



Opoademia

GUIA D'ESTUDI COMPLETA

ACTIC · Certificat mitjà (competències digitals)

Generalitat de Catalunya · Competències digitals (ACTIC)

Grup ACTIC nivell 2 (mitjà) · 5 temes amb apunts explicats

250 preguntes d'examen disponibles

Material original, redactat per Opoademia

opoademia.com

Acadèmia d'oposicions en català · Tests, simulacres i tutor IA

**AVÍS LEGAL**

Drets d'autor i condicions d'ús

© 2026 Opoademia. Tots els drets reservats.

Aquest document i tot el seu contingut (textos, estructura, esquemes, exemples i disseny) són propietat exclusiva d'Opoademia (opoademia.com) i estan protegits per la legislació espanyola i internacional sobre propietat intel·lectual, en particular pel Reial decret legislatiu 1/1996, de 12 d'abril, pel qual s'aprova el Text refós de la Llei de propietat intel·lectual.

Queda **rigorosament prohibida**, sense l'autorització escrita i expressa d'Opoademia, qualsevol forma de **reproducció, còpia, distribució, comunicació pública, transformació, lloguer, préstec, posada a disposició, revenda o explotació comercial**, total o parcial, d'aquest document, per qualsevol mitjà o procediment, electrònic o mecànic, inclosos la fotocòpia, l'escaneig i la publicació a internet.

Aquest material es lliura per a l'**ús personal, privat i intransferible** de la persona usuària que l'ha obtingut legítimament a través d'Opoademia. La seva cessió, difusió, compartició o venda a tercers en vulnera els drets d'autor.

L'incompliment d'aquestes condicions podrà donar lloc a les **responsabilitats civils i penals** corresponents, entre d'altres les previstes als articles 270 i següents del Codi penal.

Aquest material té finalitat exclusivament formativa i de suport a l'estudi. No és un document oficial i no substitueix les fonts oficials de cada convocatòria (DOGC, BOE i bases de la convocatòria), que sempre prevalen. Opoademia procura mantenir el contingut actualitzat, però no garanteix que estigui lliure d'errors ni que reflecteixi els darrers canvis normatius.

Per a autoritzacions, llicències o consultes: opoademia.com



CONTINGUTS

Índex

	PÀG.
1. Àrea 1. Alfabetització informacional i de dades	3
2. Àrea 2. Comunicació i col·laboració	17
3. Àrea 3. Creació de continguts digitals	31
4. Àrea 4. Seguretat	46
5. Àrea 5. Resolució de problemes	59

**1****TEMA****Àrea 1. Alfabetització informacional i de dades****Cercar informació de manera eficient a internet**

A nivell mitjà, l'ACTIC dona per fet que saps obrir un navegador i escriure una consulta; el que avalua és si saps convertir una necessitat d'informació en una cerca precisa. La majoria de gent escriu frases senceres al cercador ("com puc saber si...") i es conforma amb els tres primers resultats. Una cerca eficient funciona diferent: es trien un grapat de paraules clau (els termes que probablement apareixeran al document que busques, no la pregunta tal qual) i s'utilitzen operadors per acotar.

Pensa-hi com si li fessis la pregunta a algú que no pot interpretar matisos: el cercador no "entén" què vols dir, només busca patrons de text. Si vols saber quin dia és l'últim per presentar la declaració de la renda, escriure "quan he de fer la declaració de la renda si no ho he fet mai" dona resultats pitjors que escriure "termini declaració renda 2026 Agència Tributària". El primer és com parles amb un amic; el segon és com parla el document oficial que busques. Aquest pas mental (amb quines paraules ho diria el document que necessito, no jo mateix) és la base de qualsevol cerca eficient i és, de fet, la primera cosa que separa un usuari bàsic d'un usuari autònom davant d'un cercador.

Convertir una necessitat d'informació en una pregunta cercable

Abans d'escriure res al quadre de cerca, val la pena fer-se tres preguntes ràpides:

1. Quin és exactament el resultat que necessito (una dada, un document, una instrucció, una opinió contrastada)?
2. Quines paraules faria servir la font que el conté (un ajuntament, un mitjà, un fabricant) per anomenar-ho?
3. Necessito acotar per lloc, per data o per tipus de document?

Un exemple pràctic: vols saber com demanar cita al CAP del teu barri perquè el metge de capçalera et faci un volant. En lloc d'escriure "com demano hora al metge", una cerca més eficient seria "cita prèvia CAP + nom del barri" o directament anar al lloc del Servei Català de la Salut i fer servir el cercador intern amb el nom del centre. Si el que vols és un tràmit concret de l'ajuntament (per exemple, empadronar-te), la paraula clau no és "com m'empadrono" sinó "empadronament" o "alta padró municipal", combinada amb site: i el domini de l'ajuntament corresponent.

