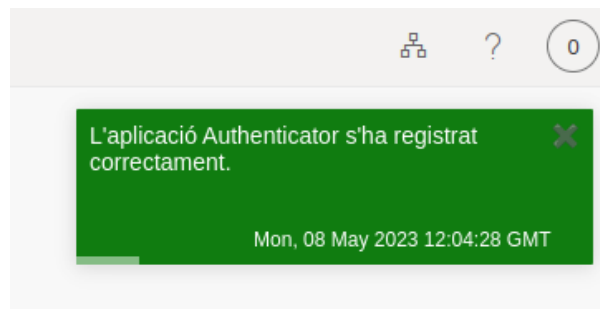


6a. A continuació, apareix una nova finestra amb un codi QR que cal escanejar amb l'aplicació d'autenticació que acabem d'instal·lar en el nostre mòbil

Això serveix per emparellar l'aplicació amb la identitat digital. Una vegada escanejat el codi QR, es continua el procés amb un clic en *Següent*.



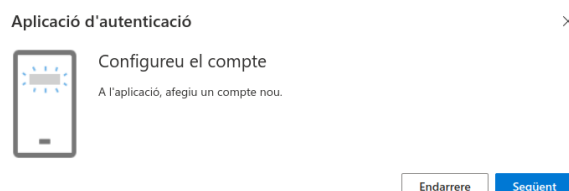
7a. Si tot el procés es realitza correctament, apareixerà un missatge de confirmació



### *Altres aplicacions d'autenticació*

En cas d'haver triat l'enllaç *Vull utilitzar una altra aplicació d'autenticador*, (és a dir, autenticació amb una aplicació diferent a Microsoft Authenticator), haureu de seguir els següents passos:

5b. Apareix la finestra *Configureu el compte*, on simplement cal fer clic en *Següent*

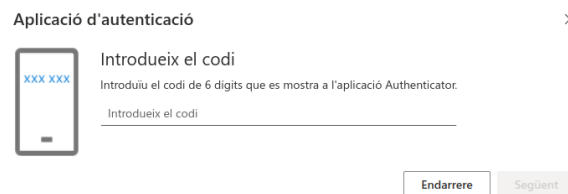


6b. A continuació, apareix una nova finestra amb un codi QR que cal escanejar amb l'aplicació d'autenticació que acabem d'instal·lar en el nostre mòbil

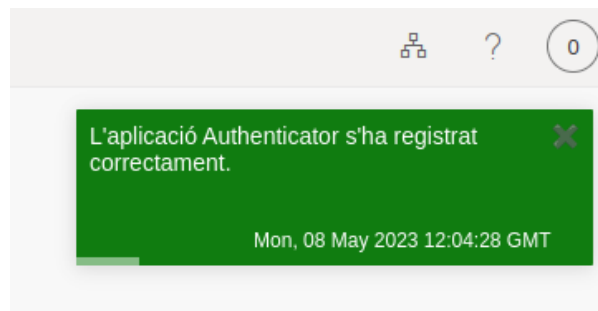
Això serveix per emparellar l'aplicació amb la identitat digital. Una vegada escanejat el codi QR, es continua el procés amb un clic en *Següent*.



7b. En l'aplicació d'autenticació es rebrà un codi de 6 dígit, que cal introduir correctament. Per finalitzar, simplement cal fer clic en *Següent*



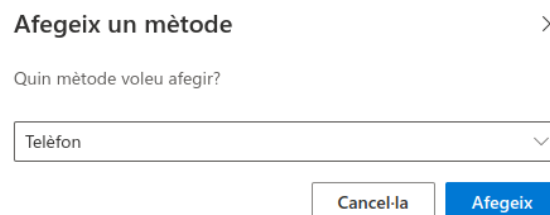
8b. Si tot el procés es realitza correctament, apareixerà un missatge de confirmació



## Telèfon

Els passos a seguir amb aquest mètode son els següents:

1. Triar l'opció *Telèfon*
2. Fer clic en el botó *Afegeix*



3. Apareixerà una finestra on cal introduir el país i el número de telèfon on es vol rebre el missatge de text (sms) amb el codi o la trucada

#### 4. Fer clic en *Següent*

### Telèfon

Per demostrar la vostra identitat, podeu respondre una trucada o enviar un codi al telèfon.

