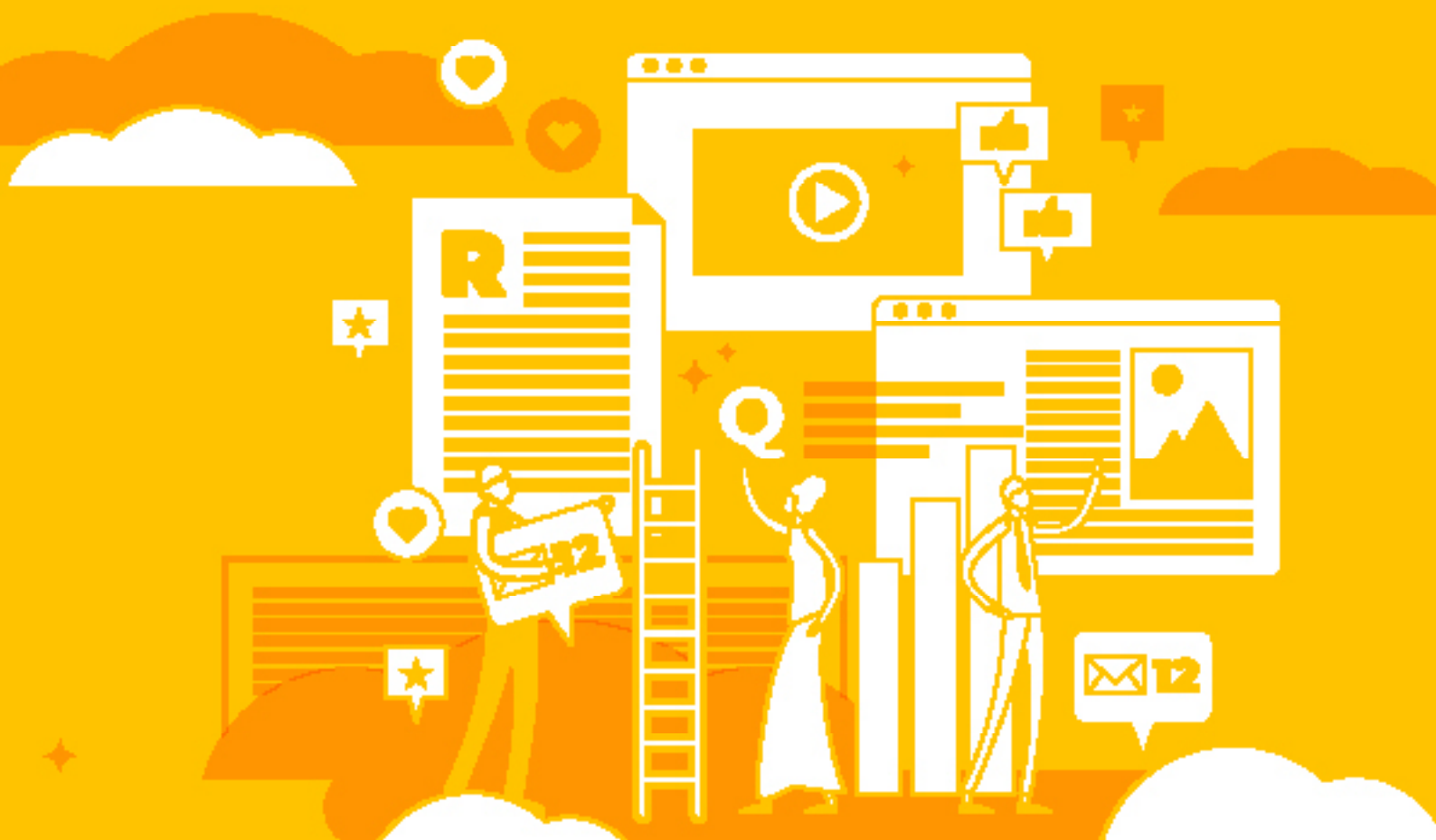




Formació en  
Competències  
Digitals

1

# Cerca i gestió d'informació i dades



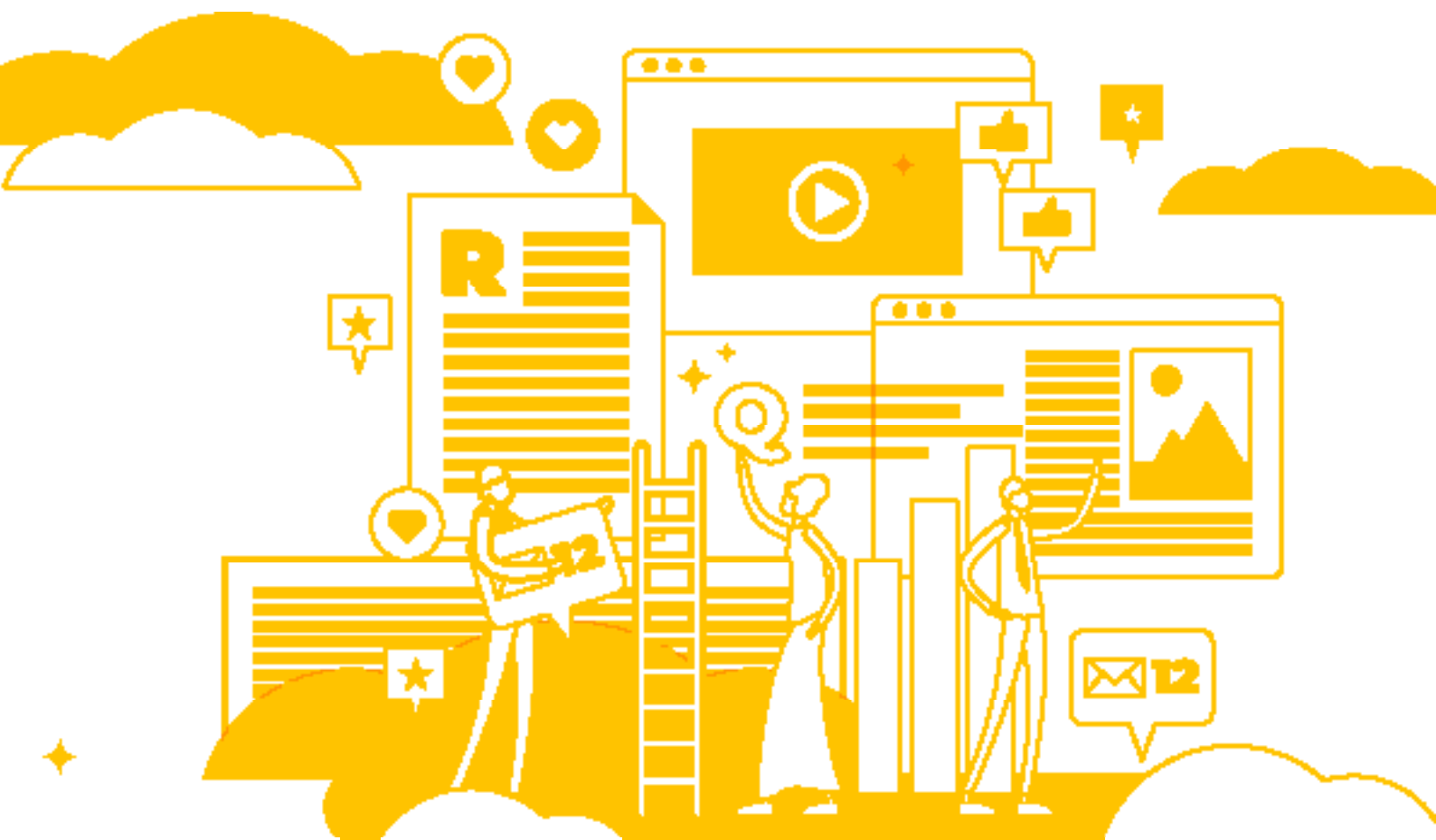


Formació en  
Competències  
Digitals



Cerca i gestió  
d'informació i dades

***Nivell B2***





## Cerca i gestió d'informació i dades

# ÍNDEX

### 1.1. NAVEGAR, CERCAR I FILTRAR DADES, INFORMACIÓ I CONTINGUTS DIGITALS

- [\*L'accessibilitat web a la navegació i cerca a Internet\*](#)
- [\*La navegació i cerca d'informació a xarxes socials\*](#)

### 1.2. AVALUAR DADES, INFORMACIÓ I CONTINGUTS DIGITAL

- [\*Guia metodològica per a la identificació del pescaclics\*](#)
- [\*Guia metodològica per a la identificació de continguts patrocinats\*](#)
- [\*Aplicació avançada de la IA a la gestió de continguts\*](#)

### 1.3. GESTIÓ DE DADES, INFORMACIÓ I CONTINGUTS DIGITALS

- [\*Gestió de dispositius\*](#)
- [\*Gestió de continguts comprimits\*](#)
- [\*Gestió de continguts de còpia de seguretat\*](#)



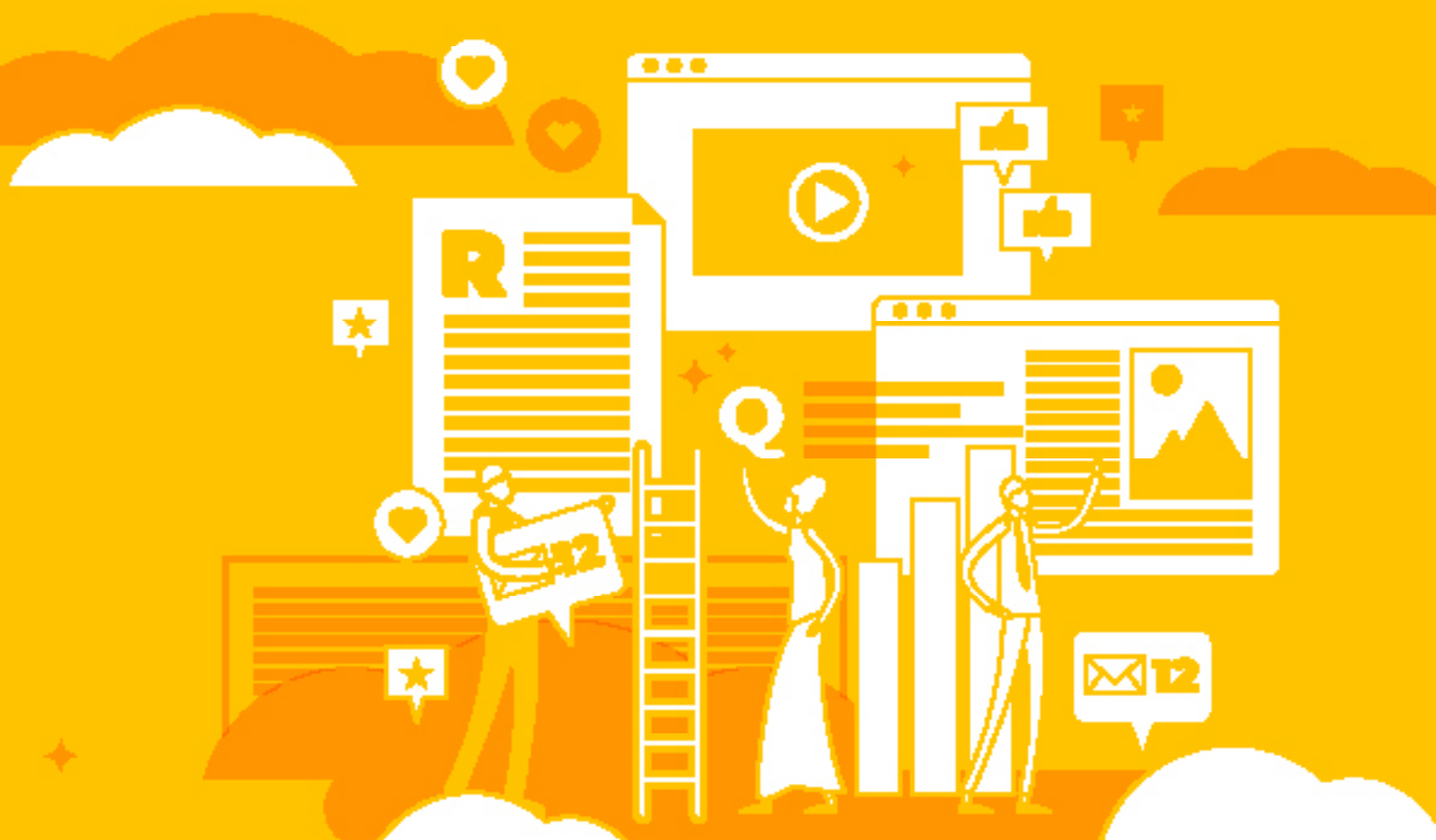


# DigitAll

Cerca i gestió  
d'informació i dades

## 1.1

### NAVEGAR, CERCAR I FILTRAR DADES, INFORMACIÓ I CONTINGUTS DIGITALS





Cerca i gestió  
d'informació i dades

**Nivel B2** 1.1 Navegar, cercar i filtrar dades,  
informació i continguts digitals

# L'accessibilitat web a la navegació i cerca a Internet





## Accessibilitat web en la navegació i en la cerca d'informació

La navegació i cerca d'informació a Internet es fa mitjançant navegadors i emprant diferents estratègies i eines de cerca. Tanmateix, l'accés a aquestes tecnologies no sempre és viable per a tothom per raó d'alguna mena de limitació, com poden ser discapacitats o malalties.

Per minvar la possible bretxa social a causa de les limitacions d'accés a les tecnologies, durant les darreres dècades s'ha desenvolupat una sèrie de normatives i guies que orienten els usuaris en com aconseguir que el disseny i desenvolupament de les pàgines, així com que els diferents llocs i portals web siguin tan entenedors com sigui possible.

L'objectiu d'aquest document és revisar el concepte d'accessibilitat per a la navegació a la xarxa i descriure algunes eines i funcionalitats bàsiques presents a navegadors i eines de cerca que faciliten que la navegació per Internet sigui més accessible.



Imatge 1. Alumnes amb discapacitat de Down Madrid treballant en el curs de Tecnologia de la Informació i Comunicació sobre la importància de l'accessibilitat de les pàgines web per garantir un accés a la informació sense barreres.

Font: Tecnobility. Foto: DOWN MADRID ([e.digitall.org.es/tecnobility](https://e.digitall.org.es/tecnobility)).



## Accessibilitat web: definició i normatives

L'accessibilitat web es refereix a una pràctica tecnològica per dissenyar i desenvolupar pàgines, llocs i portals web. És coneguda, a més, com una pràctica inclusiva, perquè defineix estàndards i criteris perquè aquests productes informàtics puguin ser utilitzats per persones amb discapacitat.

Segons el portal de l'**Administració Electrònica d'Espanya** ([e.digitall.org.es/normas-accesibilidad](https://e.digitall.org.es/normas-accesibilidad)), i en relació amb els criteris d'accessibilitat web, el desenvolupament tecnològic al país es guia fonamentalment per la norma de la Unió Europea 301 549 v3.2.1 (2021-03) "Requisits d'accessibilitat per a productes i serveis TIC", que especifica els criteris d'accessibilitat aplicables a productes i serveis que incloguin TIC (llocs web, programari, apps, documents, maquinari, etc.) i per les pautes d'accessibilitat al contingut web (WCAG) 2.1 establertes per la W3C.

### NOTA

#### W3C

Consorti WWW (en anglès: *World Wide Web Consortium*) és un consorci internacional que genera recomanacions i estàndards que assegurin el creixement de la World Wide Web a llarg termini.

Adreça web: [w3.org](https://w3.org)

### Saber-ne més

Per aprofundir en l'accessibilitat web i en les normatives, es pot consultar l'adreça web:

- Norma EN 301 549 v3.2.1 (2021-03): [e.digitall.org.es/norma-en](https://e.digitall.org.es/norma-en)
- Pautes d'accessibilitat al contingut web (WCAG) 2.1: [e.digitall.org.es/WCAG](https://e.digitall.org.es/WCAG)





## Funcionalitats i eines bàsiques d'accessibilitat web útils en la navegació i cerca d'informació

Per a la navegació i cerca d'informació a Internet s'han desenvolupat funcionalitats que en faciliten l'accessibilitat als usuaris. Les funcionalitats més utilitzades són les següents:

- **Visualització de pàgines web**

- 1| **Canviar la mida de la font**

Per canviar-ne la mida, es pressiona la tecla **CTRL** i el símbol **+** per augmentar-la o el **-** per disminuir-la. Una altra manera seria pressionar la tecla **CTRL** i moure alhora la roda del ratolí. Igualment, una altra opció és desplegar el menú de la cantonada superior dreta i accedir a l'opció de **Zoom** per modificar-ne la mida. També podria fer-se directament a través de la icona en forma de lupa.