Operadors de cerca bàsics

Els operadors més habituals a Google (i que funcionen també, amb petites diferències, a Bing o DuckDuckGo):

- Cometes ("frase exacta"): busca la cadena tal com està escrita. Útil per a cites textuais, noms d'empresa o codis d'error.
- Signe menys (-paraula): exclou resultats que continguin aquest terme. Per exemple, jaguar -cotxe si busques l'animal.
- site:domini.cat: limita la cerca a un lloc web concret o a un domini (site:gencat.cat, site:.edu).
- filetype:pdf: només mostra documents d'un format determinat.
- OR (en majúscules): combina termes alternatius, per exemple "subvenció" OR "ajut" autònoms.



- El filtre de data, disponible a "Eines" o "Cerca avançada": permet acotar per l'última setmana, mes o any, imprescindible quan la informació canvia sovint (normativa, preus, dades sanitàries).

Aquests operadors es poden combinar entre ells, i és precisament aquesta combinació el que sol distingir una pregunta d'examen de nivell mitjà: no es tracta de conèixer un operador aïllat, sinó de saber-los encadenar per resoldre una necessitat real. Per exemple, si vols trobar el text exacte d'una ordenança municipal sobre terrasses de bars però només al web oficial de l'Ajuntament de Girona, en PDF, la cerca completa seria:

"ordenança terrasses" site:girona.cat filetype:pdf

Fixa't que cada operador s'escriu enganxat al terme que afecta (site:girona.cat, no site: girona.cat, amb espai), i que els operadors es poden intercalar amb paraules soltes sense cometes. Un error molt habitual és posar espai després dels dos punts: site: gencat.cat no funciona igual que site:gencat.cat, perquè el cercador interpreta "site:" i "gencat.cat" com dues cerques diferents.

DuckDuckGo té els mateixos operadors bàsics i l'avantatge que no personalitza els resultats segons el teu historial, cosa que a vegades dona una visió més neutra. Val la pena conèixer també els cercadors especialitzats: Google Scholar per a articles acadèmics, o el cercador intern d'una administració (per exemple, el del Diari Oficial de la Generalitat) quan cerques normativa concreta.

La cerca avançada del propi cercador

Molta gent no sap que, a banda d'escriure operadors a mà, la majoria de cercadors ofereixen un formulari de "Cerca avançada" que fa exactament el mateix però amb camps separats: un camp per a "aquesta frase exacta", un altre per a "cap d'aquestes paraules", un altre per a "aquest lloc o domini". És útil quan no recordes bé la sintaxi d'un operador o quan vols combinar-ne diversos sense equivocar-te de puntuació. A Google hi arribes escrivint una cerca qualsevol i després anant a Configuració > Cerca avançada, o directament escrivint "cerca avançada google" al cercador.

A banda dels operadors del cercador, hi ha un parell de filtres que sovint es passen per alt perquè estan amagats en menús secundaris. A "Eines" (o "Cerca avançada"), a més del filtre de data, trobaràs un filtre de tipus de contingut que et permet demanar només imatges, notícies, vídeos o llocs web, cosa útil quan una paraula ambigua et retorna resultats de categories que no t'interessen. Per exemple, si busques "jaguar" per veure fotografies de l'animal i el cercador et satura de notícies sobre el cotxe, filtrar per "Imatges" primer, i després afinar amb -cotxe, sol donar resultats molt més nets que qualsevol de les dues estratègies per separat.

Pas a pas per acotar per data a Google (útil quan la informació canvia sovint, com una mesura sanitària, un preu o una normativa):

1. Fes la cerca normal al quadre de Google.
2. Un cop als resultats, fes clic a "Eines" (a sota del quadre de cerca, al costat de "Tot", "Imatges", "Notícies"...).
3. S'obrirà un desplegable amb "Qualsevol moment"; fes-hi clic i tria "Última hora", "24 hores", "Setmana", "Mes", "Any" o "Interval personalitzat" si necessites unes dates concretes.
4. Els resultats es refresquen automàticament amb el filtre aplicat.

I dins d'una pàgina web ja oberta, la combinació de tecles Ctrl+F (Cmd+F en Mac) obre un cercador intern que resalta totes les aparicions d'una paraula al document: és la manera correcta de trobar una dada concreta dins d'un PDF llarg o d'un article extens, en lloc de fer scroll llegint per sobre. Aquest gest tan senzill marca la diferència entre saber "buscar per internet" i saber "buscar la informació que necessites",



que és precisament el que avalua aquesta àrea.

Cercadors especialitzats

No tots els cercadors serveixen igual per a tot. Google Scholar (scholar.google.com) indexa només articles acadèmics, tesis i publicacions científiques, i és l'eina correcta quan necessites una font revisada per experts i no un article de divulgació. Moltes administracions tenen, a més, el seu propi cercador intern, sovint més precís que Google per trobar normativa concreta: el cercador del Diari Oficial de la Generalitat de Catalunya (DOGC), per exemple, permet filtrar per tipus de disposició, data de publicació o departament, cosa que Google no pot fer amb la mateixa precisió perquè no coneix l'estructura interna del document.

