

COM PROTEGIR LA TEVA SEGURETAT ONLINE

# Com protegir la teva seguretat online





# Sobre Barcelona Activa

Barcelona Activa és l'agència de desenvolupament econòmic local de Barcelona. Fundada el 1987, és una societat mercantil pública integrada a l'àrea d'Economia i Promoció Econòmica de l'Ajuntament de Barcelona.



**55.000**  
**persones ateses**



**7.000**  
**empreses ateses**

## Missió

Promoure l'ocupació de qualitat, l'esperit emprenedor, la competitivitat empresarial i la diversificació del teixit productiu, per assolir un model econòmic sostenible, inclusiu i just.

## Visió

Fer de Barcelona una ciutat de referència per treballar, emprendre i viure amb valors socials i ambientals.

## Valors

Ens mou l'esperit de servei públic i l'ètica professional i personal, així com la igualtat d'oportunitats i el progrés social. Treballem en cooperació dins l'organització i amb altres per a una economia social i sostenible al servei de les persones.

Segueix-nos a:



# Què fem?



**Acompanyem la ciutadania** durant tot el procés de recerca de feina.

[\*\*barcelonactiva.cat/treball\*\*](https://barcelonactiva.cat/treball)



**Ajudem les empreses i organitzacions** a créixer, connectar-se amb l'ecosistema i fer-se més competitives.

[\*\*barcelonactiva.cat/empreses\*\*](https://barcelonactiva.cat/empreses)



**Donem suport a les persones emprenedores** per convertir la seva idea de negoci en una empresa viable.

[\*\*barcelonactiva.cat/emprenedoria\*\*](https://barcelonactiva.cat/emprenedoria)



**Oferim formació** a les persones que cerquen feina, emprenedores i professionals.

[\*\*barcelonactiva.cat/formacio\*\*](https://barcelonactiva.cat/formacio)



# Xarxa d'equipaments de Barcelona Activa



## Seu Central

Oficines de Barcelona Activa.



## Centre d'Emprenedoria

L'equipament dels emprenedors i les emprenedores de la ciutat.



## Cibernàrium Nou Barris

Centre de formació digital d'iniciació ubicat al Parc Tecnològic.



## Porta22

2.000 m<sup>2</sup> per a l'ocupació i la carrera professional.



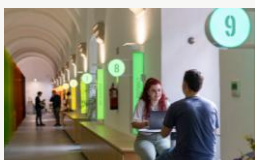
## Startup Lab

L'equipament de les empreses innovadores de nova creació.



## Parc Tecnològic

Clúster d'innovació al nord de la ciutat.



## El Convent

L'equipament referent en ocupació per a joves, a Ciutat Vella.



## Oficina d'Atenció a les Empreses

L'espai de referència per a les empreses i pimes de Barcelona.



## LIDERA

Espai per a dones professionals, directives i emprenedores.



## InnoBA

Centre per a la innovació socioeconòmica, a Ca n'Andalet.



## Cibernàrium 22@

Centre de capacitació tecnològica per a professionals i empreses.