- 2| **Canviar el color del text i del fons de la pàgina web**

Per fer-ho, s'ha d'accedir a la configuració del navegador i, posteriorment, a la secció d'aspecte.

- **Configuració d'idioma**

- 1| **Canviar l'idioma preestablert al navegador**

Per això, a Configuració heu d'accedir a l'opció Idiomes i seleccionar el que desitgeu.

- 2| **Traduir una pàgina web**

Una vegada que ha obert la pàgina web que vol traduir, ha de fer clic dret i anar a l'opció traduir a l'espanyol.

És important destacar que aquesta funcionalitat no està sempre habilitada, perquè depèn de diversos factors com el tipus de navegador i configuració de la pàgina, lloc o portal web. Així i tot, en la majoria dels casos, es podrà traduir el contingut digital.





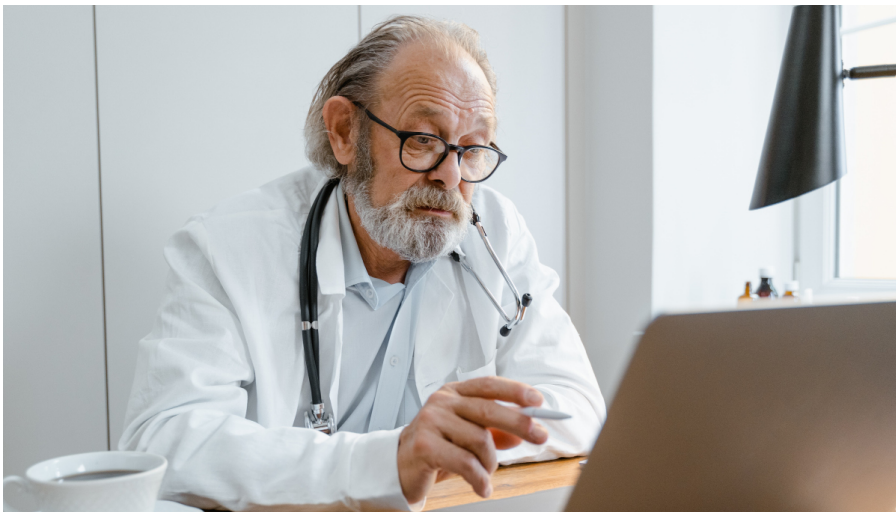


- **Accés sense ratolí o mouse**

Les persones que no puguin utilitzar un ratolí poden emprar diversos comandaments per moure's o fer alguna acció dins d'una pàgina web com, per exemple:

- 1 | **TAB**. Permet anar directament a cada enllaç web que estigui dins d'una pàgina web.
- 2 | **MAJ+TAB**. Retrocedeix entre els elements d'una pàgina web.
- 3 | **ESC**. Atura la descàrrega d'una pàgina.
- 4 | **F5**. Actualiza la pàgina actual.
- 5 | **ALT +D**. Accedeix a la barra de les direccions.
- 6 | **ALT+FLETXA A L'ESQUERRA**. Permet anar a la pàgina anterior.
- 7 | **MAJ+F10**. Mostra un menú contextual per a un vincle.
- 8 | **CTRL+TAB**. Permet avançar entre marcs.

Una altra de les funcionalitats que destaquen als dispositius mòbils i ordinadors per accedir ràpidament a diferents funcions és el **dictat per veu**. Aquesta funció és molt útil per als usuaris, ja que permet emprar l'ordinador emprant les mans el mínim. Un exemple d'això són els programaris de reconeixement de veu *Invox Medical (Vócali)* i *Dragon Medical*, que s'utilitzen als centres sanitaris i hospitals d'algunes comunitats autònomes del nostre país. Gràcies a la seva implantació, es va aconseguir augmentar la productivitat clínica a causa de la rapidesa i precisió amb la qual el programari trasllada veu a text, cosa que permet la ràpida elaboració de documents de diagnòstic i judici clínic.



**NOTA****Invox Medical i Dragon Medical**

**Invox Medical** i **Dragon Medical** són dues solucions de programari de veu desenvolupades per facilitar la transcripció d'informes mèdics. En teniu més informació en les següents adreces web.

- Adreça web: [e.digitall.org.es/invox-medical](https://e.digitall.org.es/invox-medical)
- Adreça web: [e.digitall.org.es/dragon-medical](https://e.digitall.org.es/dragon-medical)

**Saber-ne més****Dictat per veu**

Per aprofundir en com habilitar i utilitzar el dictat de veu en algun programari i dispositius, podeu consultar les següents adreces web:

- Activació per veu en sistema operatiu Windows: [e.digitall.org.es/windows-dictado](https://e.digitall.org.es/windows-dictado)
- Dictat a iPhone: [e.digitall.org.es/ios-dictado](https://e.digitall.org.es/ios-dictado)
- Dictat de documents a Word: [e.digitall.org.es/word-dictado](https://e.digitall.org.es/word-dictado)

D'altra banda, quan s'utilitza qualsevol eina de cerca, podeu seguir aquests passos per arribar a un resultat determinat:

- Prémer la tecla Tabulador (**TAB**) fins a arribar a l'enllaç que desitgeu.
- Prémer la tecla Intro (**ENTER**) per accedir a l'enllaç que desitgeu.

Pel que fa a l'ús web, s'aprofundeix en aquest contingut en altres documents complementaris.

**Saber-ne més****Accessibilitat web**

Per aprofundir en la qüestió de l'accessibilitat web, podeu consultar el material didàctic elaborat pel Ministeri d'Educació i Ciència.

Adreça web: [e.digitall.org.es/accesibilidad-web](https://e.digitall.org.es/accesibilidad-web)

**ATENCIÓ****Advertiments i errors freqüents que s'haurien d'evitar**

Al navegador, en variar la mida de la font, heu de tenir cura quan utilitzeu la roda del ratolí, ja que pot engrandir o disminuir dràsticament la mida de la lletra.



**Cerca i gestió  
d'informació i dades**

**Nivell B2 1.1** Navegar, cercar i filtrar dades,  
informació i continguts digitals

# La navegació i cerca d'informació a les xarxes socials





## La navegació i cerca d'informació a les xarxes socials

Les xarxes socials permeten cercar i compartir informació, així com comunicar-se i interaccionar amb altres usuaris. No hi existeixen estratègies de cerca estructurades com les que s'han après a nivells anteriors per localitzar informació. Per aquest motiu, l'objectiu d'aquest document és descriure accions per a la navegació i cerca d'informació a xarxes socials.

Per això, s'oferiran continguts relacionats amb la navegació i cerca d'informació, filtratge i selecció d'aquests continguts digitals; avantatges i desavantatges de la cerca d'informació a les xarxes socials; cercadors de continguts de xarxes socials; privacitat i normatives legals a l'hora de navegar; i, la cerca d'informació a les xarxes socials.

### Les diferents vies de cerca d'informació a les xarxes socials

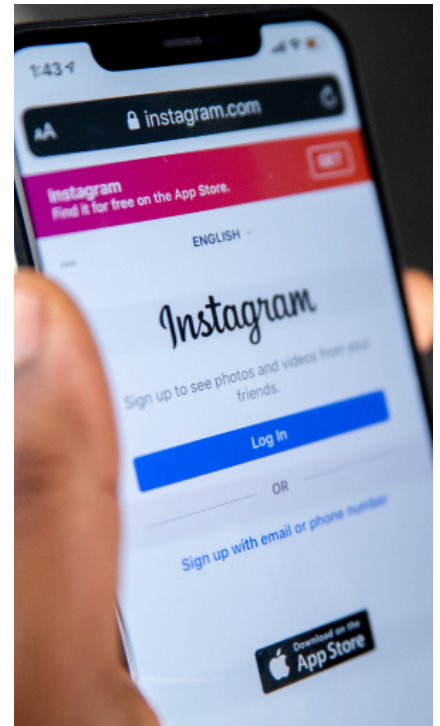
Les xarxes socials faciliten als usuaris llibertat i autonomia per navegar i publicar el que vulguin sempre tenint en compte determinats termes i condicions ètiques. En aquest context, resulta essencial la responsabilitat i el respecte a l'hora de comentar, compartir o publicar continguts, per tal d'evitar la perpetuació d'estereotips i tendències com les notícies falses no verificades o els continguts ofensius o antiètics.

Per cercar informació a les xarxes socials, podeu emprar diferents vies: mitjançant etiquetes (#), arroves (@), paraules clau i grups temàtics.

- **Cerca per etiqueta (#)**

L'etiqueta és una paraula clau "clicable". És a dir, una cadena de caràcters (una o diverses paraules concatenades i precedides per un coixinet o numeral). Permet relacionar i interactuar amb continguts digitals similars com, per exemple: #covid19, #cuina, etc.

El primer que cal fer en aquesta mena de cerques és identificar termes que en defineixin l'objectiu. Per exemple: #educació i #cuinaespanyola. Després, al cercador de la





xarxa social seleccionada (Facebook, X, LinkedIn, Instagram, etc.) s'haurà d'introduir l'etiqueta, per la qual cosa es retornaran totes les publicacions associades amb el concepte. Heu de saber que, mentre escriviu l'etiqueta en el cercador, es mostraran altres termes semblants i d'interès per a la vostra cerca. En tot cas, volem recomanar-vos que llegiu amb deteniment les etiquetes proposades per la xarxa social en qüestió, ja que diversifiquen els resultats de cerca.

- **Cerca per arrova (@)**

Per fer una cerca per arrova (@), primer heu de saber que és un identificador d'un usuari a una xarxa social. Això és que pot ser una persona o una representació de qualque institució, grup, empresa, etc. La cerca per aquest criteri es fa també mitjançant el cercador de la mateixa plataforma. Per això, cal que empreu la paraula reservada @ seguida del nom del perfil o compte. Per exemple, a Facebook @ **UNIAAndalucia** ([facebook.com/UNIAAndalucia](https://www.facebook.com/UNIAAndalucia)) fa referència al perfil de la Universitat Internacional d'Andalusia, però @ **UNIAuniversidad** ([twitter.com/UNIAuniversidad](https://twitter.com/UNIAuniversidad)) fa referència a la mateixa institució a X, i @ **uniauniversidad** ([instagram.com/uniauniversidad](https://www.instagram.com/uniauniversidad)) a Instagram.

- **Cerca per paraules claus**

Per fer aquest tipus de cerca es procedeix de manera similar a la cerca per paraules claus als cercadors i metacercadors. És a dir, heu d'aplicar els passos següents:

- 1 | Determinar els criteris de cerca**

Per això, heu de respondre les preguntes següents: Què vull cercar? Quin és l'objectiu de la meua cerca?

- 2 | Determinar la paraula clau**

En aquest moment, heu d'identificar una paraula clau o seqüència de termes que responguin als criteris de cerca establerts. Per exemple: "venda de cases" o "COVID-19".

- 3 | Utilitzar el cercador de la xarxa social**

- 4 | Una vegada identificada la paraula clau, heu d'introduir-la al cercador**

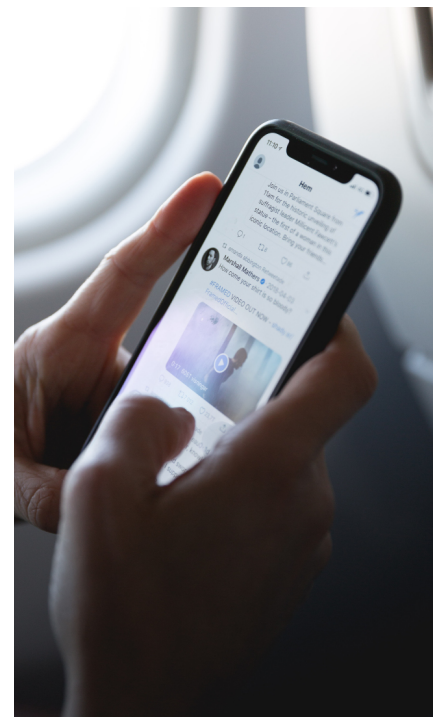
- 5 | Filtrar i triar la informació necessària**

- 6 | Triar i verificar la informació obtinguda**

### NOTA

#### L'arrova (@) a xarxes socials

És important saber que no sempre el nom d'una etiqueta es relaciona exactament amb el perfil que voleu cercar. Per tant, se suggereix sempre revisar els resultats de cerca.





## • Cerca d'informació en grups temàtics presents a xarxes socials

Generalment, es considera un grup a dues o més persones que comparteixen idees, valors, normes i cultures, i que es presenten com a tal davant les altres persones. Entre els membres s'intercanvien diàlegs i idees, i entre els principals avantatges destaquen la creació de comunitats expertes o grups temàtics com, per exemple: grups que integren amants o seguidors de l'alta cuina, cotxes, animals, música o un cantant concret. Hi ha diverses xarxes socials permeten crear grups, siguin privats o públics, entre les quals destaquen Facebook, Instagram o TikTok. Per navegar i cercar informació present en grups, podeu aplicar les accions següents:

### 1 | Determinar l'àrea temàtica

Per això heu de conèixer quin és l'objectiu de cerca i relacionar-lo amb una temàtica. Per exemple, si voleu cercar com ensenyar als vostres fills matemàtiques, podríeu optar per: educació matemàtica.

### 2 | Seleccionar la xarxa social

En coherència amb el tipus de format que desitgeu obtenir o el nivell d'aprofundiment del contingut, haureu de triar una xarxa social o una altra. Per exemple, si voleu localitzar imatges o vídeos, podeu optar per **Facebook** ([facebook.com](https://www.facebook.com)) o **TikTok** ([tiktok.com](https://www.tiktok.com)) i, si desitja buscar informació acadèmica, pot utilitzar **ResearchGate** ([researchgate.net](https://www.researchgate.net)) o **LinkedIn** ([linkedin.com](https://www.linkedin.com)).

### 👁️ NOTA

#### El grup a xarxes socials

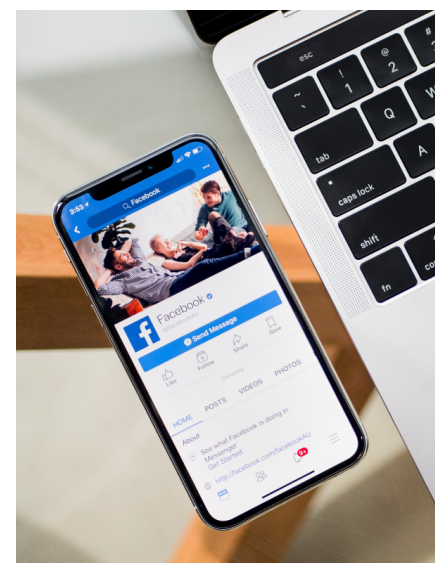
En algunes xarxes socials hi ha grups privats als quals hauràs de sol·licitar membres (permisos) per accedir a la seva informació.

### 📘 Saber-ne més

Per aprofundir en la cerca d'informació a les xarxes socials, podeu consultar els següents enllaços:

- Facebook: [e.digitall.org.es/facebook](https://e.digitall.org.es/facebook)
- X: [e.digitall.org.es/twitter](https://e.digitall.org.es/twitter)
- TikTok: [e.digitall.org.es/tiktok](https://e.digitall.org.es/tiktok)
- Instagram: [e.digitall.org.es/instagram](https://e.digitall.org.es/instagram)

En qualsevol variant que utilitzeu per cercar informació a xarxes socials, sempre heu de filtrar i seleccionar la informació. És per això que en el pròxim epígraf coneixereu accions i eines per a aquest fi.