Un truc pràctic que apareix sovint als exàmens: si vols trobar un document oficial concret (una ordre, un formulari), combinar `site:` amb `filetype:pdf` i unes quantes paraules clau sol donar el resultat en primera posició, encara que el document no estigui ben indexat pel cercador general.

Cerca inversa d'imatges

Un altre recurs de cerca avançada és la cerca inversa d'imatges: arrossegar una fotografia a Google Imatges, o fer-hi clic dret i triar "Cercar imatge amb Google", permet saber en quins altres llocs ha aparegut aquella imatge i des de quan circula per internet. No és només una eina de verificació de notícies (que també, com veurem més endavant): serveix igualment per identificar un producte a partir d'una foto, trobar la font original d'una il·lustració o comprovar si una imatge de perfil sospitosa és en realitat una foto d'estoc reutilitzada.

Pas a pas per fer una cerca inversa d'imatges des del mòbil o l'ordinador:

1. Si la imatge ja és a internet: fes-hi clic dret (ordinador) o mantén-hi el dit premut (mòbil) i tria "Cercar imatge amb Google" o "Cercar amb Google Lens".
2. Si la imatge és al teu dispositiu (una captura, una foto feta amb el mòbil): obre images.google.com, fes clic a la icona de la càmera dins del quadre de cerca, i arrossega-hi la imatge o selecciona "Penjar un fitxer".
3. Google mostrarà webs on apareix aquesta imatge o imatges visualment semblants; revisa les dates i els contextos on ha aparegut per veure si és realment recent o reciclada.

Errors habituals en la cerca

Els errors més freqüents que penalitza l'examen (i que costen punts a la vida real) són: escriure la pregunta sencera en lloc de paraules clau; no fer servir mai cap operador tot i que la cerca ho demana explícitament; oblidar el filtre de data quan la informació és sensible al temps (una mesura sanitària, un preu, una convocatòria); i confondre "el primer resultat" amb "el resultat més fiable", quan en realitat la posició depèn també del SEO (posicionament) de la pàgina, no només de la seva qualitat. Recordat també que `site:` i `filetype:` s'escriuen sense espais i en minúscules, i que OR ha d'anar en majúscules perquè el cercador no l'interpreti com una paraula normal de la cerca.

Avaluar la fiabilitat de les fonts i les dades

Trobar informació és la part fàcil; saber si te la pots creure és on falla més gent. L'ACTIC nivell mitjà espera que sàpigues aplicar uns quants criteris de manera sistemàtica, no que confiïs en la "sensació" que et fa una pàgina. Pensa en aquest bloc com una llista de verificació mental que has d'aplicar gairebé sense pensar-hi, de la mateixa manera que mires el remitent d'un correu abans d'obrir un adjunt sospitos.



Qui hi ha darrere del contingut

Mira la secció "Qui som" o "Sobre nosaltres", busca l'autor de l'article i comprova si té credencials relacionades amb el tema. Un article sobre salut signat per algú sense cap referència professional pesa menys que un de la mateixa web sense signar però amb revisió editorial coneguda: si el mateix consell sobre un medicament apareix en un fòrum anònim i al web del Departament de Salut signat per un servei farmacèutic, la segona font té molt més pes, perquè la responsabilitat i la revisió que hi ha darrere és diferent.

Quan es va publicar i si s'ha actualitzat

Una notícia de fa cinc anys sobre una llei pot estar completament desfasada. Els llocs seriosos indiquen data de publicació i, si escau, data de la darrera revisió. Si un article no mostra cap data (un error de disseny sorprenentment habitual, sobretot en pàgines que es reutilitzen o es reciclen d'un any per l'altre), pots buscar-la per altres vies: la memòria cau de Google, l'historial de la Viquipèdia si en cita una versió, o simplement contrastar la informació amb una font que sí que doni el contingut. Quan trobes un article que respon exactament al que busques però no hi ha cap data visible, l'actitud més prudent no és descartar-lo directament, sinó buscar la data per altres vies o contrastar-lo abans de donar-lo per bo: aquest matís (ni "confiar-hi cegament" ni "descartar-lo sense mirar-hi més") és exactament el tipus de resposta que demana l'examen en preguntes de situació.

Contrastar amb fonts independents

Contrastar no vol dir buscar una segona pàgina que digui el mateix (podria ser la mateixa font copiada): vol dir buscar fonts amb interessos o orígens diferents que arribin a conclusions semblants. Si només una web ho diu i cap mitjà ni institució ho recull, sospita. Per exemple, si un blog assegura que un electrodomèstic té un defecte que "ningú explica" i només trobes el mateix text copiat literalment en altres blogs, sense cap mitjà de consum ni organisme oficial que ho reculli, és un indici fort que no hi ha contrast real, sinó una mateixa font repetida.