## Espais Activa a la ciutat

- Nou Barris Activa
- Sant Andreu Activa
- Sants-Montjuïc Activa



# Barcelona Activa està present a més de 50 punts de la ciutat

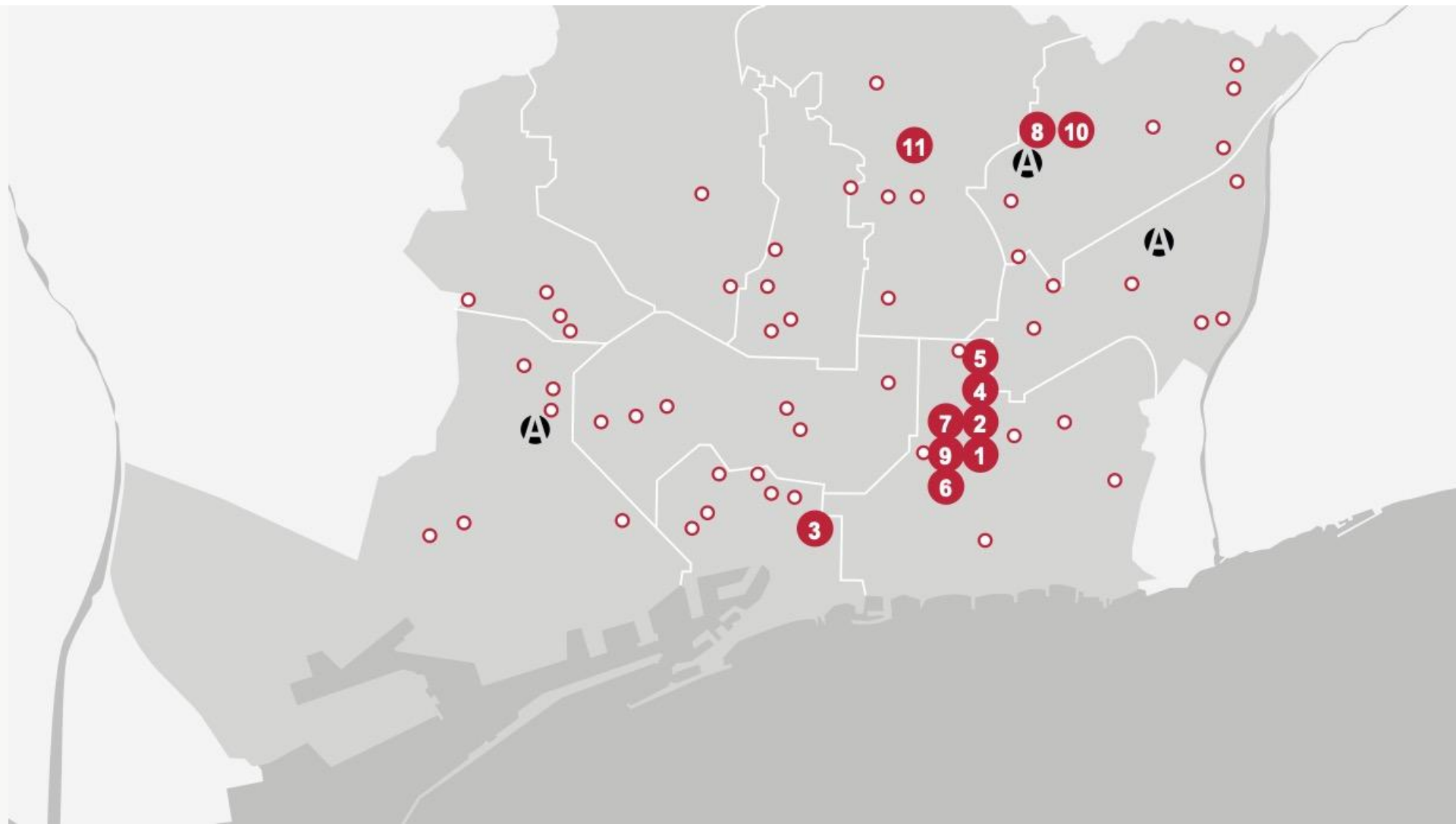
## Equipaments de Barcelona Activa

1. Seu Central
2. Porta22
3. El Convent
4. Centre d'Emprenedoria
5. Startup Lab
6. LIDERA
7. Cibernàrium 22@
8. Cibernàrium Nou Barris
9. Oficina d'Atenció a les Empreses
10. Parc Tecnològic
11. InnoBA

## Espais Activa a la ciutat

-  Nou Barris Activa
-  Sant Andreu Activa
-  Sants-Montjuïc Activa

 Altres punts d'atenció a la ciutat



# Xarxa Cibernàrium

La Xarxa Cibernàrium està distribuïda per tota la ciutat de Barcelona, oferint formació en diversos equipaments.