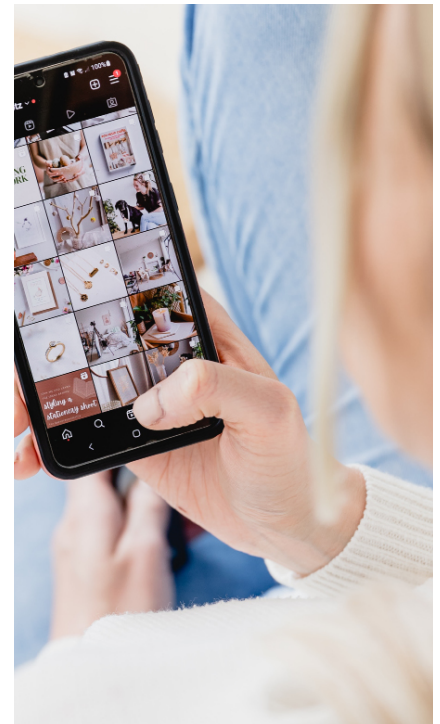




## Filtratge i selecció de la informació a les xarxes socials: accions i eines

Una vegada heu obtingut la informació a xarxes socials, heu de filtrar-la i seleccionar-ne aquella que realment respongui als vostres interessos. Per això, podeu aplicar els criteris següents:

- **Verificar el text que trobeu a la xarxa social en qüestió**  
Les informacions presents a xarxes socials normalment es repeteixen o apareixen a diversos llocs, pàgines o portals web institucionals. Per això, us suggerim fer una cerca a Internet aplicant paraules clau amb la finalitat de verificar-ne la veracitat.
- **Avaluar-ne la font**  
La primera passa és constatar el perfil de l'usuari que comparteix la informació. El coneixeu o hi teniu confiança? A més, podeu verificar els comentaris d'altres usuaris sobre aquesta informació obtinguda.
- **Verificar-ne el lloc i data**  
És important verificar quan es va publicar la informació (text, imatge, àudio o vídeo). Generalment, les informacions falses provenen de llocs i temps remots que, a vegades, les audiències tendeixen a creure.
- **Verificar la informació real vs. viral**  
Hi ha molta informació a les xarxes socials que es difon amb el propòsit d'obtenir clics o visualitzacions, cosa que crea històries sensacionalistes que, en general, no són reals.
- **Verificar la informació presentada en imatges**  
Un dels formats més emprats per falsejar informació a les xarxes socials és la imatge, ja que és altament manipulable mitjançant sistemes d'edició fotogràfica. Per això, per verificar l'autenticitat de la imatge, us volem recomanar que apliqueu la cerca inversa d'imatges mitjançant llocs web especialitzats com **TinEye** ([tinEye.com](https://tinEye.com)).
- **Verificar la informació presentada en vídeos**  
Igual que les imatges, els vídeos són un altre recurs molt emprat per a la difusió d'informació falsa a xarxes socials. En aquest sentit, també us suggerim verificar la font i data de publicació, així com parar esment als detalls del



### **NOTA**

#### **TinEye**

Motor de búsqueda de imágenes inversas desarrollado por Idée, Inc., empresa con sede en Toronto (Ontario, Canadá). Al adjuntar una imagen o añadir su URL, el sistema te permitirá comprobar su veracidad.

Dirección web: [tinEye.com](https://tinEye.com)



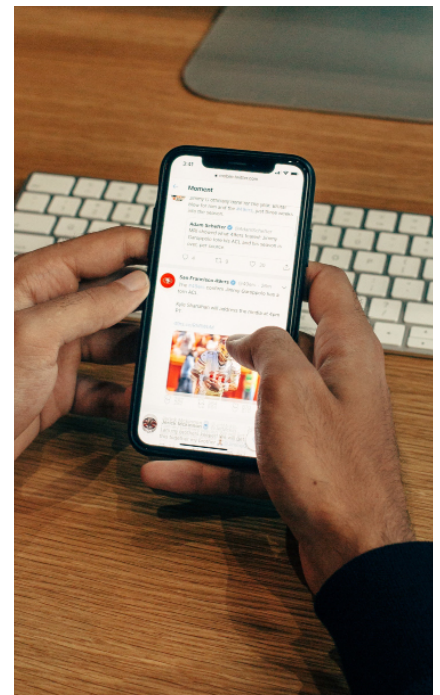
vídeo (manca de projecció d'ombres d'objectes, qualitat d'imatge, etc.). També podeu utilitzar editors de vídeo que us permetin separar el fitxer en els quadres constituents. Per exemple, podeu emprar aquests programaris gratuïts: **VLC** ([videolan.org/vlc](http://videolan.org/vlc)), **Avidemux** ([e.digitall.org.es/avidemux](http://e.digitall.org.es/avidemux)) o **Vegas Pro** ([e.digitall.org.es/vegaspro](http://e.digitall.org.es/vegaspro)).

- **Verificar la informació reproduïda a un àudio**  
No són només els vídeos i les imatges que poden ser manipulats, també ho pot ser l'àudio.

## Avantatges i desavantatges de la cerca d'informació a les xarxes socials

Hi ha estudis científics que demostren avantatges i desavantatges de la cerca d'informació a les xarxes socials, entre aquests en destaquen:

- **Tendències i conseqüències positives:**
  - 1| Milloren l'accés a la informació digital.
  - 2| Faciliten el contacte directe amb altres persones en el moment que trobeu convenient, pot ser per via síncrona o asíncrona. Això permet contactar amb l'autor de la publicació que vau trobar a les xarxes socials.
  - 3| Contribueixen a desenvolupar l'aprenentatge mitjançant la interacció amb la informació digital (en format text, imatge, àudio o vídeo) i els intercanvis mitjançant xats, grups, fòrums o pàgines web que ofereixen les mateixes plataformes.
- **Tendències i conseqüències negatives:**
  - 1| Incrementen el consum d'informació falsa.
  - 2| Augmenten la possibilitat de patir assetjament. Això es deu a causa de l'empremta digital que es deixa a les xarxes socials i a Internet. Cada vegada que accedim a Internet, hi ha la possibilitat de deixar empremtes, com per exemple: comentaris escrits a xarxes socials, imatges compartides i descarregades, l'adreça IP (adreça electrònica que especifica des de quin ordinador o dispositiu mòbil s'accedeix), informació del vostre perfil, etc. Per tant, cal tenir en compte els aspectes de privacitat i seguretat informàtica.





**NOTA****Empremta digital a xarxes socials i Internet**

Existeixen dos tipus d'empremta digital a Internet.

- **Passiva:** són dades que les plataformes digitals obtenen sense que sigui conscient d'això, per exemple: geolocalització, quantes vegades accedeix a un lloc web determinat i adreça IP.
- **Activa:** són dades ofertes per l'usuari, que són accessibles a qualsevol persona o sistema informàtic, per exemple: fotos personals, adreça, telèfon, entre altres.

**Saber-ne més**

L'Agència Espanyola de Protecció de Dades defineix l'empremta digital de dispositiu com "la informació recopilada sobre un dispositiu informàtic remot amb l'objectiu de la seva identificació, singularització i, amb això, continuar el seguiment de l'activitat de l'usuari amb la finalitat de crear-ne un perfil".

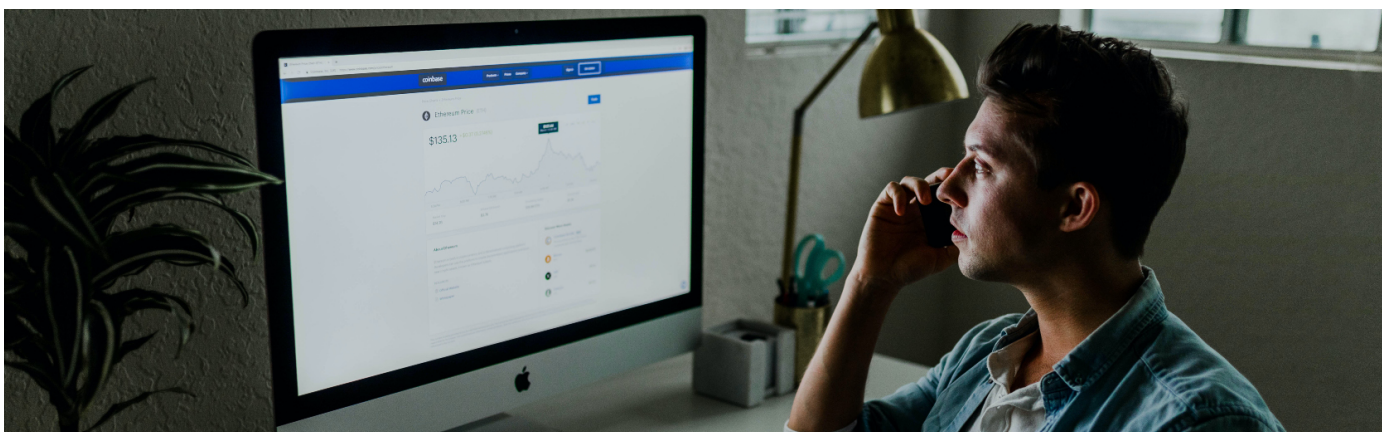
Per aprofundir qüestions en relació amb l'empremta digital, segons l'estudi fet per l'Agència Espanyola de Protecció de Dades, podeu consultar les següents adreces web:

- Empremta digital: [e.digitall.org.es/huella-digital](https://e.digitall.org.es/huella-digital)
- Riscos i frauds a les xarxes socials [e.digitall.org.es/riesgos-redes](https://e.digitall.org.es/riesgos-redes)
- Egosurfing: Quina informació hi ha sobre mi a Internet?  
[e.digitall.org.es/egosurfing](https://e.digitall.org.es/egosurfing)
- Esborrar i disminuir la teva empremta digital: [e.digitall.org.es/video-huella-digital](https://e.digitall.org.es/video-huella-digital), [e.digitall.org.es/borrar-huella-digital](https://e.digitall.org.es/borrar-huella-digital), [incibe.es/ciudadania](https://incibe.es/ciudadania).

**Saber-ne més**

Per aprofundir en els beneficis i riscos de l'ús d'Internet i xarxes socials, pot consultar el document publicat per l'Observatori Nacional de Tecnologia i Societat, o el canal de professionals de la salut:

- Adreça web: [e.digitall.org.es/beneficios-riesgos](https://e.digitall.org.es/beneficios-riesgos)
- Adreça web: [e.digitall.org.es/jovenes-redes](https://e.digitall.org.es/jovenes-redes)





## Cercadors de contingut a les xarxes socials digitals

Per agilitzar la cerca simultània en diverses xarxes socials, s'han creat cercadors de contingut com: *Social Searcher*, *Social Mention* i *Talkwalker*.

- **Social Searcher** ([social-searcher.com](https://social-searcher.com)). És un motor de cerca gratuït de xarxes socials. Permet localitzar contingut en aquestes plataformes en temps real i proporciona dades analítiques en profunditat. Els usuaris poden cercar informació pública sense iniciar sessió a X, Facebook, YouTube, Instagram, Tumblr, Reddit, Flickr i Vimeo. Permet fer cerques per nom d'usuari, etiqueta i tendències. És a dir, podeu trobar informació referent a persones, etiqueta i tendències actuals a les xarxes socials.
- **Social mention** ([mention.com/es](https://mention.com/es)). És un portal web que permet a les marques i qualsevol tipus d'agència (privades o governamentals) gestionar la seva presència en línia a través de l'escolta de l'anàlisi de les xarxes socials i Internet. És a dir, facilita un mostreig de comentaris, imatges i vídeos que els usuaris comparteixen. És una eina potencial dirigida a empreses o autònoms amb presència a xarxes socials. La majoria de les funcions són privades, per la qual cosa es requereix el pagament d'una quota.
- **Talkwalker** ([talkwalker.com/es](https://talkwalker.com/es)). És també una eina que permet l'anàlisi i monitoratge de xarxes socials. El públic objectiu coincideix amb el de *Social Mention*.

Sigui quina sigui l'estratègia que vulgueu fer servir per cercar informació a les xarxes socials (etiqueta, arrova, paraules claus o cercadors de continguts), heu de tenir en compte la privacitat i les normatives legals nacionals i internacionals. Aquests aspectes els revisarem en el pròxim epígraf.



## Privacitat i normatives legals en la navegació i cerca d'informació a les xarxes socials

La importància de controlar la privacitat en aquestes plataformes és elevada, perquè, a vegades, es comparteixen o visualitzen dades (adreces postals, telèfons, fotos, vídeos personals) a les quals poden accedir milions d'usuaris de tot el món. L'eix principal de la privacitat, per tant, radica a protegir la integritat de cadascú, cosa que redueix els riscos relacionats amb estafes i robatoris.

Tenint en compte la **Llei Orgànica 3/2018** ([e.digitall.org.es/3-2018](https://e.digitall.org.es/3-2018)), entre les mesures per resguardar la privacitat en la navegació i cerca d'informació a xarxes socials, s'hi troben:

- **Dret a l'oblit en cerques d'Internet** (article 93 de la Llei orgànica 3/2018 [[e.digitall.org.es/3-2018](https://e.digitall.org.es/3-2018)])

Com a usuari d'Internet, teniu dret que les plataformes que utilitzeu per fer cerques a Internet us facilitin l'opció d'eliminar les vostres galetes i traces (cerca realitzada). No obstant això, és important destacar que "l'exercici del dret no impedirà l'accés a la informació publicada al lloc web a través de la utilització d'altres criteris de cerca diferents del nom de qui exercís el dret" (article 93.2 de la **Llei Orgànica 3/2018** [[e.digitall.org.es/3-2018](https://e.digitall.org.es/3-2018)]).

En el context de la cerca d'informació a xarxes socials, si **feu un comentari** per sol·licitar o argumentar-hi una determinada informació en un grup o pàgina web, i si un altre usuari també hi fa una cerca i el seu contingut es relaciona amb el **comentari que va fer**, aleshores la xarxa social té potestat per retornar el vostre **comentari** entre els resultats de cerca.

- **Dret a l'oblit a serveis de xarxes socials i serveis equivalents** (article 94 de la **Llei Orgànica 3/2018** [[e.digitall.org.es/3-2018](https://e.digitall.org.es/3-2018)])

facilitat per a la publicació per serveis de xarxes socials i serveis de la societat de la informació equivalent" (article 94.1 de la **Llei Orgànica 3/2018** [[e.digitall.org.es/3-2018](https://e.digitall.org.es/3-2018)])





Si feu una cerca a xarxes socials, i en aquest procés compartiu informació personal en un grup temàtic o amb usuari en específic, la plataforma ha de donar-vos la possibilitat d'eliminar-ne la informació.

- **Protecció dels drets de menors d'edat**

En la cerca d'informació per xarxes socials heu de tenir en compte, en relació amb els menors d'edat, que:

**1| Article 84.2 de la Llei Orgànica 3/2018 ([e.digitall.org.es/3-2018](https://e.digitall.org.es/3-2018)):** "L'ús o difusió d'imatges o informació personal de menors a les xarxes socials i serveis de la societat de la informació equivalents que puguin implicar una intromissió il·legítima en els seus drets fonamentals, determinarà la intervenció del Ministeri Fiscal, que instarà les mesures cautelars i de protecció previstes en la Llei orgànica 1/1996, de 15 de gener, de Protecció Jurídica del Menor".

Per tant, en la cerca i obtenció d'informació a xarxes socials, si descobriu imatges o vídeos en què apareguin menors d'edat, haureu de vetllar pel compliment d'aquesta normativa.

#### **NOTA**

##### **Normatives legals**

A la Llei orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals, s'aborda, entre altres aspectes, l'ús ètic de les xarxes socials, els drets i deures de l'usuari, i l'ús d'aquestes plataformes per part dels menors.

Adreça web: [e.digitall.org.es/3-2018](https://e.digitall.org.es/3-2018)



A vegades, quan se cerca d'informació a xarxes socials una publicació redirigeix a una pàgina, lloc o portal web extern, i el navegador o l'antivirus alerta que ha detectat una possible pàgina no de confiança o fraudulenta. Us suggerim no accedir-hi, perquè els ciberdelinqüents poden utilitzar tècniques com la suplementació (*spoofing*) i la pesca (*phishing*) per robar-vos la identitat digital.

**NOTA****Tècniques usades per suplantar o robar identitats digitals**

Les tècniques més comunes són la suplementació (spoofing) o la pesca (phishing). Ambdues estan orientades a robar la identitat digital d'un usuari. La primera falsifica l'adreça electrònica d'un correu electrònic o d'una pàgina, lloc o portal web, mentre que la segona envia missatges suplantant una entitat legítima com, per exemple, un banc o institució governamental.

Per aprendre més sobre aquestes tècniques, podeu consultar les següents URL:

- Adreça web: [e.digitall.org.es/spoofing](https://e.digitall.org.es/spoofing)
- Adreça web: [incibe.es/ciudadania](https://incibe.es/ciudadania)

## Recomanacions per a la cerca d'informació a l'hora de fer ús de les xarxes socials

A continuació, compartim alguns suggeriments que podeu seguir durant la cerca d'informació en xarxes socials:

### 1 | Verificar la necessitat d'accedir a vincles o descàrregues d'informació

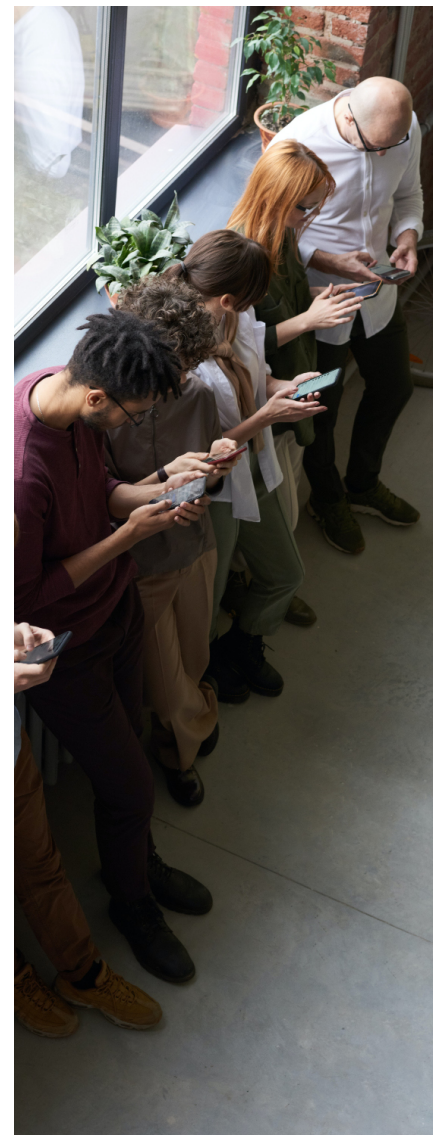
És molt habitual trobar continguts que redirigeixen a una altra localització a Internet o que us possibiliten descarregar un fitxer. Es recomana verificar aquest contingut i reflexionar abans de fer-hi clic per evitar possibles atacs delictius (virus o programa maligne que roba informació o infecta el dispositiu). Heu de vetllar per l'accés a continguts autèntics.