El domini i el to del contingut

Els dominis .gov, .edu o els oficials d'una administració (.gencat.cat, .administracion.gob.es) tenen un control editorial més alt, tot i que això no els fa infal·libles. Un to molt emocional, titulars en majúscules o que et demanen compartir "abans que ho censurin" són senyals típics de desinformació, dissenyats precisament per provocar una reacció emocional immediata que et faci compartir abans de pensar-hi, i és un dels exemples més recurrents a l'examen.

Biaix versus mentida

No tota font esbiaixada menteix: un mitjà pot seleccionar quines notícies destaca segons la seva línia editorial sense inventar-se dades. Reconèixer el biaix (a favor de qui juga la informació, què s'omet) és una competència diferent de detectar un bulo directe, i l'examen sol distingir-les. Per exemple, si un mitjà dona molta cobertura a les manifestacions d'un partit polític i pràcticament ignora les d'un altre, això és un biaix editorial en la selecció de notícies, no necessàriament una mentida; en canvi, si aquell mateix mitjà publica una xifra de participants que és clarament inventada o inflada sense cap font, això ja és desinformació directa. La clau per distingir-ho és preguntar-se: "hi ha una dada concreta que sigui falsa, o simplement s'ha triat parlar d'unes coses i no d'unes altres?".

Bombolles de filtre i algorismes

Un altre mecanisme que distorsiona el que veus, sense que cap font concreta menteixi, és el de la



bombolla de filtre: les xarxes socials i molts cercadors personalitzen els resultats segons el que has clicat abans, amb l'objectiu de mantenir-te més temps a la pantalla. El resultat pràctic és que dues persones que busquin el mateix tema poden veure continguts molt diferents, i que amb el temps només et vagin arribant opinions que ja coincideixen amb la teva, reforçant-la sense contrast. Ser conscient que l'algorisme selecciona per tu (no per rellevància objectiva, sinó per allò que preveu que et farà interactuar) és part de l'avaluació crítica que demana l'ACTIC: la solució passa per diversificar fonts de manera activa i no assumir mai que el que surt primer és "el més important", sinó "el que l'algorisme calcula que et retindrà més".

Un exemple quotidià: si a les xarxes només segueixes comptes que pensen com tu sobre un tema polèmic, l'algorisme et mostrarà cada vegada més contingut similar perquè detecta que hi interactues, fins que et pot semblar que "tothom" pensa igual que tu. Diversificar de manera activa vol dir buscar deliberadament mitjans amb un punt de vista diferent, no esperar que l'algorisme t'ho posi davant sol, perquè per disseny no ho farà.

Deepfakes i imatges generades per intel·ligència artificial

Cada cop és més freqüent trobar-se fotografies, vídeos o àudios fabricats o alterats amb intel·ligència artificial que semblen absolutament reals: una cara que diu paraules que mai ha dit, una imatge d'un esdeveniment que mai ha passat. Alguns indicis poden ajudar a sospitar-ho (mans amb dits de més, textos il·legibles dins la imatge, ombres que no quadren, llavis que no encaixen amb l'àudio), però com que la tecnologia millora molt ràpid, el criteri més fiable no és "mirar-ho amb ulls d'expert" sinó aplicar la lògica de sempre: buscar si el mateix contingut apareix contrastat per una font independent, i fer servir la cerca inversa per veure si ja circulava abans en un altre context, cosa que sol destapar tant fotografies reciclades com muntatges fets amb IA.

Davant d'un vídeo sospitos d'una persona coneguda, l'estratègia més fiable no és quedar-se mirant mans o llavis, sinó comprovar si el mateix contingut ja apareix contrastat per fonts independents o circulava abans en un altre context, mitjançant la cerca inversa: els indicis visuals ajuden a aixecar la sospita, però no són prova concloent perquè els generadors milloren cada mes.

Verificadors de fets

Per a aquests casos existeixen mitjans especialitzats en desmentir bulos i continguts manipulats, com Verificat (a Catalunya) o Maldita.es (a nivell estatal), que analitzen missatges virals, imatges i vídeos i publiquen si són certs, falsos, descontextualitzats o manipulats. Consultar-los davant d'un contingut viral dubtós, especialment si t'arriba per xarxes socials o missatgeria (on circulen molts bulos precisament perquè no hi ha revisió editorial), és un hàbit de verificació que l'examen valora, sobretot abans de compartir alguna cosa que sembla massa impactant per ser certa.

El matís entre "fals" i "descontextualitzat" és important: una imatge pot ser real però correspondre a un fet o un lloc diferent del que s'afirma (per exemple, una fotografia autèntica d'una inundació, però de fa deu anys i en un altre país, que es fa circular com si fos d'ahir mateix). En aquests casos la imatge no és falsa, però l'ús que se n'ha fet sí que enganya.