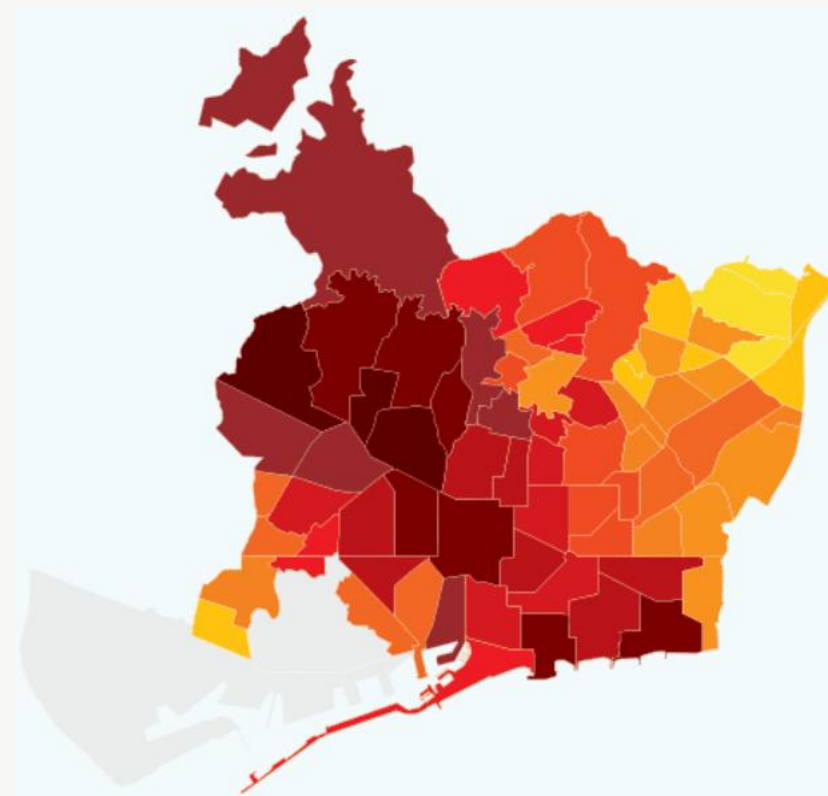
Recorda que també et pots formar en línia des de casa, amb [Aules Virtuals](#).

Consulta les activitats que pots realitzar als diferents equipaments:

- [Activitats a BIBLIOTEQUES](#)
- [Activitats a CIBERNÀRIUM NOU BARRIS](#)
- [Activitats a CANÒDROM](#)
- [Activitats a PLAÇA CATALUNYA \(Movistar Centre\)](#)
- [Activitats a SANTS-MONTJUÏC ACTIVA](#)



[On estem?](#)



# Formació tecnològica per a tothom



# Com protegir la teva seguretat online



1. Programari maliciós i programari no desitjat
2. Tipus i efectes del programari maliciós
3. Com podem protegir-nos? Antivirus i Tallafocs
4. Contrasenyes i gestors de contrasenyes
5. Protecció de dades de caràcter personal
6. Privadesa a les xarxes socials
7. Privadesa en la navegació
8. Vols ampliar el teu coneixement?
9. Sabies què?

# 1. Programari maliciós (Malware) (I)



Quan naveguem per internet estem **exposats a diferents problemes** que poden afectar a la nostra seguretat i privacitat. Per això és important conèixer-los per saber quins són, com actuen i què podem fer per prevenir-los.

**L'objectiu del Malware** és obtenir algun benefici econòmic o d'un altre tipus que pot suposar:

- ☐ Robatori d'informació.
- ☐ Danys al sistema.
- ☐ Extorsió o xantatge
- ☐ Control remot del sistema
- ☐ Molèsties com mostrar anuncis no desitjats, alentir el funcionament de l'ordinador.



