

# Seguretat dels comptes d'usuari

## *Guia per a l'activació del segon mètode d'autenticació*

Data de revisió: 10/2023

**UAB**

Universitat Autònoma  
de Barcelona

## 1. Justificació

L'autenticació de doble factor afegeix una capa extra de seguretat al nivell bàsic d'autenticació, que només requereix un compte i una contrasenya. Amb el doble factor s'introdueix un pas addicional amb l'objectiu d'impedir que algú que s'hagi pogut fer amb la nostra contrasenya pugui accedir fàcilment als serveis que tenim autoritzats. La implantació del doble factor d'autenticació està en línia amb els preceptes d'aplicació de mesures de seguretat en els sistemes d'informació, per un costat, i la regulació per a protecció de dades, drets i llibertats, per l'altre.

La protecció passa de ser només “alguna cosa que se sap” (la contrasenya) a ser aquesta mateixa més una conformitat a un avís des d'alguna cosa que es té” (un dispositiu).

La informació per a verificació de seguretat addicional només es farà servir per a finalitats de seguretat del compte.

L'existència del doble factor d'autenticació manté la necessitat de tenir una contrasenya segura. Aquesta ha de contenir, com a mínim, 8 caràcters. Per a construir-la s'ha d'utilitzar un mínim de 3 d'aquests tipus de símbols: majúscules, minúscules, números i caràcters especials. A la contrasenya no s'utilitzaran dades personals ni contrasenyes anteriors.

## 2. Procediment d'activació

El doble factor s'activa automàticament amb la creació del compte, però cada persona és responsable de definir quin mètode li interessa més, vigilant que cada vegada que vulgui accedir als serveis ha de tenir el dispositiu accessible. S'ha de definir més d'un mètode i seleccionar el que es vol com a principal. Es recomana que un dels mètodes escollits sigui una aplicació d'autenticació compatible amb estàndards OATH TOTP. Se'n pot disposar més d'una de manera simultània i en diferents dispositius.

Revisar i configurar els mètodes d'autenticació es pot fer des de la web del correu, opció Visualitza el compte -> Informació de seguretat.

## 3. Aplicacions d'autenticació

Per a fer servir en estació de treball o des de mòbil:

- [Microsoft Authenticator](#) Disponible per a dispositius mòbils.
- [2fast – Two Factor Authenticator](#) Disponible per a estacions de treball amb Windows.
- [FreeOTP Authenticator](#) Disponible per a dispositius mòbils.

Implementada a través d'una extensió de navegador (opció recomanada per a qui prefereixi no fer servir Microsoft Authenticator):

- [Authenticator-Extension](#) Disponible per a Chrome, Firefox, Edge i Safari