Per verificar imatges o vídeos, recorda que la cerca inversa (arrossegant la imatge a Google Imatges o fer-hi clic dret i "Cercar imatge amb Google") permet saber si una foto s'ha fet servir abans en un context diferent, un recurs habitual per destapar notícies falses que reciclen imatges antigues, i també per identificar contingut generat o manipulat que es presenta com a real.

Casos pràctics de verificació ràpida



Imagina que reps per WhatsApp un missatge que diu que un determinat aliment "cura" una malaltia greu, citant un "estudi de la universitat". Passos ràpids, en ordre: primer, comprova si el to és alarmista o et demana reenviar-lo "abans que ho censurin" (senyal d'alerta). Segon, busca el nom de l'estudi o de la universitat entre cometes, per veure si existeix realment. Tercer, mira si algun verificador (Verificat, Maldita.es) o un mitjà de salut oficial ja n'ha parlat. Quart, si dubtes, no el reenviïs: la responsabilitat de no difondre desinformació recau també en qui la reenvia, no només en qui la crea.

Dades obertes i com interpretar-les

Una part de la competència en dades que avalua l'ACTIC no és treballar amb fulls de càlcul complexos, sinó saber trobar i llegir correctament dades públiques. Moltes administracions catalanes i estatals publiquen dades obertes (open data): conjunts d'informació pública, actualitzada i reutilitzable per qualsevol persona, sense necessitat de demanar permís. Portals com dadesobertes.gencat.cat o datos.gob.es recullen des de dades de pressupostos municipals fins a estadístiques de trànsit o resultats electorals. Saber que aquests portals existeixen, i que la informació pública oficial no cal buscar-la sempre en un article de premsa sinó que sovint es pot consultar directament a la font, és un dels punts que distingeixen l'usuari mitjà del bàsic.

Portals de dades obertes

A Catalunya, el portal de referència és dadesobertes.gencat.cat, que agrupa conjunts de dades de tots els departaments de la Generalitat: des del pressupost detallat de cada exercici fins a la ubicació dels centres educatius, passant per estadístiques de trànsit, dades mediambientals o indicadors de salut. A escala estatal, el portal equivalent és datos.gob.es, que a més fa de catàleg agregat, amb enllaços a portals de dades obertes d'ajuntaments, diputacions i comunitats autònomes de tot l'Estat. Molts ajuntaments grans (Barcelona, per exemple, amb opendata.bcn.cat) tenen també el seu propi portal municipal amb dades molt més locals, com el cens d'arbrat urbà o els punts de recàrrega elèctrica. Si vols saber quant s'ha gastat el teu ajuntament en enllumenat públic l'últim any, l'opció correcta no és buscar-ho en un article de premsa que en parli de passada, sinó anar directament al portal de transparència o de dades obertes de l'ajuntament i consultar el pressupost executat, que sol estar desglossat per partides.

Formats de dades: CSV i els seus problemes

Aquestes dades solen distribuir-se en formats oberts perquè es puguin reutilitzar amb qualsevol programa, i el més habitual és el CSV (comma-separated values, valors separats per comes): un fitxer de text pla on cada línia és un registre i cada valor va separat per una coma (o, sovint als portals catalans, per un punt i coma, perquè la coma ja s'utilitza com a separador decimal). Un CSV es pot obrir amb un editor de text senzill però normalment es treballa amb un full de càlcul, que el converteix automàticament en columnes i files. La gràcia d'aquest format és que és lleuger, llegible per humans i per màquines, a diferència d'un PDF, que és pensat per llegir-se però no per processar-se automàticament (extreure dades d'una taula en PDF sol donar problemes de format).

Si obres un CSV descarregat d'un portal de dades obertes català i veus que els valors van separats per punt i coma en lloc de coma, no és cap error del fitxer: la coma ja s'utilitza com a separador decimal en la notació catalana i espanyola (1.234,56 euros), de manera que si també fos separador de camps, el programa no distingiria un número decimal d'una separació entre columnes. Per això el CSV "europeu" fa servir el punt i coma com a delimitador.

Pas a pas per obrir correctament un CSV amb el punt i coma com a separador a l'Excel o al Google



Sheets, quan el programa no el reconeix bé i t'ho amunteguen tot en una sola columna:

1. Obre el full de càlcul en blanc (no facis doble clic directament sobre el CSV).
2. A l'Excel: ves a Dades > Des de text/CSV (o Obtenir dades > Des d'un fitxer > Des de text/CSV) i selecciona el fitxer; l'assistent et deixarà triar el delimitador (coma, punt i coma, tabulador).
3. Al Google Sheets: Fitxer > Importa > Puja el fitxer, i a la finestra que apareix tria "Detecta automàticament" o especifica manualment el separador a "Tipus de separador".
4. Revisa la vista prèvia abans de confirmar: si les columnes es veuen correctament separades, ja pots importar-lo.