# 1. Programari maliciós i programari no desitjat (II)

El **programari maliciós** es pot propagar de diverses maneres:

- ☐ Per correus electrònics amb adjunts maliciosos.
- ☐ Descàrregues de programes no fiables.
- ☐ Vulnerabilitat del sistema a través de diferents navegadors.
- ☐ Amb dispositius extraïbles: USB o discs durs externs.
- ☐ A través de xarxes socials o missatgeria instantània.



El **programari no desitjat** es aquell que s'instal·la els nostres ordinadors sense consentiment explícit. Tot i que no es maliciós com un virus pot ser molest, perquè mostra molta publicitat, por alentir l'ordinador o recopilar dades.

El **programari no desitjat** es propaga també de diverses maneres:

- ☐ A través de instal·lacions de programes gratuïts
- ☐ Amb anuncis enganyosos.
- ☐ Descarregues de llocs webs no oficials.



## 2. Tipus i efectes del programari maliciós

Els tipus més comuns de programari maliciós son:

- ❑ **Virus** que s'adhereixen a programes o documents quan es fan servir. Fins i tot poden eliminar aquets documents.
- ❑ **Cucs**, són com els virus però es propaguen de forma més ràpida sense necessitat d'obrir programes o documents.
- ❑ **Troians**, semblen programes autèntics però un cop instal·lats obren portes per robar dades.
- ❑ **Ransomware**, xifren el dispositiu perquè no es pugui fer servir i demanen una recompensa a canvi.
- ❑ **Adware**, mostra publicitat no desitjada.
- ❑ **Rootkits**, permeten a un tercer accedir al teu dispositiu i no es pot detectar.
- ❑ **Botnets**, son xarxes d'ordinador afectats controlats per un atacant per enviament de Spam.



### 3. Com podem protegir-nos?

**Programari  
maliciós**

**Programari  
maliciós**



- ☐ Antivirus
- ☐ Tallafocs
- ☐ Actualitzacions de seguretat
- ☐ Còpies de seguretat
- ☐ Limitar permisos
- ☐ Sentit comú

El **programari maliciós** és una amenaça constant al món digital i és molt important la prevenció i la vigilància són claus per mantenir els nostres sistemes segurs.

### 3. Com podem protegir-nos?

## Antivirus (II)

Un **antivirus** és un programa informàtic utilitzat per a prevenir, detectar i eliminar virus informàtics maliciosos. La majoria d'aquests programes també estan capacitats per a detectar altres amenaces.

**Antivirus**



1. Gratuïts
  2. Pagament (més opcions de protecció)
- 
1. En línia (Menys eficaços, no hi ha protecció permanent, només escaneig)
  2. Escriptori

# Antivirus

## 3. Com podem protegir-nos?

### Tallafocs (III)

Un **tallafoc** o **Firewall** és un element de maquinari o programari utilitzat en una xarxa o equip informàtic per controlar les comunicacions, permetent-les o denegant-les segons la configuració que li haguem donat. Un tallafoc configurat correctament afegeix protecció extra.

Aconsegum:

- ✓ Protegir la informació d'atacs externs.
- ✓ Mantenir la privacitat de la informació.
- ✓ Impedir l'ús abusiu dels serveis.

● **Tallafoc: Activat**

Desactivar el tallafoc

El tallafoc està activat i configurat per evitar que aplicacions, programes i serveis no autoritzats acceptin connexions d'entrada.

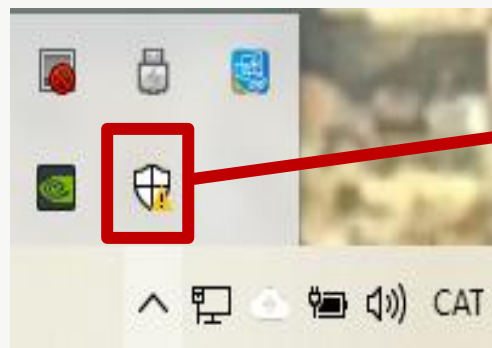
Opcions del tallafoc...