### 2 | Afegir i conversar amb coneguts

És freqüent que us interessin diverses informacions resultants de la cerca d'informació o que, a vegades, vulgueu contactar amb el creador o qui va publicar aquesta informació. Heu d'anar alerta perquè sovint es desconeix qui pot haver-hi darrere aquest perfil.

### 3 | Promoure una relació adequada entre ètica i llibertat d'expressió

No es poden difondre notícies falses, continguts ofensius o denigrants, i, per això, cal emprar un llenguatge inclusiu, evitar el biaix informatiu i respectar les postures ideològiques o de religió alienes.





## ⚠ ATENCIÓ

### Advertències i errors freqüents que s'haurien d'evitar

Per cercar informació a xarxes socials, cal que eviteu els errors següents:

- Aceptar un determinado contenido sin antes verificarlo.
- No respetar las normativas legales establecidas en la Ley Orgánica 3/2018.

## 📄 Saber-ne més

### Ús adequat de les xarxes socials

Per aprofundir sobre les xarxes socials i l'ús ètic d'aquestes, podeu consultar les següents adreces web:

- Privacitat i conseqüències de l'ús de xarxes socials:  
[e.digitall.org.es/psicoeducativa](https://e.digitall.org.es/psicoeducativa), [e.digitall.org.es/prisma-social](https://e.digitall.org.es/prisma-social)
- Ús educatiu de les xarxes socials:  
[e.digitall.org.es/uso-educativo-redes](https://e.digitall.org.es/uso-educativo-redes)
- Ús de les xarxes socials científiques: [e.digitall.org.es/redes-cientificas](https://e.digitall.org.es/redes-cientificas)





# DigitAll

Cerca i gestió  
d'informació i dades

## 1.2

### AVALUAR DADES, INFORMACIÓ I CONTINGUTS DIGITALS





Cerca i gestió  
d'informació i dades

**Nivell B2 1.2** Avaluar dades, informació  
i continguts digitals

# Guia metodològica per a la identificació del pescaclics







## Guia metodològica per a la identificació del pescaclics

El fenomen del pescaclics s'ha explicat àmpliament en dos vídeos de la col·lecció. L'objectiu d'aquest document és recopilar una sèrie de pautes que permetin reconèixer aquesta classe de titulars i així evitar als usuaris de les xarxes accedir a continguts mancats d'interès, decebedors i, fins i tot, perillosos.



### PESCACLICCS

*Definició de pescaclics. Identificació de continguts potencialment perillosos o no desitjats.*

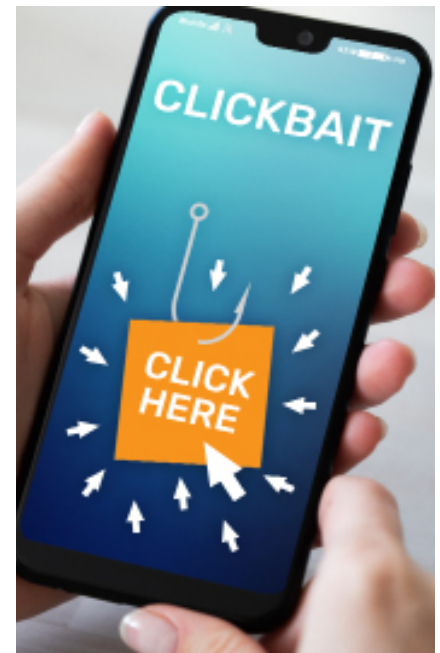
[e.digitall.org.es/A1C12B1V04](https://e.digitall.org.es/A1C12B1V04)



### IDENTIFICACIÓ AVANÇADA DEL PESCACLICCS

*Identificació avançada de continguts potencialment perillosos o no desitjats. Identificació i anàlisi dels resultats i enllaços.*

[e.digitall.org.es/A1C12B2V02](https://e.digitall.org.es/A1C12B2V02)



El terme pescaclics s'utilitza per denominar una sèrie de titulars enganyosos l'objectiu dels quals és atreure els lectors a un determinat contingut web.

## Tipus de continguts

Una de les principals característiques del pescaclics és la falta de connexió que existeix entre les expectatives creades pels encapçalaments i el contingut al qual estan enllaçats. A continuació, es presenten diversos exemples del tipus de pàgines a què s'accedeix a través de titulars de pescaclics:

- Llocs en què no s'accedeix directament a la informació promesa, sinó que són una successió de pàgines que s'obren quan es clica un botó següent al final de cadascuna d'aquestes. Per exemple, a: **Celebritats que aconseguiren baixar notablement de pes** ([e.digitall.org.es/celebridades](https://e.digitall.org.es/celebridades)), la persona "esquer" que apareix a la foto del titular, no hi és quan s'avancen moltes pàgines. Quan es fa clic contínuament, és molt probable accedir



a algun anunci o contingut no desitjat. Un altre dels objectius d'aquesta mena de format és recopilar un munt de clics que no aporten res més que l'increment de la taxa d'aquestes accions en la pàgina com per exemple a: **Aquesta nena diu només una paraula durant la seva adopció i la jutgessa decideix detenir l'audiència** ([e.digitall.org.es/daily-story](https://e.digitall.org.es/daily-story)).

- Articles en què es repeteix la informació que hi ha al titular juntament amb una sèrie de dades ja conegudes sobre el tema fins a arribar a una conclusió decebedora: **El joc del calamar. es confirmen sospites sobre participació de Leonardo DiCaprio** ([e.digitall.org.es/dicaprio](https://e.digitall.org.es/dicaprio)).
- Continguts en els quals, utilitzant un esquer com el que ha aconseguit un famós, o donant l'oportunitat d'aconseguir una ganga després d'un material breu, es patrocina algun tipus de producte: **Índia Martínez lluu la seva rutina de gimnàs amb un modelet ideal** ([e.digitall.org.es/india-martinez](https://e.digitall.org.es/india-martinez)).

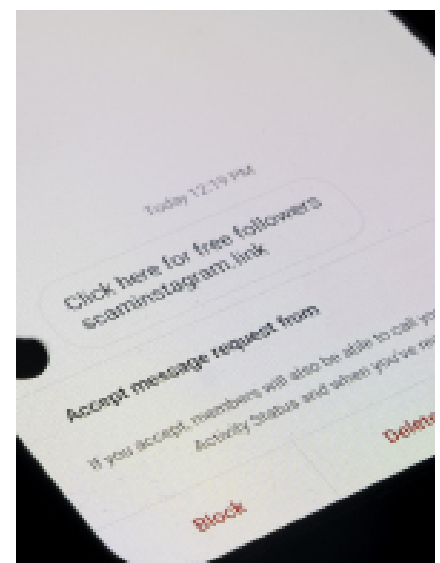
Tots aquests exemples tenen com a objectiu principal aconseguir un rendiment econòmic, ja que, a més d'incrementar la seva taxa de clics, inclouen un altre tipus de titulars de pescaclics amb el mateix objectiu o mostren una gran quantitat de publicitat obtinguda probablement per aquest increment de visites. Per tant, una vegada s'hagin identificat aquesta mena de continguts, el millor que es pot fer és evitar aquestes pàgines.

#### ⚠ ATENCIÓ

Per evitar el pescaclics, una vegada reconegut un d'aquests titulars, s'ha de bloquejar el lloc web de destinació, ja que sempre oferirà continguts d'aquest tipus. Igualment, no s'han de seleccionar els enllaços que apareguin en aquesta pàgina. Com més titulars de pescaclics accediu, més us hi conduirà.

Els agregadors de notícies i les pàgines de suggeriments de les xarxes socials són també ubicacions probables de material pescaclics.

Per no perdre temps amb aquests continguts, existeixen espais "esbudelladors" de pescaclics com **Saved you a clic** ([twitter.com/savedyouaclick](https://twitter.com/savedyouaclick)).





## Característiques dels titulars

Al punt anterior s'han mostrat pautes per identificar el pescaclics a posteriori i, així, poder detectar llocs que s'han d'evitar visitar.

Encara que no es pot considerar que tots els titulars de pescaclics siguin similars, a la taula **CARACTERÍSTIQUES DELS TITULARS DE PESCACLICIS** es recullen característiques que fa fàcil localitzar-ne. En algun dels exemples que s'hi presenten, aquesta classe de titulars apareix a l'agregador de notícies, per la qual cosa és molt diferent del que surt a la pàgina de destinació i que, potser fa que no atregui gaire l'atenció.

### CARACTERÍSTIQUES DELS TITULARS AMB PESCACLICIS

Pauta	Exemple
<b>Moltes paraules, encara que n'hi ha que no tenen contingut significatiu: articles, pronoms, preposicions...</b>	<i>És tan simple, però no puc pensar en això, moltes persones ho seguiran.</i> ( <a href="http://e.digitall.org.es/ejemplo-1">e.digitall.org.es/ejemplo-1</a> )
<b>Redacció complexa. Per exemple, el subjecte i el verb estan artificialment separats</b>	<i>aragossa, amb una guia turística: així ha empitjorat.</i> ( <a href="http://e.digitall.org.es/ejemplo-2">e.digitall.org.es/ejemplo-2</a> ) L'enllaç porta al titular correcte diferent del titular esquer.
<b>Ús d'un llenguatge excessivament col·loquial</b>	<i>A Froilán li han posat una "cuidadora d'uniforme" perquè no visqui les mil i una nits d'Abu Dhabi.</i> ( <a href="http://e.digitall.org.es/ejemplo-3">e.digitall.org.es/ejemplo-3</a> )
<b>Ús excessiu de signes de puntuació i majúscules</b>	<i>Vaig col·locar Vela de Mosquits a l'AIGUA i NO creuràs el que Va succeir.</i> ( <a href="http://e.digitall.org.es/ejemplo-4">e.digitall.org.es/ejemplo-4</a> )
<b>Ús d'hipèrboles i exageracions</b>	<i>My Hero Academia entra en pausa per un motiu desolador.</i> ( <a href="http://e.digitall.org.es/ejemplo-5">e.digitall.org.es/ejemplo-5</a> )
<b>Apel·lació directa al lector: ús de la segona persona</b>	<i>Tres motius per ficar dues pilotes de tennis a la teva rentadora.</i> ( <a href="http://e.digitall.org.es/ejemplo-6">e.digitall.org.es/ejemplo-6</a> )
<b>Frases comuns:</b> • No t'ho creuràs... • No hauries de....sense haver llegit això primer • .... et farà plorar	<ul style="list-style-type: none"> <li>• Els seus ulls tristos pregaven ajuda... no et creuràs com va acabar! (<a href="http://e.digitall.org.es/ejemplo-7">e.digitall.org.es/ejemplo-7</a>)</li> <li>• No instal·leu panells solars en 2023 fins que hàgiu llegit això. (<a href="http://e.digitall.org.es/ejemplo-8">e.digitall.org.es/ejemplo-8</a>)</li> </ul>
<b>Ús de números a llistes i rànquings</b>	<ul style="list-style-type: none"> <li>• Els 10 estadis de futbol més bonics del món: la resposta de la intel·ligència artificial.. (<a href="http://e.digitall.org.es/ejemplo-9">e.digitall.org.es/ejemplo-9</a>)</li> </ul>

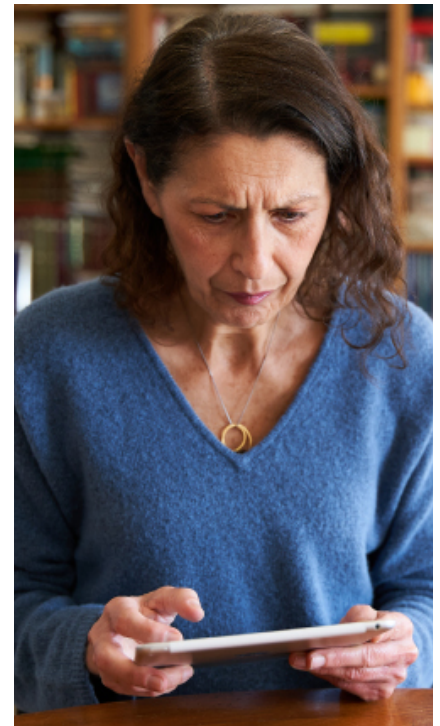
Es pot comprovar com moltes d'aquestes pautes es combinen en els diferents exemples. Aquestes estratègies cerquen tant ocultar informació com apel·lar les emocions per tal de crear la curiositat necessària amb l'objectiu d'aconseguir que siguin seleccionats pels usuaris dels mitjans digitals i de xarxes socials.



## Ús d'imatges pescaclics

Els titulars que s'han descrit poden dirigir-vos tant a noves pàgines web com a continguts en xarxes socials. En molts casos van acompanyats d'imatges amb el mateix objectiu de crear artificialment expectació. Es poden identificar diferents tipus d'imatges per aconseguir-ho:

- Imatges estranyes i, fins i tot, desagradables.
- Imatges que transmeten emocions: **Polèmica a la Festa amb el retorn del col·laborador que ha posat en guerra Mediaset: "Estic desitjant tornar a la meva feina"**. **Emma García haurà de cedir-li pas** ([e.digitall.org.es/polemica-fiesta](https://e.digitall.org.es/polemica-fiesta)). A més, es tracta d'un titular molt llarg i de redacció estranya, està acompanyat d'una imatge de la presentadora del programa plorant.
- Imatges que no tenen a veure amb el contingut.



Per evitar que les imatges utilitzades com a miniatures representatives dels vídeos de YouTube actuïn com a imatges esquer, es pot instal·lar al navegador l'extensió **Clickbait Remoure**. Aquesta eina detecta imatges que no pertanyen al vídeo i les reemplaça per algun dels seus fotogrames. A més, modifica els títols reemplaçant majúscules per minúscules.

### Saber-ne més

Ús del pescaclics als mitjans nadius digitals espanyols. Una anàlisi del Confidencial, L'Espanyol, Eldiario.es i Ok Diario.

[e.digitall.org.es/clickbait-medios](https://e.digitall.org.es/clickbait-medios)

Què és el pescaclics i com usar-lo de manera correcta?

[e.digitall.org.es/clickbait-correcto](https://e.digitall.org.es/clickbait-correcto)

Les millors extensions per bloquejar la publicitat de YouTube o eliminar el pescaclics.

[e.digitall.org.es/bloquear-clickbait](https://e.digitall.org.es/bloquear-clickbait)



Cerca i gestió  
d'informació i dades

**Nivell B2** 1.2 Avaluar dades, informació  
i continguts digitals

# Guia metodològica per a la identificació de continguts patrocinats





## Guia metodològica per a la identificació de continguts patrocinats

La principal font d'ingressos dels mitjans digitals és la publicitat. Al vídeo Continguts patrocinats es presenten diferents estratègies de màrqueting digital en pàgines web i xarxes socials. D'una banda, hi ha els anuncis en els quals el contingut publicitari s'expressa directament. En aquest document s'indiquen pautes per reconèixer aquells continguts associats al suport econòmic d'una empresa, però que no s'identifiquen clarament com a publicitat.



### CONTINGUTS PATROCINATS

*Definició de continguts patrocinats. Anuncis i missatges de màrqueting. Conseqüències dels continguts patrocinats. Fals patrocini.*

[e.digitall.org.es/A1C12B2V03](https://e.digitall.org.es/A1C12B2V03)



## Exemples de patrocini correcte

Una de les estratègies que segueixen les empreses per posicionar-se en el món digital és mitjançant el patrocini de llocs i continguts. Això vol dir que donen alguna mena de suport a aquests continguts, perquè els consideren adequats perquè apareguin lligats a la seva marca. Aquest suport pot ser econòmic, de difusió o de creació de continguts. No hi presenten els seus productes directament, simplement associen la seva marca, per la qual cosa n'apareixerà el nom o el logo per identificar aquest patrocini.