Si necessites treballar amb una taula de dades que només trobes en format PDF, el problema que et trobaràs més probablement és que extreure-la per processar-la automàticament sol donar problemes de format, ja que el PDF és pensat per llegir-se, no per processar-se: columnes que es fusionen, capçaleres que es dupliquen, números que es parteixen en dues cel·les. Per això, quan una administració publica les mateixes dades en PDF i en CSV, la versió correcta per treballar-hi (filtrar, sumar, ordenar) és sempre el CSV, i el PDF només si el que vols és llegir-lo o imprimir-lo tal qual.

Gràfics enganyosos

Un cop tens les dades, cal saber-les llegir amb esperit crític, i aquí és on entren els gràfics enganyosos. Un dels trucs més habituals és truncar l'eix vertical: si un gràfic de barres no comença a zero sinó, per exemple, a 80, una diferència real petita (de 82 a 86) es representa com una barra el doble d'alta que una altra, exagerant una tendència que en realitat és modesta. Un altre parany freqüent és barrejar percentatges amb valors absoluts sense indicar-ho, o triar un interval temporal esbiaixat (mostrar només els dos mesos on una xifra ha pujat, ignorant els deu anys anteriors on baixava). Davant de qualsevol gràfic, el primer que cal mirar no és la forma de la barra sinó els eixos: què marquen, on comencen, i quina unitat fan servir.

Aquest cas del 82 al 86 amb l'eix començant a 80 és, probablement, el parany gràfic més preguntat a l'examen, perquè és el més fàcil de reconèixer un cop t'hi han fixat l'atenció i el més fàcil de passar per alt si no ho fas. L'altre parany clàssic, mostrar només els dos últims mesos d'una pujada i amagar els deu anys anteriors de baixada constant, funciona per la mateixa lògica: un interval temporal esbiaixat dona una imatge parcial de la tendència real. La lliçó pràctica és sempre la mateixa: quan una xifra o un gràfic et sorprenen, pregunta't "què no m'estan ensenyant", i sovint la resposta és a l'eix o al període triat.

Percentatges, punts percentuals i mitjanes

Interpretar estadístiques bàsiques també implica no confondre conceptes que sonen semblants però no ho són: un percentatge de variació no és el mateix que un punt percentual (passar del 10% al 15% és un augment de 5 punts percentuals, però d'un 50% en termes relatius), i una mitjana pot amagar molta diferència interna (el sou "mitjà" d'una empresa pot estar desvirtuat per un parell de sous molt alts). No cal fer càlculs complexos per a l'examen, però sí detectar quan una xifra es presenta d'una manera que indueix a error, perquè aquest tipus de pregunta ("mira aquest gràfic, què hi falla") és un clàssic del bloc de dades del nivell mitjà.

Confondre "5 punts" amb "5%" és un error tan freqüent en titulars de premsa com en respostes d'examen: val la pena memoritzar l'exemple del 10% al 15% (5 punts percentuals, un 50% en termes relatius) perquè la lògica es transfereixi a qualsevol altra parella de xifres. El mateix passa amb les mitjanes desvirtuades: si el sou "mitjà" d'una empresa és de 2.500 euros però la majoria cobra molt menys i un parell de directius cobren xifres molt altes, l'exemple il·lustra que una mitjana pot amagar molta diferència interna i no reflectir



la situació de la majoria. És exactament el tipus de pensament crític que l'ACTIC vol comprovar amb un exemple numèric senzill, no amb estadística avançada.

Gestió i organització de fitxers

Aquesta part de l'àrea sembla la més "administrativa" però és on es cometen més errors pràctics. Una bona organització de carpetes segueix una lògica que qualsevol altra persona (o tu mateix d'aquí sis mesos) pugui entendre sense preguntar: per projecte, per any, o combinant totes dues (2026_Projecte_Nom). Barrejar criteris sense pensar-hi (unes carpetes per client, d'altres per data, d'altres per tipus de document) és el motiu número u de "no trobo el fitxer". Una estructura eficient sol tenir poques carpetes de primer nivell (les grans categories, estables en el temps) i va afinant en subcarpetes a mesura que cal, en lloc de crear-ne dotzenes de nivell superior que acaben duplicant-se; com a norma pràctica, si per trobar un document necessites obrir més de tres o quatre nivells de carpetes, probablement l'estructura és massa fragmentada i convindria repensar-la.

Estructura de carpetes: com muntar-la des de zero

Si tens una carpeta de projectes on unes subcarpetes estan organitzades per client, unes altres per any i unes altres per tipus de document, barrejades sense cap criteri fix, el problema principal d'aquesta organització és que fa molt difícil trobar la informació perquè no segueix un criteri consistent. La solució no és eliminar cap d'aquests criteris (client, any, tipus), sinó decidir-ne un com a criteri principal (el de primer nivell) i deixar els altres com a subnivells sempre en el mateix ordre. Per exemple:

- Nivell 1 (primer nivell, estable): nom del client o del projecte.
- Nivell 2: any.
- Nivell 3, si cal: tipus de document (Factures, Contractes, Correspondència).