Si tenim instal·lat un antivirus i ho complementem amb un tallafocs aconseguim un bon sistema de protecció.

# Tallafocs

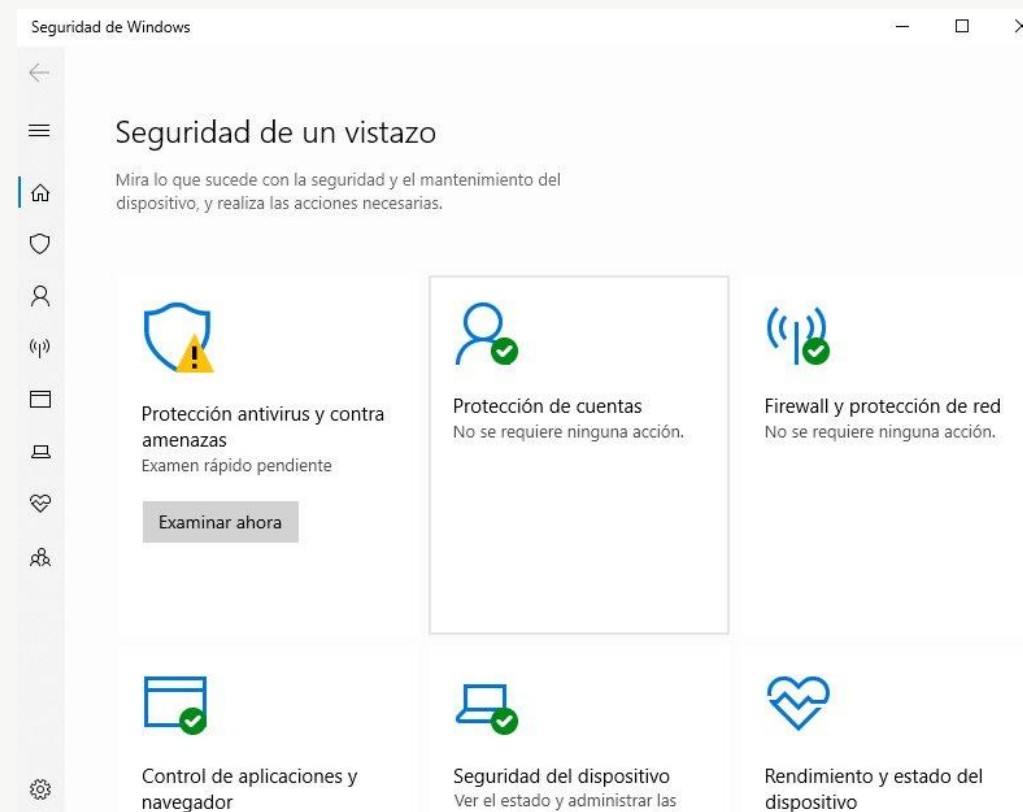
### 3. Com podem protegir-nos? La seguretat a Windows (TV/)

## La seguretat a Windows



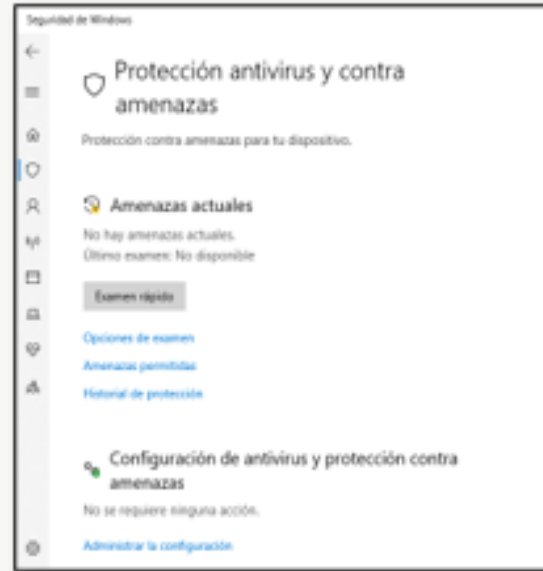
Botó per accedir a "Seguretat de Windows", des de la barra d'inici