Quin número de telèfon voleu utilitzar?

Espanya (+34)

Envia'm un codi  
 Truca'm

Pot ser que s'apliquin tarifes de missatgeria i dades. Si trieu Següent, significa que accepteu la [Condicions del servei](#) i [Declaració de privadesa i galetes](#).

Si s'ha triat l'opció *Truca'm*, es rebrà una trucada des de l'estranger (sol ser +1 855-330-8653) i cal seguir les instruccions de la locució (normalment es sol·licita prémer la tecla #).

AVÍS IMPORTANT > Si s'està utilitzant una línia IP, com en el cas dels telèfons en centres educatius, abans de marcar # cal activar la **marcació per tons** polsant **\*90**. Per tant, després de rebre la trucada i escoltar la locució amb les instruccions, cal polsar **\*90** i després #.

Si s'ha triat l'opció *Envia'm un codi*, en la nova finestra, s'ha d'introduir el codi de 6 dígits que es rep en el missatge de text (sms).

### Telèfon

Acabem d'enviar un codi de 6 dígits al telèfon +34 . Introduïu-lo a continuació.

[Torna a enviar el codi](#)

Si tot el procés es realitza correctament, apareixerà un missatge de confirmació.

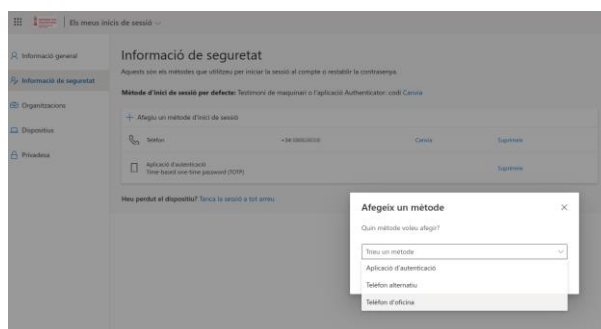
### Telèfon

S'ha respost la trucada. El telèfon s'ha registrat correctament.

### Telèfon

L'SMS s'ha verificat. El telèfon s'ha registrat correctament.

I, a més, a la pantalla d'*informació de seguretat* ja apareixerà el nou mètode d'autenticació.



## 4. La nostra recomanació d'ús del doble factor d'autenticació

Existeix un límit en la quantitat de dispositius que es poden fer servir per a cada mètode en el doble factor d'autenticació. Són aquests:

- Nombre màxim de telèfons: 3 (1 telèfon + 1 telèfon alternatiu + 1 telèfon d'oficina)
- Nombre màxim de dispositius amb l'aplicació d'autenticació: 5

Donat aquest límit, us presentem la nostra recomanació d'ús del doble factor, simplement com a guia per si us serveix d'ajuda per planificar la vostra tasca diària.

### **Doble autenticació en la identitat digital de centre (IDC)**

Cada membre de l'equip directiu que vullga fer ús de la IDC fora de la xarxa del centre, ha d'instal·lar l'aplicació d'autenticació en el seu mòbil i configurar l'accés amb la IDC (veure apartat 4).

I, a més, es configura el telèfon del centre per rebre el codi de verificació mitjançant una trucada, com a sistema secundari (per als casos en què, en algun moment determinat, cap dels membres de l'equip directiu tinga la possibilitat d'accedir a l'aplicació d'autenticació del seu mòbil).

## 5. En cas de tenir algun dubte sobre l'autenticació amb doble factor, on cal adreçar-se?

Per a qualsevol dubte o incidència, contactar amb el SAI bé a través de l'aplicació d'incidències gvaSAI: <https://gvasai.edu.gva.es/> a la categoria *Nou tiquet sobre altres serveis o aplicacions educatives > Incidència > Centre Digital Col·laboratiu > Consultes/Incidències tècniques*, o bé a través del telèfon 961207685 de dilluns a divendres de 8h a 20h.