Aplicat de manera consistent, aquest esquema permet que qualsevol document tingui una ubicació previsible: si busques una factura del 2026 d'un client concret, saps que ha d'estar a Client > 2026 > Factures, sense pensar-hi dues vegades. Necessitar obrir més de tres o quatre nivells de subcarpetes per trobar un document és exactament el que caldria evitar, perquè cada nivell addicional multiplica el temps de cerca.

Nomenclatura de fitxers

Els noms dels fitxers també compten com a competència avaluable: evitar espais i accents en documents que es compartiran entre sistemes diferents, fer servir el format AAAA-MM-DD si vols que s'ordenin cronològicament (perquè "2026-01" ordena bé i "1 de gener de 2026" no), i incloure una versió (v1, v2, _final, _revisat) quan un document passa per diverses mans. Un nom de fitxer sistemàtic combina normalment aquests tres elements: data, contingut i versió, en un ordre fix (per exemple 2026-03-12_informe-vendes_v2), de manera que en una llista alfabètica els fitxers relacionats queden agrupats i ordenats sols, sense haver-los de reorganitzar a mà.

Si vols que una sèrie de fitxers d'informes mensuals s'ordenin cronològicament de manera automàtica dins la carpeta, el format de nom que has de fer servir és any-mes-dia (per exemple, 2026-01-informe, 2026-02-informe...), perquè és l'únic ordre numèric que coincideix amb l'ordre alfabètic que fa servir l'explorador de fitxers per defecte. Si en canvi anomenessis els fitxers "Informe gener 2026", "Informe febrer 2026", l'ordenació alfabètica els barrejaria (agost aniria abans que gener, per exemple), i hauries d'ordenar-los manualment cada vegada.

Quan has d'enviar un document a un sistema informàtic extern que sovint dona problemes amb noms de



fitxer "raros", la pràctica més recomanable és evitar espais, accents i caràcters especials en el nom del fitxer. Molts sistemes antics o mal programats interpreten l'espai com un separador de comandes, o no reconeixen bé accents i la ñ, i el resultat és que el fitxer no es puja correctament, es corromp el nom, o directament dona error. La convenció més segura és fer servir guionets o guions baixos en lloc d'espais (informe_vendes en lloc d'"informe vendas") i evitar lletres accentuades encara que el text del document sí que en tingui.

Quan un document passa per diverses persones que hi van fent canvis abans de la versió definitiva, la pràctica de nomenclatura que evita confusions és afegir un indicador de versió al nom del fitxer (v1, v2, _final). Sense aquest indicador, és fàcil acabar amb diverses còpies obertes alhora sense saber quina és la més recent, un error que es multiplica quan el document es comparteix per correu en lloc de treballar-hi sobre un únic fitxer al núvol amb historial de versions (que veurem més endavant en aquest mateix capítol).

Cerca avançada de fitxers a l'explorador

Quan la carpeta creix i els noms ja no basten per trobar res a ull, entra en joc la cerca avançada de fitxers, disponible tant a l'explorador de Windows com al Finder de Mac o als gestors de fitxers de mòbil. Més enllà d'escriure un nom aproximat al quadre de cerca, es pot filtrar per tipus de fitxer (només mostrar .docx o .jpg), per data de modificació o creació (fitxers editats la darrera setmana), per mida, o fins i tot cercar per contingut text dins de documents, ja que l'explorador indexa el text de molts formats i troba fitxers que contenen una paraula concreta encara que el nom del fitxer no la mencioni. Estalvia haver de recordar exactament on vas guardar alguna cosa, sobretot quan es col·labora amb altres persones que no segueixen la mateixa lògica de noms que tu.

Pas a pas per fer una cerca avançada a l'Explorador de fitxers de Windows:

1. Obre l'Explorador de fitxers i ves a la carpeta (o a "Aquest equip" si vols cercar-ho tot) on vols buscar.
2. Fes clic al quadre de cerca de la cantonada superior dreta i escriu una part del nom o del contingut.
3. A la barra superior apareixerà una pestanya "Cerca" (o "Eines de cerca"); fes-hi clic per veure filtres com "Tipus", "Mida" i "Data de modificació".
4. Selecciona el filtre que et convingui (per exemple, Tipus > Document de Word, o Data de modificació > La setmana passada) i la llista es refina automàticament.