Accedim a aquest panell des d'on podem gestionar la seguretat: Antivirus, Tallafocs

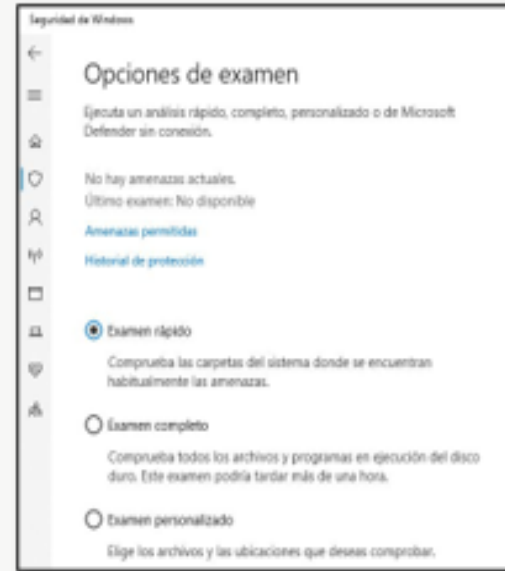


### 3. Com podem protegir-nos? La seguretat a Windows (TV)

## La seguretat a Windows



Panell per realitzar un anàlisi de virus. Podem analitzar tot el PC, carpetes o arxius concrets.



Panell del Tallafocs (Firewall)



## 4. Contrasenyes i gestors de contrasenyes

Una altra mesura de protecció són les **contrasenyes**, que són la primera línia de defensa per protegir la nostra informació. Actualment gairebé tots els nostres dispositius i les nostres aplicacions requereixen una contrasenya, per aquest motiu és molt important **crear contrasenyes segures**.

**COTRASENYA SEGURA**



**entre 8 i 12 caràcters + Majúscules +  
Minúscules + Números + Símbols**

Les contrasenyes han de ser:

**ORIGINALS**

No facis servir informació personal com el nom, la data de naixement o el nom de la mascota.

**ALEATORIES**

Evita seqüències de números o paraules.

**EXCLUSIVES**

No facis servir la mateixa contrasenya per diferents aplicacions o comptes.



[Vídeo Càpsula Contrasenyes Segures](#)

**Contrasenyes  
segures**

## 4. Contrasenyes i gestors de contrasenyes

Si fem servir moltes contrasenyes podem **utilitzar una aplicació per gestionar-les**. Aquestes aplicacions permeten emmagatzemar diverses contrasenyes en un únic compte i clau.

A la botiga d'aplicacions del vostre mòbil en podeu trobar diverses.

Alguns exemples de **Gestors de Contrasenyes**



[Dashlane](#)



[Keeper](#)



[LastPass](#)



[1Password](#)

**Contrasenyes  
segures**

# 5. Protecció de dades de caràcter personal

La protecció de dades és un **dret fonamental** que garanteix a les persones el control sobre la seva informació personal. Aquest dret fonamental està regulat pel **Reglament General de Protecció de Dades (RGPD)** regulat al 2016/679 del Parlament Europeu i Consell de 27 d'abril de 2016 que a Espanya es complementa per la **Llei Orgànica de Protecció de Dades Personals i garantia del drets digitals (LOPDGDD)**.