Al patrocini no s'anuncia directament un producte o marca. Les empreses donen suport a un contingut al qual volen lligar la seva imatge.

La col·lecció de vídeos "**Aprendem junts 2030**" ([aprendemosjuntos.bbva.com](https://aprendemosjuntos.bbva.com)) associats a la formació en objectius de desenvolupament sostenible estan patrocinats per BBVA i distribuïts per El País. No hi apareix cap referència als productes oferts pel banc.



La secció “*L’Espanya despoblada*” ([e.digitall.org.es/despoblacion](http://e.digitall.org.es/despoblacion)) al web de la Cadena Ser està patrocinada per Fenie Energia. Simplement hi apareix el seu logo.

Quan es clica sobre els logos, s’accedeix als webs de les empreses, la qual cosa també els és un benefici.

## Patronicis a les cerques

Les empreses paguen als cercadors perquè, si una cerca es relaciona amb la seva marca, les pàgines web en siguin els primers resultats. És fàcil identificar-les, ja que sempre apareix una frase clau al costat del resultat de **pagament**. A la imatge es mostren algunes d’aquestes marques. Poden ser molt visibles com el **Patrocinat** de Google o més difícils de localitzar com l’**Anunci** de Bing o DuckDuckGo. En alguns casos, la frase serveix per a tot un grup de sortides com el cas d’**Anuncis relacionats** de Yahoo Search.

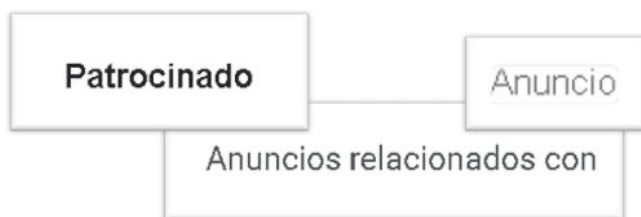


Figura 1. Indicadors que els resultats d’una cerca són de pagament.

## Publicitat oculta en forma de patrocini

Finalment, per acabar aquest document, es mostraran exemples de continguts associats a una marca i els productes, però que no es mostren directament com a anuncis. En general, han d’anar marcats com a continguts patrocinats amb frases com les que es mostren a la figura 1, i, així, seran fàcilment identificables. En moltes ocasions apareixen a seccions específiques dels diaris:

- Zones **aparador**, on es recopilen els millors productes que es veuen a Internet.
- Zones **gastro**, on es promocionen productes o locals concrets.
- Zones **viatges**, on s’aconsellen destinacions o escapades.
- Zones **oci**, amb suggeriments de sèries i a quina plataforma veure-les.



Es tracta de seccions tradicionals de la premsa i no sempre estan associades al patrocini. Cal vigilar, sobretot, si finalitzen amb indicacions concretes sobre **on i a quin preu** podem comprar ingredients d'una recepta, **quines companyies aèries porten a una determinada destinació** o **quines marques són les més adequades** per proporcionar aquesta cura al nostre bebè o mascota que s'ha descrit al contingut.

#### ⚠ ATENCIÓ

No cal oblidar-se dels continguts a xarxes socials que s'han desenvolupat entorn d'un producte determinat. Els creadors d'aquests continguts reben una gratificació perquè aquests productes apareguin a les seves publicacions.

#### 📄 Saber-ne més

Pràctiques comercials deslleials. Web oficial de la Unió Europea.

[e.digitall.org.es/practicas-desleales](https://e.digitall.org.es/practicas-desleales)

Llibre blanc del màrqueting d'influenciadors de IAB Spain, l'associació de la publicitat, el màrqueting i la comunicació digital a Espanya.

[e.digitall.org.es/libro-blanco-marketing](https://e.digitall.org.es/libro-blanco-marketing)







Cerca i gestió  
d'informació i dades

**Nivell B2 1.2** Avaluar dades, informació  
i continguts digitals

# Aplicació avançada de la IA a l'hora de gestionar continguts





## Aplicació avançada de la IA a l'hora de gestionar continguts

### Aplicació de la intel·ligència artificial a la gestió de dades i continguts digitals

La Intel·ligència Artificial (IA) transforma la manera com dirigim les dades. Amb l'augment de la quantitat d'informació disponible en línia, la IA s'ha convertit en una eina essencial per processar i analitzar grans conjunts de dades en temps real. Les eines d'anàlisis de dades basades en IA poden identificar patrons i tendències a dades que poden ser útils per a la presa de decisions.

Des de la personalització de continguts fins a la detecció d'**hipertrucatge**, la IA és utilitzada en una àmplia gamma d'aplicacions per millorar l'eficiència i la precisió en la gestió de dades i continguts digitals.

En aquest sentit, s'ha convertit en una tecnologia clau per a empreses i organitzacions que cerquen optimitzar les seves operacions i oferir una millor experiència als usuaris.

A les seccions següents es mostraran les principals aplicacions de la IA a la gestió de dades i continguts digitals. Alhora, es proporcionaran casos o exemples reals de l'ús d'aquestes.

#### NOTA

Aquest tema guarda relació amb tots els vídeos del nivell B2 de la competència C1.2 anomenada "Avaluació de dades, informació i continguts digitals".



### Recomanacions personalitzades

La IA es pot utilitzar per personalitzar continguts digitals, com notícies, anuncis i recomanacions de productes. Mitjançant l'anàlisi de les dades dels usuaris i l'historial de navegació i compres, pot oferir continguts que siguin rellevants i atractius per a cada usuari.



A continuació, es mostren exemples reals d'empreses que empren aquesta tècnica per a la generació de recomanacions personalitzades:

- **Netflix.** Analitza el comportament de visualització dels usuaris i utilitza aquesta informació per oferir recomanacions de pel·lícules i programes de televisió que podrien ser d'interès.
- **Amazon.** Mitjançant l'anàlisi de l'historial de compres, les cerques i la navegació al lloc, ofereix recomanacions rellevants i suggeriments de productes.
- **Spotify.** Estudia el comportament d'escolta per oferir productes musicals i crear llistes de reproducció personalitzades basades en les preferències dels usuaris.
- **The Washington Post.** Personalitza els titulars de les notícies i crea resums personalitzats per als lectors mitjançant l'anàlisi del comportament de lectura dels usuaris.
- **H&M.** Revisa l'historial de compres i les preferències d'estil dels usuaris i ofereix recomanacions de productes que s'hi adaptin.



## Classificació automàtica de continguts

Els continguts digitals, com imatges, vídeos i documents, poden ser classificats automàticament en categories específiques. Això és molt útil, per exemple, per a empreses de mitjans de comunicació, ja que els permet la classificació automàtica dels articles en diferents seccions.

A continuació, us compartim dues empreses rellevants que usen aquest sistema:

- **Shutterstock.** Aquesta empresa utilitza la IA per etiquetar i classificar-hi automàticament milions d'imatges i vídeos. L'empresa analitza cada imatge i vídeo per identificar objectes, persones, animals i altres elements, i assigna etiquetes precises i rellevants a cada arxiu. Aquesta classificació automatitzada permet als usuaris trobar fàcilment els continguts que necessiten per als seus projectes.



### Saber-ne més

Shutterstock és un repositori estatunidenc de fotografia, vídeo i música, a més de proveïdor d'eines d'edició. La seu està situada a Nova York i va ser fundada el 2003 pel programador i fotògraf Jon Oringer. Actualment, Shutterstock manté una biblioteca d'aproximadament 125 milions de fotos i il·lustracions amb llicència lliure i devers 4 milions de videoclips i pistes de música disponibles amb llicència. El funcionament inicial del servei era mitjançant subscripció, però a partir de 2008 es va modificar a preus a la carta.

[shutterstock.com/es](https://shutterstock.com/es)

- **Adobe.** La seva eina de classificació d'imatges, Adobe Sensei, utilitza la IA per etiquetar automàticament les imatges amb informació detallada sobre el contingut, composició i estil visual. Això permet als usuaris trobar ràpidament les imatges que necessiten per als seus projectes creatius. A més, de cara al màrqueting, Sensei proporciona informació per a la presa de decisions, atès que pot predir el comportament dels clients i oferir-los experiències personalitzades ([adobe.com/sensei](https://adobe.com/sensei)).

## Anàlisi de sentiment

L'anàlisi de sentiment és una tècnica de processament del llenguatge natural que utilitza algorismes d'aprenentatge automàtic per identificar, classificar i extreure informació de les opinions, actituds i emocions expressades en textos, com ressenyes de productes, publicacions a xarxes socials i comentaris dels clients. Aquesta tècnica cerca comprendre i quantificar el to emocional d'un text, i el pot classificar com a positiu, negatiu o neutre.

L'anàlisi de sentiment mitjançant IA s'utilitza en diversos camps, i hi inclou el màrqueting, l'atenció al client, la recerca de mercats i la gestió de reputació en línia. Aquesta informació pot ser utilitzada per les empreses per entendre millor els seus clients i oferir-los una experiència millor, la qual cosa els permet alhora, un major creixement empresarial.

A continuació, es mostren alguns exemples d'empreses que utilitzen anàlisis de sentiment mitjançant IA a l'activitat comercial:



- **Airbnb.** Mitjançant l'anàlisi de sentiment analitza les opinions dels hostes sobre les experiències d'allotjament i millora així el servei per al client.
- **Coca-cola.** Avalua les opinions dels consumidors sobre els productes i campanyes de màrqueting per ajustar-ne les estratègies.
- **X.** La classificació de les piulades segons el seu to emocional proporciona una anàlisi de les tendències.
- **Ford.** Avalua les opinions dels clients sobre els vehicles per millorar-ne el disseny i fabricació.

## Automatització de tasques

L'automatització de tasques mitjançant IA ha revolucionat la manera en què les empreses manegen els processos de negoci. La IA permet a les empreses automatitzar accions i tasques repetitives, tot alliberant els empleats per enfocar-se en activitats més importants i creatives. També millora l'eficiència i qualitat dels processos, i en redueix els costos i els fa més efectius.

La IA s'ha convertit en una eina fonamental per millorar la productivitat i la competitivitat de les empreses en un entorn cada vegada més digital i automatitzat.

Hi ha moltes empreses que utilitzen la IA per automatitzar processos. A continuació, se'n mostren alguns exemples:

- **Amazon.** La companyia utilitza robots als magatzems per recollir i enviar comandes. Els robots estan equipats amb càmeres i sensors que els permeten navegar de manera autònoma pels dipòsits i així poden recollir els articles de manera eficient.
- **Siemens.** Optimitza la gestió de l'energia a edificis, mitjançant el control automàtic en funció de factors com l'ocupació de l'edifici i les condicions meteorològiques, la qual cosa redueix els costos i millora l'eficiència energètica.





- **Uber.** Gestiona la flota de conductors i optimitza les rutes de viatge. Els algorismes analitzen dades en temps real per prendre decisions sobre l'assignació de trajectes, així com perquè els xofers trobin la ruta més eficient per cada viatge.

## Millora de la seguretat de les dades

La seguretat de dades és una preocupació cada vegada més present en la societat digital. En aquest aspecte, la IA ofereix solucions prometedores per millorar la protecció de dades confidencials.

Un dels principals avantatges és la capacitat que té per detectar patrons en temps real que podrien indicar activitats sospitoses, o, fins i tot, identificar vulnerabilitats a la infraestructura de seguretat.

D'aquesta manera, es podria no només prevenir intrusions en els sistemes de seguretat, sinó també reduir el temps necessari per detectar i respondre aquestes amenaces potencials. Així es veu millorada l'eficiència en la protecció de la informació confidencial dels usuaris.

Això és especialment important en entorns laborals on es manegen dades molt delicades. Alguns exemples d'aquesta qüestió es mostren a continuació:

- **IBM.** Aquesta empresa utilitza la plataforma Watson per analitzar grans quantitats de dades de seguretat en temps real i detectar patrons o anomalies que poguessin indicar activitats malicioses.
- **Microsoft.** Utilitza la intel·ligència artificial per protegir els serveis en línia, com Office 365 i Azure.
- **Amazon.** Té una plataforma de seguretat pròpia anomenada *Amazon GuardDuty* per millorar la seguretat dels sistemes de comerç electrònic i emmagatzematge al núvol.

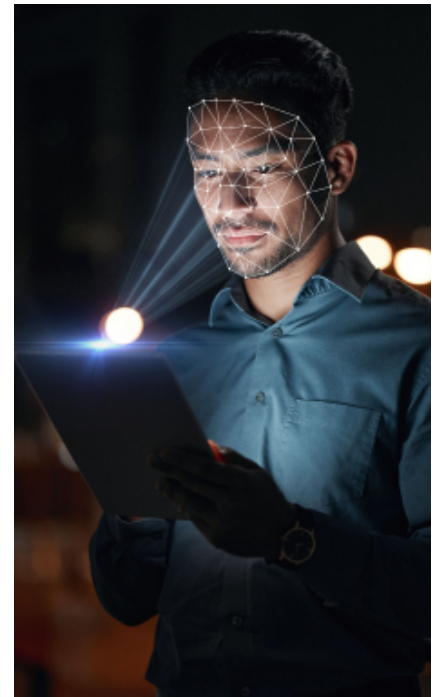


## Detecció d'hipertrucatge

Encara que la IA és la responsable de la generació d'hipertrucatge, també ens permet que nosaltres ho puguem detectar.

Els patrons i les característiques de les imatges o vídeos es poden analitzar per determinar si són autèntics o falsos. Es tracta d'un camp que està en constant evolució. Algunes de les tècniques disponibles actualment són:

- 1 | Falta de sincronització labial.** Es pot detectar que el moviment dels llavis del subjecte no coincideix amb el so que es reproduïx, la qual cosa resulta indicatiu que es tracta d'un hipertrucatge.
- 2 | Anàlisi de la textura i la il·luminació.** Se'n pot analitzar la textura i la il·luminació per comprovar si ha estat manipulada. Els hipertrucatges poden denotar-se en una aparença poc realista.
- 3 | Consistència facial.** Pot passar que les cares mostrin una falta de consistència, cosa que ens indica que les diferents parts de la cara no coincideixen entre si. Així, es pot detectar aquesta discrepància.
- 4 | Anàlisi de les característiques facials.** Es pot detectar si hi ha hagut manipulació a la captura de característiques facials subtils, com el parpelleig i les microexpressions.
- 5 | Qualitat de la imatge.** S'analitza la qualitat de la imatge per detectar si ha estat manipulada. Les fotografies marcades per l'hipertrucatge solen presentar una qualitat inferior.



## Riscos de la IA en la gestió de dades i continguts digitals

A mesura que la IA es converteix en una tecnologia cada vegada més omnipresent en la gestió de dades i continguts



digitals, també sorgeixen preocupacions sobre els seus riscos i desafiaments.

Si bé la IA pot millorar l'eficiència i precisió en la classificació, processament i anàlisi de dades, també pot introduir biaixos i errors que afecten negativament la qualitat i la integritat de les dades.

A més, la IA també pot utilitzar-se per a la creació d'hipertrucatge i la manipulació de continguts, la qual cosa planteja preocupacions ètiques i de seguretat entorn de l'autenticitat i la veracitat de la informació en línia.

En aquest sentit, és important comprendre els riscos i desafiaments de la IA en la gestió de dades i continguts digitals, i treballar per mitigar-los i garantir que la IA s'utilitzi de manera responsable i ètica.

## Reforç d'opinió

La IA també pot ser utilitzada per reforçar les opinions dels usuaris en diversos àmbits.

Per exemple, en màrqueting, mitjançant l'anàlisi de les dades dels consumidors, es generen recomanacions personalitzades, la qual cosa contribueix a reforçar l'opinió sobre determinats productes o serveis. També es poden detectar tendències i opinions populars, que serviran de base per definir-ne les estratègies de màrqueting i comunicació, i fomentar, encara més, l'opinió en un sentit únic.

En política, mitjançant l'anàlisi del discurs i la retòrica dels polítics, es pot influir en l'opinió dels votants respecte de candidats determinats.

Finalment, a les xarxes socials s'usen algorismes específics per mostrar als usuaris continguts que ja han estat compartits o que són similars als que han compartit en el passat. Això pot reforçar les seves opinions i se'n pot veure limitada l'exposició a opinions diferents.

L'exposició dels usuaris a informació que només confirma les seves creences preexistents pot conduir a una polarització de la societat i a una minva de la comprensió entre diferents grups de persones.





A més, la IA també es pot utilitzar per a la creació d'hipertrucatge i la manipulació de continguts, la qual cosa contribueix a generar desinformació i notícies falses.

Això pot socavar la confiança en la informació i afeblir la democràcia. Per tant, és important que es tracti el problema del reforç d'opinió, atès que planteja preocupacions ètiques i de seguretat entorn de l'autenticitat i la veracitat de la informació en línia.

