

# RECOMANACIONS DE SEGURETAT

1

## UTILITZEU SEMPRE ANTIVIRUS

- **Instal·leu l'antivirus corporatiu.** Funciona en comunicació amb un servidor que proporciona la configuració adequada, actualitza els fitxers de patrons de virus i pot executar accions d'emergència per a protegir en cas d'epidèmia.
- **Mantenir actualitzat l'antivirus permanentment** per a la detecció i eliminació de virus.
- **La instal·lació de l'antivirus corporatiu es fa a través de xarxa.** El requisit fonamental és no tenir un altre antivirus instal·lat.

2

## MANTINGUEU L'EQUIP ACTUALITZAT

- Mantingueu **actualitzades les aplicacions i el sistema operatiu.**
- Els **sistemes operatius i aplicacions obsolets** no disposen de suport.  
Conseqüències:
  - en cas d'incidència, no podrà ser solucionada;
  - no existeixen actualitzacions per a millorar-ne errors i seguretat;
  - presència de vulnerabilitats que permeten l'accés d'agents no autoritzats i nocius a la informació del nostre equip.

3

## VERIFIQUEU CADA CORREU ELECTRÒNIC ABANS D'OBRIR-LO

- **No obriu cap enllaç** ni descarregueu cap fitxer adjunt procedent d'un correu electrònic que presente qualsevol indicatiu o patró fora del que és habitual.
- **Verifiqueu-ne el remitent.** No confieu en el nom del remitent, comproveu que el domini del correu és de confiança.

# RECOMANACIONS DE SEGURETAT

4

## NO US DONEU D'ALTA AMB L'USUARI DE LA UV EN TERCERES ENTITATS

- No us doneu d'alta en serveis oferits per terceres empreses o organismes (exemple: plataformes de *streaming* tipus Netflix o HBO, *marketplaces* com Amazon...) amb l'usuari de la Universitat de València.
- Si per algun motiu, fora necessari i inevitable donar-se d'alta amb l'usuari de la UV en alguna entitat externa, **no utilitzeu la mateixa contrasenya** que en els serveis de la Universitat.

5

## NO DESCARREGUEU PROGRAMES EN LLOCS NO SEGURS DE LA XARXA

La instal·lació de programes no segurs pot afectar el rendiment i comprometre la seguretat de dispositius i equips.

- Descarregueu únicament **programes disponibles en** <https://software.uv.es>. Empreu programari legal i vigent ofereix garantia i suport.
- Instal·leu i mantingueu **pedaços i actualitzacions de seguretat**.

6

## REALITZEU CÒPIES DE SEGURETAT PERIÒDICAMENT

- Si hi ha informació que desitgeu mantenir, la Universitat de València posa a la nostra disposició dos serveis que realitzen còpies de seguretat periòdiques: [disco.uv.es](https://disco.uv.es) o [nuvol.uv.es](https://nuvol.uv.es). Garanteixen la seguretat amb un **sistema de còpies centralitzades**.
- Si tens alguna incidència o dubte amb aquests serveis, pots contactar amb el **Centre d'Atenció a l'Usuari (CAU)**.

# RECOMANACIONS DE SEGURETAT

7

## UTILITZEU USUARI SENSE PRIVILEGIS

Treballar en el sistema com a **usuari sense privilegis** per a tasques genèriques. Eviteu treballar com a “Administrador”. Raons:

- la majoria de les **tasques comunes** no necessiten un usuari amb privilegis;
- Si algun **virus** o un altre programa maliciós vol entrar en el nostre equip, es veurà molt **limitat** en la seua capacitat per a causar mal.

8

## NETEJA DE DOCUMENTS

- **Inspeccioneu i esborreu les metadades** i altres dades ocultes existents en els documents.
- Les metadades són **incorporades de manera automàtica** pels programes de generació i tractament de documents, o pels mateixos usuaris o usuàries de l'organització.

9

## DOBLE FACTOR D'AUTENTICACIÓ

Parlem de **doble factor en l'autenticació** (2FA) quan li diem als nostres sistemes que:

- usarem el nostre **usuari i una contrasenya** (o un certificat digital);
- i una segona dada que permeta **comprovar la nostra identitat**.

Objectiu: evitar els casos en què alguna persona malintencionada vulga fer un **ús fraudulent de la vostra identitat d'usuari de la UV**.

- Actualment, alguns serveis o aplicacions de la Universitat de València requereixen la doble autenticació per accedir-hi.