- ☐ Dret d'accés
- ☐ Dret de rectificació
- ☐ Dret d'oposició
- ☐ Dret de supressió ("a l'oblit")
- ☐ Dret a la limitació del tractament
- ☐ Dret a la portabilitat



<https://www.aepd.es/>

## Dades pròpies

**Pràctica 1** - Consulta els drets que protegeixen les teves dades de caràcter personal a l'AEPD. Es mencionen a la política de privacitat dels llocs web que acostumem a visitar?

## 6. Privadesa a les xarxes socials

### Xarxes socials

És molt important que **establim el control** sobre la nostra informació personal a les xarxes socials, hem de controlar:

- ☐ Qui pot veure la teva informació personal, publicacions i activitat
- ☐ Qui et pot trobar, contactar i etiquetar
- ☐ Quines aplicacions poden accedir al teu compte
- ☐ Ubicació i personalització d'anuncis



**Pràctica 2** - Revisa els ajustaments de privadesa del teu compte a una xarxa social que facis servir habitualment. Estàs compartint allò que pensaves?

# 7. Privadesa en la navegació

La privacitat a la navegació fa referència al **grau de control que tenim sobre la nostra informació** personal mentre naveguem per les xarxes. En el moment que obrim un navegador ja deixem una **empremta digital** que pot ser rastrejada i recopila informació nostra. Es important:

- ☐ Triar un **navegador** centrat en la privacitat: Brave, Firefox, DuckDuckGO Browser)
- ☐ Utilitza un **cercador** també centrat en la privacitat: DuckDuckGO o Startpage.
- ☐ **Gestiona les cookies**: fes neteja regularment, configura-les.
- ☐ Navega en mode **privat/ incògnit**.
- ☐ Sigues prudent amb la **informació que comparteixes**: formularis, acceptació de cookies...
- ☐ **Revisa els permisos** dels llocs webs abans d'acceptar.



## Navegador

**Pràctica 3** - Prova les següents opcions de privadesa de Google Chrome. Troba-les també al dispositiu mòbil.

# 8. Vols ampliar els teus coneixements?

Saber navegar per la xarxa és molt útil pel nostre dia a dia, però hem de ser conscients que ho hem de fer amb **seguretat i protegint-nos de possibles amenaces**, per aquest motiu hem de seguir els següents consells:

1. **Sigues conscient de les estafes en línia** com per exemple el **Phishing** (robatori de les nostres dades): desconfia dels correus electrònics, SMS o missatges que ens **demanen dades personals**. **Verifica sempre el remitent d'aquests missatges** i no et deixis portar per les emocions.
2. **Utilitza connexió HTTPS** sempre que sigui possible: assegurat que la URL comença per https://, per tant evita els llocs que només comencin per http://.
3. **Mantén els teus programes actualitzats**: el sistema operatiu, el navegador i altres programes habituals com reproductors, editors....
4. **Vigila amb el Wi-Fi públic**: sovint son insegures perquè no estan xifrades i qualsevol persona pot accedir al teu dispositiu a través d'elles, no facis transaccions bancaries ni compres online quan estiguis connectat en aquestes xarxes.
5. **Utilitza antivirus**: un cop instal·lat al teu dispositiu tingues l'antivirus actualitzat, fes revisions sovint.
6. **Fes còpies de seguretat** en un disc dur o núvol.
7. **Revisa els permisos** de les aplicacions y webs abans d'accedir-hi.



## 9. Sabies què?



El **Reglament General de Protecció de Dades (RGPD)** de la Unió Europea **és el més estricte del món** en matèria de protecció de dades.

Aquest reglament s'ha establert a Europa però afecta a la resta del món, d'aquesta manera **les empreses i organitzacions que volen treballar a Europa han de seguir aquesta normativa** dins i tot si la seva seu social està fora d'aquest territori.



Font de la imatge: [Universitat de Valencia](https://www.universitatdevalencia.es/)

**Web amb enllaços per practicar i aprendre més:**

[bit.ly/IT3Taller6](https://bit.ly/IT3Taller6)



[barcelonactiva.cat](http://barcelonactiva.cat)