## Biaix mitjançant IA

Els biaixos en la intel·ligència artificial poden sorgir de diverses maneres, com la selecció de dades d'entrenament inadequada, o la reproducció d'estereotips presents a la societat als algorismes d'aprenentatge desenvolupats.

Les conseqüències d'aquests biaixos a la IA poden incloure la perpetuació de la discriminació, la disminució de la confiança en els sistemes de IA l'exclusió d'uns certs grups de la societat a l'hora d'accedir a determinats serveis o recursos.

Per exemple, el 2018 es va publicar que el sistema de reconeixement facial de Amazon, anomenat Rekognition, va confondre a 28 congressistes amb sospitosos de la policia. Es comenta que es va fer una prova per contrastar fotos de polítics estatunidencs amb una base de dades policial pública de 25.000 fotos de delinqüents. El sistema de reconeixement facial va relacionar especialment els integrants negres i llatins del Congrés amb les persones mostrades a les fotos policials ([e.digitall.org.es/rekognition](https://e.digitall.org.es/rekognition)).

La mateixa empresa va haver de deixar d'usar un algorisme d'aprenentatge que feien servir per a la contractació dels empleats perquè va resultar ser sexista, i va perjudicar les dones a l'hora de la contractació laboral ([e.digitall.org.es/algoritmo-amazon](https://e.digitall.org.es/algoritmo-amazon)).

Per tot això, és important abordar aquests biaixos de manera proactiva i treballar per desenvolupar algorismes de IA més equitatius i justos.



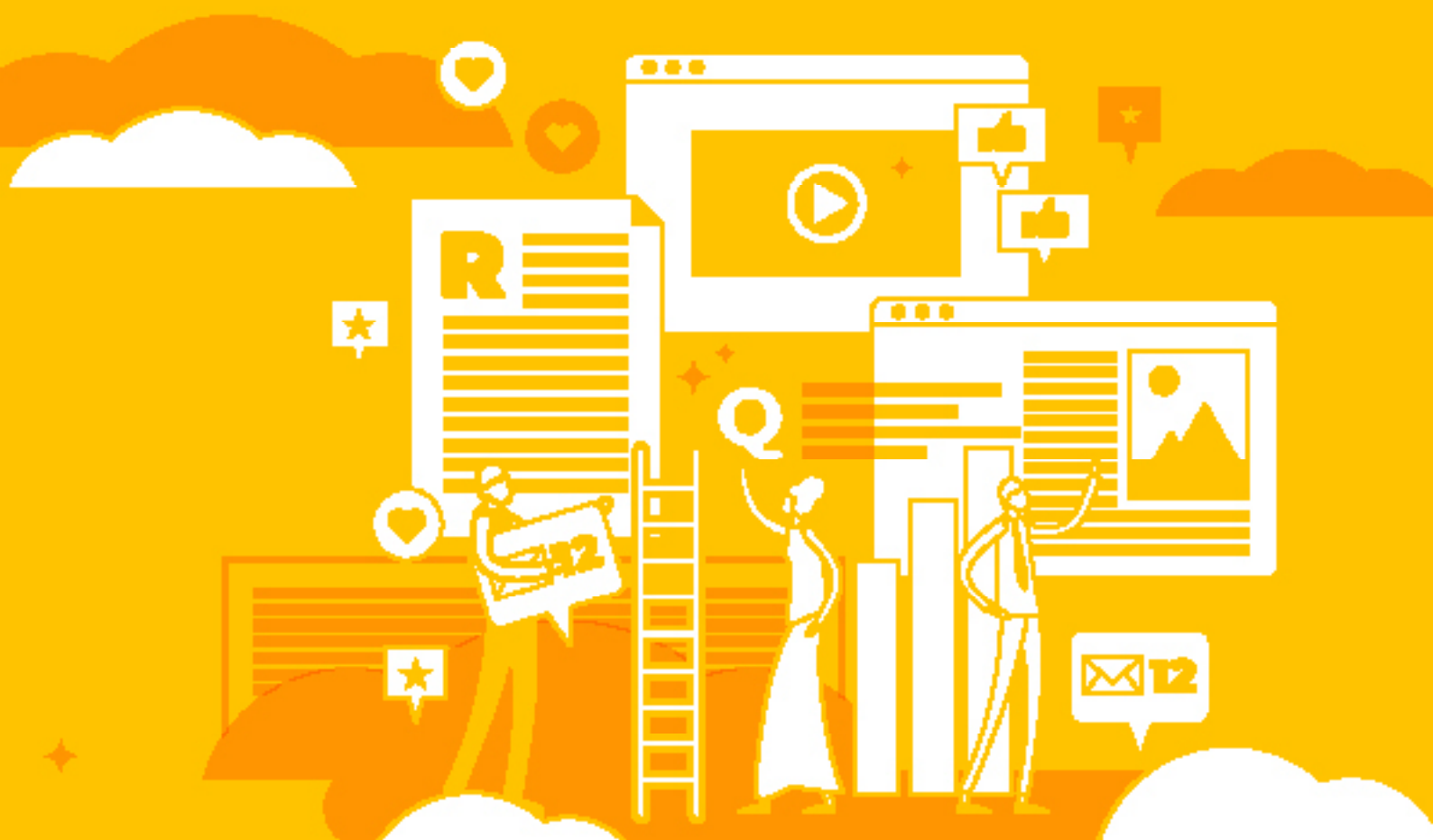


# DigitAll

Cerca i gestió  
d'informació i dades

## 1.3

### GESTIÓ DE DADES, INFORMACIÓ I CONTINGUTS DIGITALS





Cerca i gestió  
d'informació i dades

**Nivell B2 1.3** Gestió de dades, informació  
i continguts digitals

# Gestió de dispositius





## Gestió de dispositius

### Particions d'unitats d'emmagatzematge

La creació de particions en una unitat d'emmagatzematge secundari permet la gestió independent de diferents volums de dades. Cada sistema operatiu disposa d'un programa gestor d'emmagatzematge que permet crear, esborrar i modificar sistemes de fitxers aïllats a les particions creades.



#### DISPOSITIUS D'EMMAGATZEMATGE LOCALS

*Formatació d'unitats d'emmagatzematge. Formatació ràpida i a baix nivell per poder esborrar permanentment la informació. Còpia de la informació mitjançant eines de comprensió d'arxius per transferir volums de dades grans i arxius de còpies de seguretat.*

[e.digitall.org.es/A1C13B2V03](http://e.digitall.org.es/A1C13B2V03)

La taula o mapa de particions descriu les particions que hi ha en un disc. La taula de partició GUID (GPT) és l'esquema més emprat avui dia. Existeixen diversos tipus de particions, en funció de l'ús final que tinguin. Per una banda, les particions primàries estan destinades a emmagatzemar el sistema operatiu i, per altra, les de tipus estès, són volums de dades que estan organitzades jeràrquicament. Les particions d'arrencada permeten emmagatzemar un programa que carrega els sistemes operatius i poden ser de tipus BIOS o, les més modernes, de tipus EFI.

#### Tipus de particions per a sistemes Windows

L'esquema de particions a Windows 11 per a un ordinador amb Interfície Unificada de Programari Extensible UEFI conté una partició del sistema, una partició reservada Microsoft anomenada MSR, la partició on s'instal·la el sistema operatiu Windows amb format de tipus NTFS i una partició extra de recuperació del sistema.





### **i Saber-ne més**

L'esquema de particions de Windows permet l'ús de la tecnologia d'encriptat de discos durs BitLocker.

Podeu tenir-ne més informació al següent enllaç:

[e.digitall.org.es/hard-drive-partition](https://e.digitall.org.es/hard-drive-partition)

## Tipus de particions per a sistemes MacOS

L'esquema de particions per als sistemes MacOS utilitzen una taula de particions GUID i admet la instal·lació del sistema operatiu en particions amb format de tipus Apple APFS o Mac OS Extended per a versions del sistema operatiu anteriors a les 10.13.

### **i Saber-ne més**

L'esquema de particions de MacOS permet compatibilitat per a la instal·lació que prové de sistemes operatius de tipus Windows a equips amb processadors Intel.

Podeu tenir-ne més informació als següents enllaços:

[e.digitall.org.es/particiones-mac](https://e.digitall.org.es/particiones-mac) i [e.digitall.org.es/disk-utility](https://e.digitall.org.es/disk-utility)

## Tipus de particions per a unitats d'emmagatzematge externes

El particionat d'unitats d'emmagatzematge externes que, per exemple, podem connectar amb un USB, pot fer-se mitjançant el programa gestor d'emmagatzematge a Windows o la utilitat de discos a MacOS. Si volem un emmagatzematge que pugui ser compartit amb versions recents de sistemes operatius haurem d'utilitzar un esquema de taula de particions GPT i de particions amb format MS-DOS (FAT32) o ExFAT. Aquestes darreres permetran emmagatzemar fitxers de mida superior als 4 gigaoctets.

### **i Saber-ne més**

El sistema d'arxius ExFAT va ser patentat per Microsoft i constitueix una extensió de l'anterior FAT32.

Podeu tenir-ne més informació al següent enllaç:

[e.digitall.org.es/formatos-discos-mac](https://e.digitall.org.es/formatos-discos-mac)





## Eines per a la formatació de particions

És recomanable que, per a la creació, eliminació i formatació de particions utilitzem l'administrador de discos en els sistemes Windows i la utilitat de discos als dispositius Apple MacOS.

A més, existeixen altres eines desenvolupades per tercers que podem també podem emprar.

### Administració de discos de Windows

Al programa per a l'administració de discos de Windows pot accedir-se fent clic amb el botó dret del ratolí damunt el botó d'Inici.

La part central de la finestra ens mostra totes les unitats connectades a l'equip (internes o externes) i les particions que hi contenen.

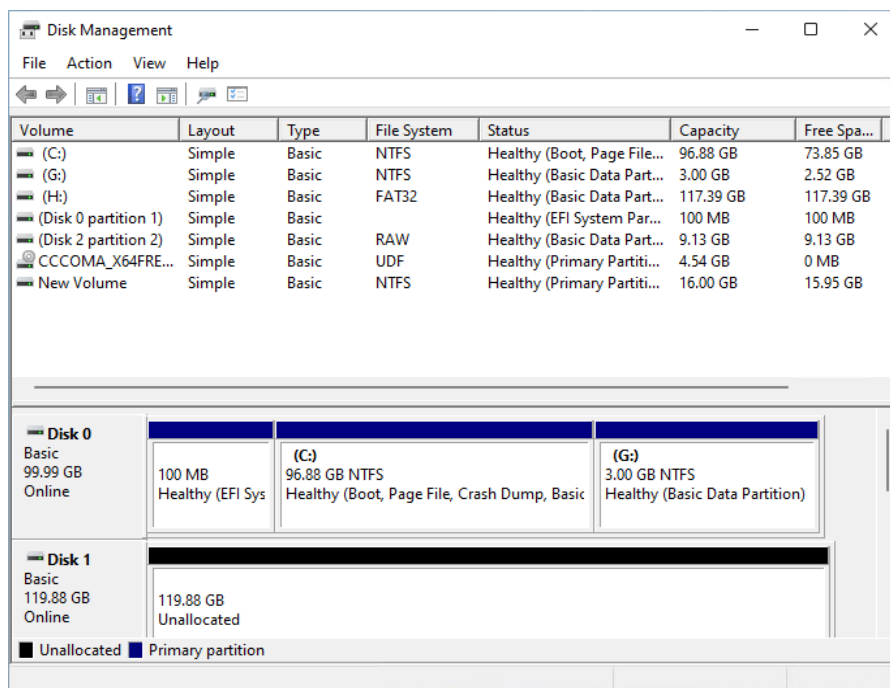


Figura 1. Finestra principal del programa de gestió de discos de Windows. Imatge amb llicència CCC obtinguda de [e.digitall.org.es/captura-gestion-discos-windows](http://e.digitall.org.es/captura-gestion-discos-windows).



Si volem triar una partició, podem accedir-hi amb el botó dret al menú d'opcions. Si preferim l'opció de formatjar la partició, entre les opcions disponibles, podrem triar el tipus de formatació: ràpida o de baix nivell.

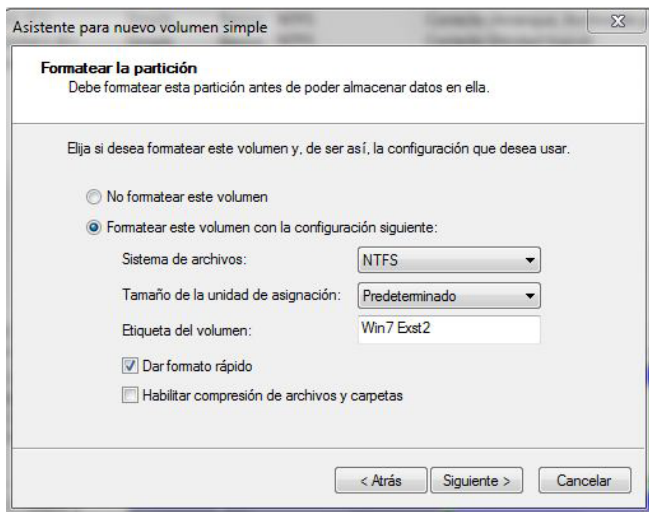


Figura 2. Opcions de formatació per a una partició del programa de gestió de discos de Windows. Imatge amb llicència CCC obtinguda d'[e.digitall.org.es/captura-formateo-particion](http://e.digitall.org.es/captura-formateo-particion).

## Utilitat de Discos de MacOS

La utilitat de discos d'Apple es troba a la carpeta d'Aplicacions dins d'una altra carpeta anomenada Utilitats.

La part esquerra de la finestra ens mostra totes les unitats connectades a l'equip (internes o externes) i les particions que hi contenen.

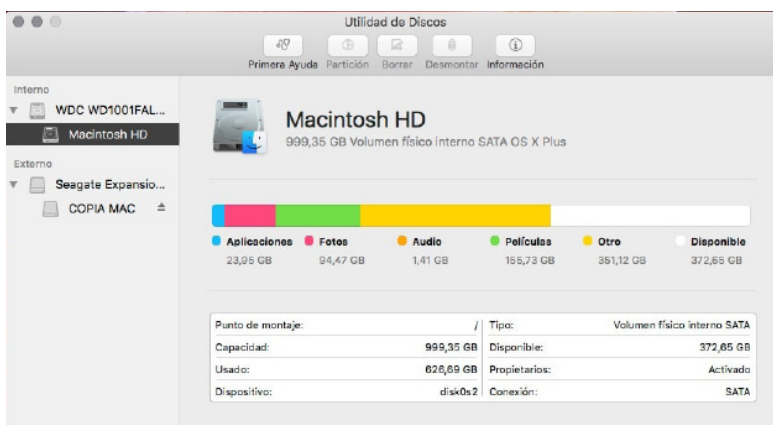


Figura 3. Finestra principal de la utilitat de discos de MacOS. Imatge amb llicència CCC obtinguda d'[e.digitall.org.es/captura-utilidad-discos](http://e.digitall.org.es/captura-utilidad-discos).



Si seleccionem una partició, podem veure, a la part superior de la finestra, les opcions disponibles. Si seleccionem la pestanya "Esborrar" podem triar el tipus de formatació fent clic al botó d'"Opcions de seguretat".

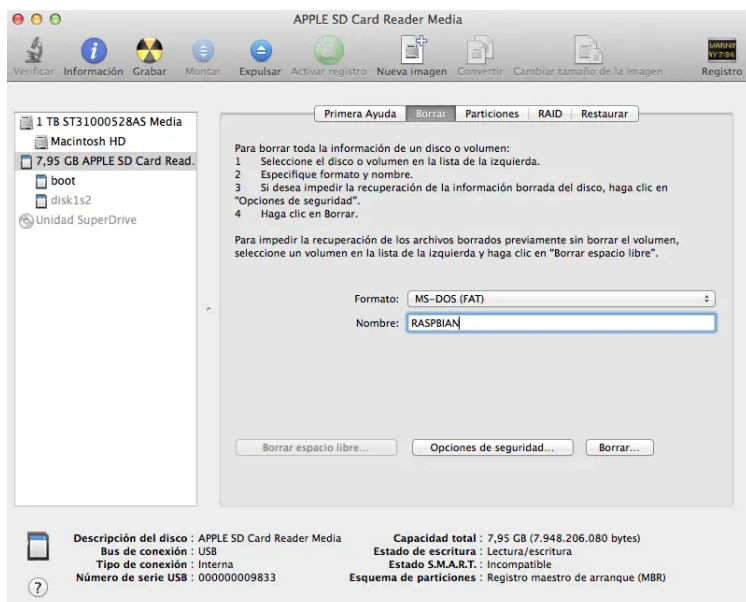


Figura 4. Opcions de formatació per a una partició de la utilitat de discos de MacOS. Imatge amb llicència CCC obtinguda [e.digitall.org.es/ibai](http://e.digitall.org.es/ibai).







## Estratègies per evitar pèrdues d'informació

L'ús diari de dispositius electrònics com ordinadors, tauletes i telèfons intel·ligents planteja la necessitat de definir estratègies per preservar la informació que volem emmagatzemar-hi.

Us volem proposar un conjunt d'idees que podem aplicar per evitar pèrdues d'informació.

- Heu de procurar que els vostres dispositius no pateixin cops, caigudes i que no funcionin en entorns amb molta humitat o pols.
- Cal que feu net habitualment els ventiladors dels ordinadors de sobretaula i portàtils usant aire comprimit.
- Feu servir Sistemes d'Alimentació Ininterrompuda (SAI) per a ordinadors de taula.
- És convenient que empreu alimentadors i carregadors adequats per al vostre portàtil i dispositius mòbils. Comprovau el bon estat del cablejat de connexió.
- Protegiu els dispositius de càrregues electroestàtiques.
- Feu còpies de seguretat de les dades en unitats de memòria externes amb regularitat. Podeu utilitzar:
  - Discos durs USB per fer còpies de seguretat de l'ordinador o portàtil.
  - Targetes de memòria Flaix SD per als dispositius Android o connexió directa per cable per als dispositius IOS d'Apple.
  - Sistemes d'emmagatzematge de núvol per tenir còpia de les dades disponibles per a tots els dispositiu que tingueu
- Programes antivirus i programari antimaliciós.
- Protegiu les teves contrasenyes, per exemple, amb algun programa gestor de contrasenyes i actualitza-les periòdicament.
- Cal que actualitzeu sovint tant el sistema operatiu com les aplicacions dels dispositius quan hi hagi actualitzacions disponibles.



Cerca i gestió  
d'informació i dades

**Nivell B2 1.3** Gestió de dades, informació  
i continguts digitals

# Gestió de continguts comprimits



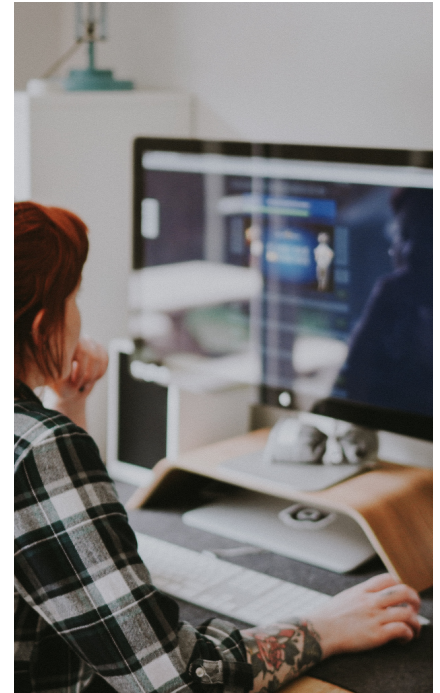


## Gestió de continguts comprimits

### Compressió de fitxers

La compressió de fitxers és una pràctica habitual per reduir la mida de les dades emmagatzemades i transferir-les a altres dispositius. Els mètodes típics de compressió de fitxers cerquen patrons de repetició de bits per reduir la quantitat d'emmagatzematge necessari per desar la informació original.

Hi ha tipus de fitxers que produeixen ràtios baixes de compressió, ja que plantegen una estructura d'emmagatzematge d'informació molt compacta. Aquest és el cas de formats multimèdia com MP3, JPG o AVI i també alguns documents, com PDF i els de Microsoft Office.



#### DISPOSITIUS D'EMMAGATZEMATGE LOCALS

*Formatació d'unitats d'emmagatzematge. Formatació ràpida i formatació a baix nivell per eliminar permanentment la informació. Còpia de la informació amb l'ús d'eines de compressió d'arxius per transferir volums de dades grans i arxius de còpies de seguretat.*

[e.digitall.org.es/A1C13B2V03](http://e.digitall.org.es/A1C13B2V03)

La comprensió de fitxers permet als usuaris fer còpies de seguretat i emmagatzemar la informació amb més rapidesa, especialment quan es tracta de fitxers molt grans. A més, fa que la transferència de fitxers sigui més àgil i es millora la integritat de dades que puguin veure's afectades per la corrupció de fitxers. Per altra banda, als arxius comprimits, no s'hi pot accedir directament, ja que convé descomprimir-los abans d'accedir al contingut.



## Fitxers .zip

El format de fitxer ZIP suporta la comprensió de dades sense pèrdues d'informació. Un fitxer ZIP pot contenir diversos fitxers i directoris. L'extensió que empra pot ser .zip o .ZIP. És el format de comprensió d'arxius més emprat i l'any 2015 es va concretar un estàndard amb restriccions per garantir la compatibilitat entre plataformes.

### Saber-ne més

El format de fitxers ZIP es va crear el 1989 com a substitut del format de comprensió ARC. Suporta diferents esquemes de comprensió i el mètode DEFLATE és el més comú.

Podeu tenir-ne més informació al següent enllaç:

[e.digitall.org.es/zip](http://e.digitall.org.es/zip)



## Fitxers .rar

El format de fitxer RAR és un format d'arxiu privat amb un algorisme de compresió sense pèrdues que va ser desenvolupat per l'enginyer rus de programari Eugene Roshal. L'algorisme de compresió és més lent que el format ZIP, però té una taxa de compresió i una redundància de dades millors. L'extensió de fitxer que s'utilitza per al volum compromès és .rar, i per al volum de recuperació s'empra .rev. A banda, admet la divisió de fitxers comprimits en volums (fitxers amb extensions .r00, .r01, etc.).

### Saber-ne més

El format de fitxers RAR es va crear el 1993. La versió 3 està basada en els mètodes de compresió Lempel-ZIV i LZSS i d'emparellament parcial predictiu PPM.

Podeu tenir-ne més informació als enllaços següents:

[e.digitall.org.es/rar](http://e.digitall.org.es/rar)



## Fitxers .7z

El format de fitxer 7z és un format d'arxiu que suporta diferents nivells de compressió de dades i, fins i tot, d'encryptació.

L'estàndard es va fer públic el 2008 sota una llicència GNU i cada vegada és més popular. Proporciona nivells de compressió millors, encara que el format de fitxer RAR és més lent. També admet la divisió de fitxers comprimits en volums.

Com a limitació principal, no emmagatzema permisos dels fitxers que es comprimeixen, per la qual cosa resulta inadequat per fer còpies de seguretat. Tampoc no incorpora la possibilitat de crear volums de recuperació de dades.

### Saber-ne més

El format de fitxers .7z empra com a mètode de compressió més habitual LZMA i suporta encryptació AES amb clau de 256 bits.

Podeu tenir-ne més informació al següent enllaç:

[e.digitall.org.es/7z](http://e.digitall.org.es/7z)





## Eines per a la comprensió de fitxers

Els sistemes operatius Microsoft Window i Apple MacOS tenen suport per a la comprensió i descomprensió de fitxers en format ZIP sense la necessitat d'instal·lar aplicacions de tercers. No obstant això, existeixen altres eines gratuïtes o de pagament per llicència desenvolupades per tercers que es poden fer servir.

### Microsoft Windows

Una alternativa molt coneguda per manejar fitxers ZIP als sistemes Microsoft Windows és WinZIP. El programa permet comprimir fitxers seleccionats a l'Explorador de Windows amb una opció directa amb el botó dret del ratolí.

La part central de la finestra ens mostra tots els fitxers comprimits amb la ràtio de comprensió que s'aconsegueix. A més, l'eina facilita afegir fitxers a un arxiu ZIP que ja existeixi (per exemple, seleccionant els fitxers i arrossegant-los a la zona central de la finestra), extreure'ls individualment o previsualitzar-los.



Figura 1. Finestra principal del programa WinZIP per a Windows. Imatge amb llicència CCC obtinguda d'[e.digitall.org.es/captura-winzip](http://e.digitall.org.es/captura-winzip).



Una altra eina molt emprada per manejar fitxers RAR als sistemes Microsoft Windows és WinRAR. El programa té les mateixes característiques i una interfície d'usuari semblant a WinZIP.

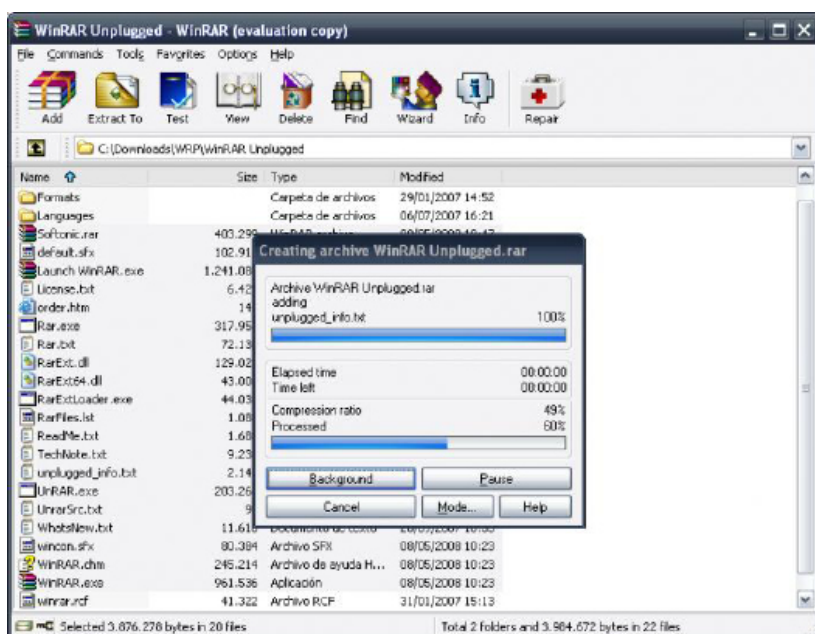


Figura 2. Finestra principal del programa WinRAR per a Windows. Imatge amb llicència CCC obtinguda d'[e.digitall.org.es/captura-winar](http://e.digitall.org.es/captura-winar)

Finalment, per controlar fitxers 7z als sistemes Windows tenim el programa 7-Zip. El programa té les mateixes característiques i una interfície d'usuari similar als anteriors.

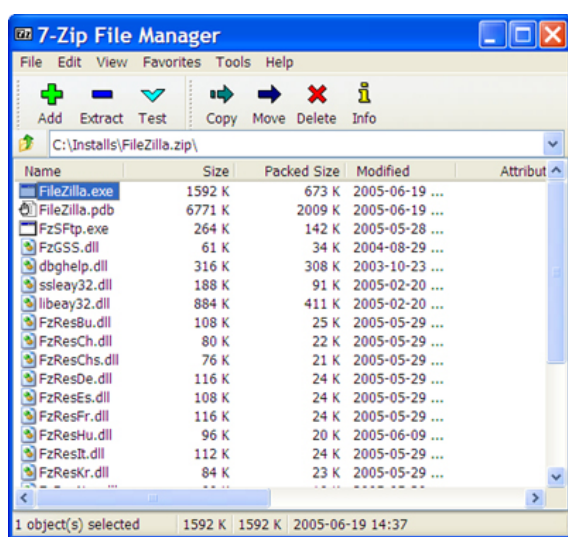


Figura 3. Finestra principal del programa 7-Zip per a Windows. Imatge amb llicència CCC obtinguda d'[e.digitall.org.es/captura-7z](http://e.digitall.org.es/captura-7z).



## Apple MacOS

Existeixen versions de WinZip, WinRar i 7-Zip per als sistemes Apple MacOS, amb les mateixes funcionalitats que a Microsoft Windows. Altres compressors molt emprats als sistemes Apple MacOS són The Unarchiver, KeKa i iZip.

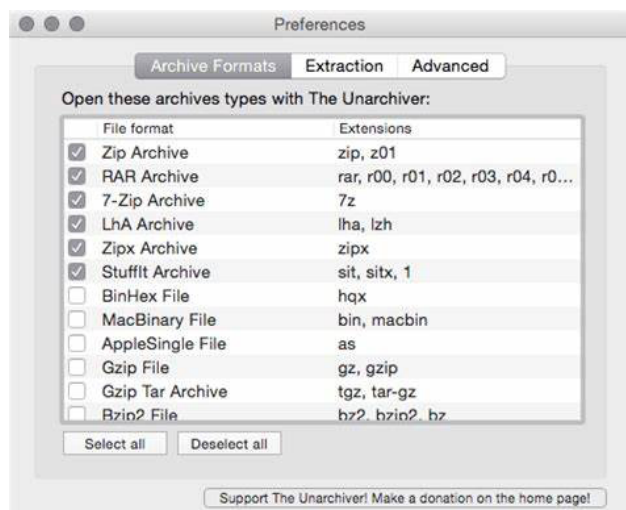


Figura 4. Opcions de format d'arxiu comprimit disponibles per a The Unarchiver. Imatge amb llicència obtinguda d'[e.digitall.org.es/unarchiver](http://e.digitall.org.es/unarchiver).

### Saber-ne més

A aquest document només hem anomenat alguns dels programes més utilitzats per a la comprensió i descomprensió dels formats d'arxiu comprimit ZIP, RAR i 7z.

Existeixen molts de programes que podeu consultar a la taula disponible a l'enllaç següent:

[e.digitall.org.es/comparison-archivers](http://e.digitall.org.es/comparison-archivers)





Cerca i gestió  
d'informació i dades

**Nivell B2 1.3** Gestió de dades, informació  
i continguts digitals

# Gestió de continguts de còpies de seguretat





## Gestió de continguts de còpies de seguretat

### Gestió de còpies de seguretat

La còpia de seguretat consisteix a emmagatzemar periòdicament la informació crítica personal o de treball en un altre dispositiu o localització secundària, per tal d'evitar pèrdues d'informació quan existeix la possibilitat d'errors que afecten l'emmagatzematge principal: maquinari, errors humans, ciberatacs, corrupció dels fitxers o desastres naturals. La informació que es considera crítica sol consistir en documents, imatges, vídeos i arxius de configuració.

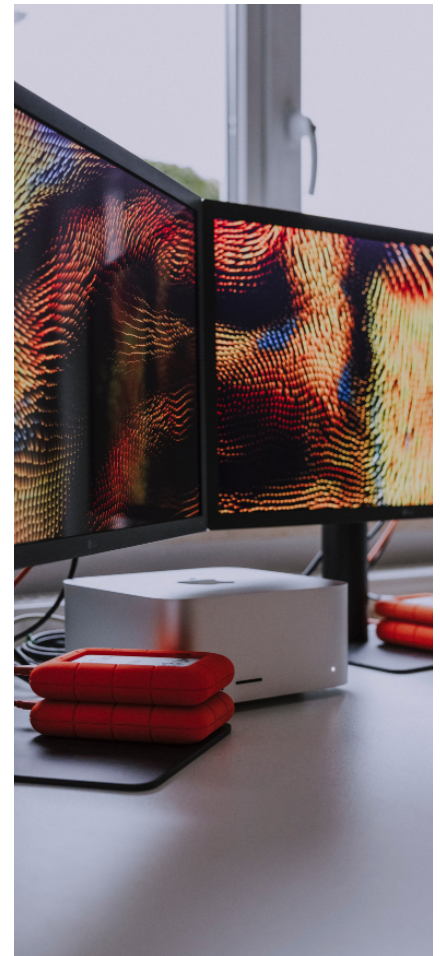
Una estratègia de còpia de seguretat adequada haurà de permetre, en un temps adequat, la recuperació dels fitxers de dades a un estat adient anterior de quan es va perdre.

### Tipos de copia de seguridad

Una còpia de seguretat completa de totes les dades és la que requereix més temps i més espai d'emmagatzematge.

La còpia de seguretat incremental es produeix quan es crea una còpia d'aquells arxius nous o modificats des de la darrera vegada que es va fer la còpia de seguretat. Aquesta estratègia és més ràpida que la còpia de seguretat completa i exigeix menys emmagatzematge. Si la recuperació de dades fos necessària caldria disposar de totes les còpies de seguretat incrementals. Igualment, si s'ha de recuperar la còpia de seguretat d'un fitxer en concret, hauríem de menester cercar-lo per tot el repositori de còpies incrementals.

La còpia de seguretat diferencial radica a crear la còpia d'aquells arxius nous o modificats des de la darrera vegada que es va fer una còpia de seguretat completa.





### **i** Saber-ne més

El temps de còpies de seguretat que garanteix que es perdin el mínim de dades es coneix com a Protecció de Dades Contínua (CDP) o còpia de seguretat en temps real. Aquest plantejament és molt intensiu per als recursos, atès que fa còpia de seguretat de cada fitxer sempre que s'hi fa algun canvi.

Podeu tenir-ne més informació al següent enllaç:

[e.digital.org.es/data-protection](https://e.digital.org.es/data-protection)

## Bones pràctiques

La primera passa és planificar correctament les còpies de seguretat. Per aquesta raó, convé considerar els següents aspectes:

### **1** | Determinar la importància de les dades i el corresponent nivell de disponibilitat

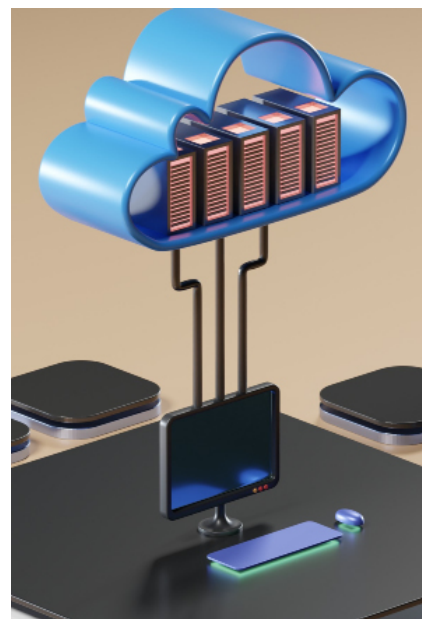
El volum d'informació i el temps necessari per fer les còpies de seguretat i poder-les recuperar són aspectes fonamentals.

Si és necessari fer una còpia de seguretat d'un gran volum d'informació, caldrà que se n'identifiqui la informació crítica. Aquest fet facilitarà definir les propietats segons la importància que tinguin.

### **2** | Decidir la freqüència i mitjans per a les còpies de seguretat

El nivell d'importància de dades i la freqüència amb què s'actualitzen els fitxers són aspectes clau per decidir quina serà la freqüència de les còpies de seguretat i els recursos que hàgim d'emprar durant el procés.

Les opcions per fer còpies de seguretat són extenses. Quan hi ha un gran volum de dades, es poden emprar directament dispositius externs com CDs, DVDs, discos Blu-Ray, discos durs HDD o memòries externes. També, es podran utilitzar dispositius externs adhoc que proporcionaran tant maquinari com programari. Una altra opció és l'ús de programari per a la còpia de seguretat o serveis que es basen en el núvol.





### 3 | Implementar el pla de còpia de seguretat

Una vegada hem identificat les necessitats per a la còpia de seguretat, és convenient que es defineixi un responsable que administri (si és una organització) les còpies de seguretat, les eines i suports físics, l'àmbit de les còpies de seguretat, la planificació temporal, el nivell d'automatització del procés i els temps de recuperació necessaris.

L'administrador serà el responsable de documentar el procés de còpia de seguretat i recuperació.

### 4 | Comprovar la correcció de la còpia de seguretat

El responsable de la còpia de seguretat de les dades n'haurà de verificar periòdicament el procés i correcció. Això és important per garantir que, en cas que sigui necessari, es minimitzin les pèrdues de dades. A més, pot donar una mesura dels temps necessari per a la recuperació de la informació.

### 5 | Definir criteris per revisar posteriorment el pla de còpia de seguretat

Els canvis d'activitat poden modificar el tipus i els volums de dades que s'empren. L'administrador responsable de les còpies de seguretat podrà identificar els canvis dels volums de dades i els temps necessaris per fer còpies de seguretat de l'organització que requereixen la revisió del pla d'aquestes còpies.

#### Saber-ne més

Una estratègia molt utilitzada per aquestes còpies és la que es coneix com a 3-2-1. L'estratègia planteja la realització de tres còpies de seguretat de les dades. Aquestes s'han de fer en almenys dos dispositius o recursos diferents, i com a mínim, una còpia s'ha de desar remotament.

Podeu tenir-ne més informació en el següent enllaç:

[e.digitall.org.es/backup](https://e.digitall.org.es/backup)



## Eines de còpia de seguretat

Si cal automatitzar el procés de realització de còpies de seguretat es pot utilitzar un programari específic que fa les còpies de manera programada.

Els programes de còpia de seguretat incorporen un sistema de control de versions automàtic. Aquest permet fer un seguiment dels canvis que es duen a terme dels fitxers i estructures de directoris fent servir un sistema de control de dades de creació de les còpies de seguretat i dels fitxers hi continguts. Una versió, revisió o edició d'una còpia de seguretat és l'estat en què es troba el conjunt de dades en un moment donat.

### Ordinadors amb sistemes operatius Microsoft Windows i Apple MacOS

Les versions recents de Microsoft Windows disposen d'un programa senzill anomenat "Còpia de seguretat i restauració" que permet gestionar còpies de seguretat dels fitxers que tenim, per exemple, en un disc dur HDD connectat mitjançant USB. Apple MacOS disposa d'una utilitat anàloga anomenada Time Machine. Si hi ha emmagatzematge de núvol podem, fer-hi les còpies de seguretat directament.

Existeixen nombroses eines amb funcionalitats més sofisticades que permeten còpies de seguretat incrementals, còpies de seguretat diferencials o la creació d'unitats externes d'arrencada per a la recuperació de l'ordinador. Aquest és el cas de MiniTool ShadowMaker o Iperius Còpia de seguretat.



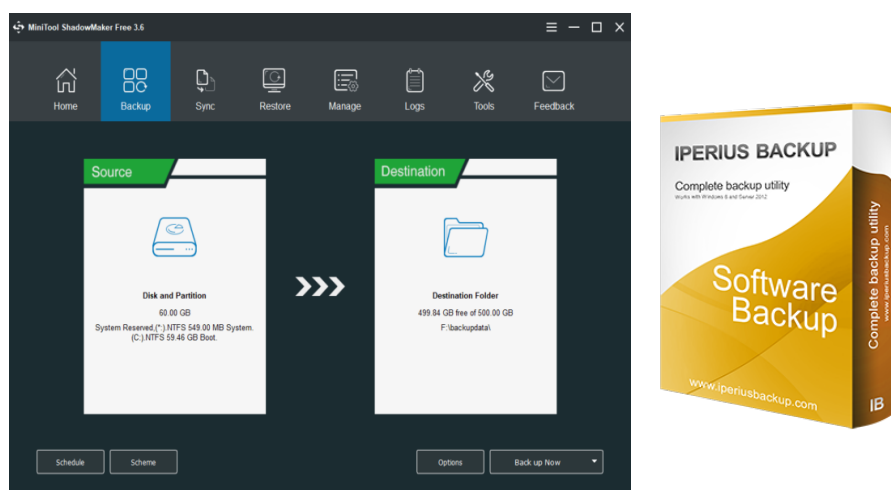


Figura 1. Programari de còpia de seguretat per a Windows MiniTool ShadowMaker i Iperius Backup. Imatges de llicència CCC obtingudes d'[e.digitall.org.es/shadowmaker](http://e.digitall.org.es/shadowmaker), [e.digitall.org.es/iperius](http://e.digitall.org.es/iperius).

## Dispositius Android

Per als dispositius mòbils amb sistema operatiu Android hi ha moltes utilitats que podem instal·lar per fer còpies de seguretat fent servir una targeta de memòria Flaix SD. Aquest és el cas de Solid Explorer o Dr.Fone.

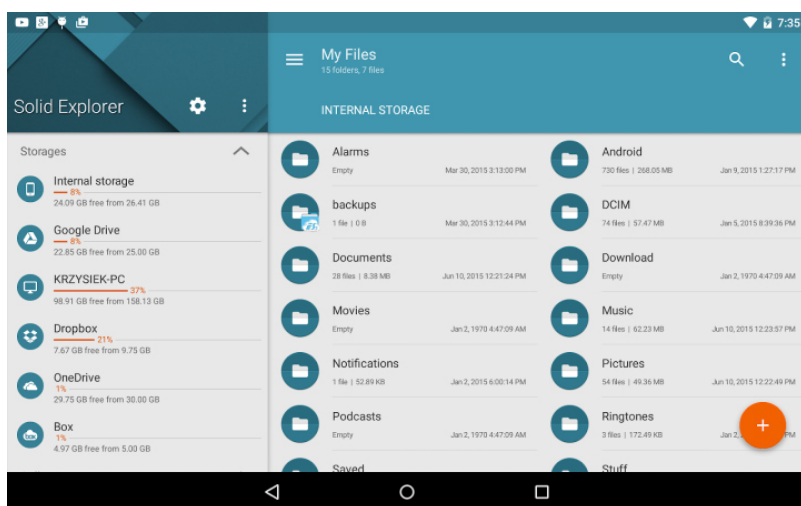


Figura 2. Aplicacions de còpia de seguretat per a Android a les targetes d'emmagatzematge SD. Imatges de llicència CCC obtingudes d'[e.digitall.org.es/solid-explorer](http://e.digitall.org.es/solid-explorer), [e.digitall.org.es/drfone](http://e.digitall.org.es/drfone).



## Solucions de còpia de seguretat al núvol

Una de les estratègies recomanades en la realització de còpies de seguretat és la poder tenir una còpia de les dades en una altra ubicació física diferent.

El creixement dels serveis basats en el núvol ha permès l'aparició de solucions molt més completes que permeten fer còpies de seguretat de la informació que hi ha als ordinadors i dispositius mòbils de manera transparent i automàtica. L'únic requisit indispensable és que tinguin connexió a Internet per poder fer la còpia de seguretat quan s'hagi estipulat.



Figura 3. Entorn de còpia de seguretat al núvol IDrive, BlackBlaze i Acronis Cyber Protect s. Imatges amb llicència CCC obtingudes d'[e.digitall.org.es/idrive](https://e.digitall.org.es/idrive), [e.digitall.org.es/blackblaze](https://e.digitall.org.es/blackblaze), [e.digitall.org.es/acronis](https://e.digitall.org.es/acronis).



# DigitAll

Formación en  
Competencias  
Digitales





## Coordinación General

**Universidad de Castilla-La Mancha**  
Carlos González Morcillo  
Francisco Parreño Torres

## Coordinadores de área

### Área 1. Búsqueda y gestión de información y datos

**Universidad de Zaragoza**  
Francisco Javier Fabra Caro

### Área 2. Comunicación y colaboración

**Universidad de Sevilla**  
Francisco Javier Fabra Caro  
Francisco de Asís Gómez Rodríguez  
José Mariano González Romano  
Juan Ramón Lacalle Remigio  
Julio Cabero Almenara  
María Ángeles Borrueco Rosa

### Área 3. Creación de contenidos digitales

**Universidad de Castilla-La Mancha**  
David Vallejo Fernández  
Javier Alonso Albusac Jiménez  
José Jesús Castro Sánchez

### Área 4. Seguridad

**Universidade da Coruña**  
Ana M. Peña Cabanas  
José Antonio García Naya  
Manuel García Torre

### Área 5. Resolución de problemas

**UNED**  
Jesús González Boticario

## Coordinadores de nivel

### Nivel A1

**Universidad de Zaragoza**  
Ana Lucía Esteban Sánchez  
Francisco Javier Fabra Caro

### Nivel A2

**Universidad de Córdoba**  
Juan Antonio Romero del Castillo  
Sebastián Rubio García

### Nivel B1

**Universidad de Sevilla**  
Francisco de Asís Gómez Rodríguez  
José Mariano González Romano  
Juan Ramón Lacalle Remigio  
Montserrat Argandoña Bertran

### Nivel B2

**Universidad de Castilla-La Mancha**  
María del Carmen Carrión Espinosa  
Rafael Casado González  
Víctor Manuel Ruiz Penichet

### Nivel C1

**UNED**  
Antonio Galisteo del Valle

### Nivel C2

**UNED**  
Antonio Galisteo del Valle

## Maquetación

**Universidad de Salamanca**  
Fernando De la Prieta Pintado  
Pilar Vega Pérez  
Sara Alejandra Labrador Martín

# Creadores de contenido

## Área 1. Búsqueda y gestión de información y datos

### 1.1 Navegar, buscar y filtrar datos, información y contenidos digitales

#### Universidad de Huelva

Ana Duarte Hueros (coord.)  
Arantxa Vizcaíno Verdú  
Carmen González Castillo  
Dieter R. Fuentes Cancell  
Elisabetta Brandi  
José Antonio Alfonso Sánchez  
José Ignacio Aguaded  
Mónica Bonilla del Río  
Odriel Estrada Molina  
Tomás de J. Mateo Sanguino (coord.)

### 1.2 Evaluar datos, información y contenidos digitales

#### Universidad de Zaragoza

Ana Belén Martínez Martínez  
Ana María López Torres  
Francisco Javier Fabra Caro  
José Antonio Simón Lázaro  
Laura Bordonaba Plou  
María Sol Arqued Ribes  
Raquel Trillo Lado

### 1.3 Gestión de datos, información y contenidos digitales

#### Universidad de Zaragoza

Ana Belén Martínez Martínez  
Francisco Javier Fabra Caro  
Gregorio de Miguel Casado  
Sergio Ilarri Artigas

## Área 2. Comunicación y colaboración

### 2.1 Interactuar a través de tecnología digitales

Iseazy

### 2.2 Compartir a través de tecnologías digitales

#### Universidad de Sevilla

Alién García Hernández  
Daniel Agüera García  
Jonatan Castaño Muñoz  
José Candón Mena  
José Luis Guisado Lizar

### 2.3 Participación ciudadana a través de las tecnologías digitales

#### Universidad de Sevilla

Ana Mancera Rueda  
Félix Biscarri Triviño  
Francisco de Asís Gómez Rodríguez  
Jorge Ruiz Morales  
José Manuel Sánchez García  
Juan Pablo Mora Gutiérrez  
Manuel Ortigueira Sánchez  
Raúl Gómez Bizcocho

### 2.4 Colaboración a través de las tecnologías digitales

#### Universidad de Sevilla

Belén Vega Márquez  
David Vila Viñas  
Francisco de Asís Gómez Rodríguez  
Julio Barroso Osuna  
María Puig Gutiérrez  
Miguel Ángel Olivero González  
Óscar Manuel Gallego Pérez  
Paula Marcelo Martínez

### 2.5 Comportamiento en la red

#### Universidad de Sevilla

Ana Mancera Rueda  
Eva Mateos Núñez  
Juan Pablo Mora Gutiérrez  
Óscar Manuel Gallego Pérez

### 2.6 Gestión de la identidad digital

Iseazy

## Área 3. Creación de contenidos digitales

### 3.1 Desarrollo de contenidos

#### Universidad de Castilla-La Mancha

Carlos Alberto Castillo Sarmiento  
Diego Cordero Contreras  
Inmaculada Ballesteros Yáñez  
José Ramón Rodríguez Rodríguez  
Rubén Grande Muñoz

### 3.2 Integración y reelaboración de contenido digital

#### Universidad de Castilla-La Mancha

José Ángel Martín Baos  
Julio Alberto López Gómez  
Ricardo García Ródenas

### 3.3 Derechos de autor (copyright) y licencias de propiedad intelectual

#### Universidad de Castilla-La Mancha

Gabriela Raquel Gallicchio Platino  
Gerardo Alain Marquet García

### 3.4 Programación

#### Universidad de Castilla-La Mancha

Carmen Lacave Roderó  
David Vallejo Fernández  
Javier Alonso Albusac Jiménez  
Jesús Serrano Guerrero  
Santiago Sánchez Sobrino  
Vanesa Herrera Tirado

## Área 4. Seguridad

### 4.1 Protección de dispositivos

#### Universidade da Coruña

Antonio Daniel López Rivas  
José Manuel Vázquez Naya  
Martíño Rivera Dourado  
Rubén Pérez Jove

### 4.2 Protección de datos personales y privacidad

#### Universidad de Córdoba

Aida Gema de Haro García  
Ezequiel Herruzo Gómez  
Francisco José Madrid Cuevas  
José Manuel Palomares Muñoz  
Juan Antonio Romero del Castillo  
Manuel Izquierdo Carrasco

### 4.3 Protección de la salud y del bienestar

#### Universidade da Coruña

Javier Pereira Loureiro  
Laura Nieto Riveiro  
Laura Rodríguez Gesto  
Manuel Lagos Rodríguez  
María Betania Groba González  
María del Carmen Miranda Duro  
Nereida María Canosa Domínguez  
Patricia Concheiro Moscoso  
Thais Pousada García

### 4.4 Protección medioambiental

#### Universidad de Córdoba

Alberto Membrillo del Pozo  
Alicia Jurado López  
Luis Sánchez Vázquez  
María Victoria Gil Cerezo

## Área 5. Resolución de problemas

### 5.1 Resolución de problemas técnicos

Iseazy

### 5.2 Identificación de necesidades y respuestas tecnológicas

Iseazy

### 5.3 Uso creativo de la tecnología digital

Iseazy

### 5.4 Identificar lagunas en las competencias digitales

Iseazy



El material del proyecto DigitAll se distribuye bajo licencia CC BY-NC-SA 4.0. Puede obtener los detalles de la licencia completa en: <https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>