Pas a pas equivalent al Finder de Mac:

1. Obre el Finder i prem Cmd+F, o fes clic a la lupa de la cantonada superior dreta.
2. Escriu el terme de cerca; per defecte, el Finder busca en "Aquest Mac".
3. Fes clic al signe "+" que apareix sota la barra de cerca per afegir criteris: tipus d'element, data de creació, data d'última obertura, mida, i molts més.
4. Combina tants criteris com necessitis; els resultats es filtren en temps real.

Recordes que un document conté una paraula concreta, però no recordes el nom del fitxer ni on el vas guardar: la funció de l'explorador de fitxers que et permet trobar-lo igualment és la cerca avançada per contingut de text, que indexa el text dins de molts formats de document. Tant Windows com Mac indexen en segon pla el contingut de documents de text, PDFs i fulls de càlcul, de manera que una cerca per una paraula concreta pot trobar un fitxer encara que aquella paraula no aparegui al nom.

Compressió i format ZIP

Quan cal enviar diversos fitxers junts, o un de sol molt pesant, comprimir-los en un únic arxiu .zip té dos avantatges: redueix la mida (sobretot en documents de text o fulls de càlcul, menys en fotos o vídeos que



ja van comprimits) i els empaqueta en un sol fitxer que es pot adjuntar o enviar sense haver-ne d'enviar quinze per separat. Crear un ZIP no requereix cap programa extra en els sistemes actuals: n'hi ha prou de seleccionar els fitxers, clic dret i "Comprimir" (o "Enviar a > Carpeta comprimida" a Windows), i per obrir-lo, doble clic el descomprimeix als fitxers originals. És una operació senzilla que apareix sovint en preguntes de situació pràctica ("has d'enviar quinze fitxers per correu, quina és la manera més eficient"), perquè combina gestió d'arxius amb sentit pràctic d'ús quotidià.

Pas a pas per comprimir diversos fitxers a Windows:

1. Selecciona tots els fitxers que vols agrupar (clic sobre el primer, Maig premut sobre l'últim si són consecutius, o Ctrl premut mentre fas clic per triar-los un a un).
2. Fes clic dret sobre la selecció.
3. Tria "Enviar a > Carpeta comprimida (en zip)" (o directament "Comprimir a ZIP" en versions més recents de Windows).
4. Es crearà un fitxer .zip a la mateixa carpeta, amb el nom del primer fitxer seleccionat per defecte; pots renombrar-lo abans d'enviar-lo.

Pas a pas a Mac:

1. Selecciona els fitxers al Finder.
2. Fes clic dret i tria "Comprimeix X elements".
3. Es genera un fitxer "Archive.zip" a la mateixa carpeta, que pots renombrar.

Has d'enviar per correu una carpeta amb quinze fitxers diferents relacionats amb un mateix projecte: la manera més pràctica de fer-ho és comprimir-los en un únic fitxer .zip, en lloc d'adjuntar-los un per un (a banda de ser més ràpid, molts gestors de correu limiten el nombre d'adjunts o la mida total, i un ZIP sol quedar per sota d'aquest límit encara que els fitxers originals junts no hi cabrien).

Tipus i formats de fitxer

Cal saber diferenciar formats segons per a què serveix el document: un PDF és ideal per compartir un document que no s'ha de modificar (manté el format en qualsevol dispositiu); un .docx o .odt quan s'espera que l'altra persona hi editi; un .csv per a dades tabulars que s'han d'importar a un altre programa; un .zip quan cal enviar diversos fitxers junts o reduir-ne la mida. Els formats d'imatge també tenen un ús diferenciat: JPG per a fotografies (comprimeix bé, perd una mica de qualitat), PNG quan cal transparència o text nítid (captures de pantalla, logotips), i formats com l'SVG per a gràfics vectorials que s'han d'escalar sense perdre qualitat.

Si has de compartir un document perquè es visualitzi exactament igual en qualsevol dispositiu, sense que ningú el pugui modificar per error, tria .pdf: "congela" el format de manera que es vegi igual independentment del programa o del dispositiu que l'obri, a diferència d'un .docx, que pot desquadrar-se amb una versió diferent del programa o un tipus de lletra que no té instal·lat. Si el que vols exportar és una llista de dades tabulars (noms, imports, dates) perquè s'importin en un altre programa de gestió, el format adequat és .csv, per la mateixa raó vista a l'apartat de dades obertes: és lleuger, no depèn de cap programa concret i qualsevol full de càlcul el pot llegir sense conversions.

Pel que fa a imatges: per una captura de pantalla amb text nítid i transparència de fons, el PNG encaixa millor perquè, a diferència del JPG, no aplica compressió amb pèrdua sobre les vores del text (que quedarien borroses) i admet capes transparents; per a una fotografia normal, el JPG sol ser preferible perquè ocupa molt menys espai amb una pèrdua de qualitat imperceptible a ull nu. I per a un logotip que s'hagi de poder ampliar molt (un cartell gran) sense perdre gens de qualitat, l'SVG és l'opció correcta: és



un format vectorial, definit per fórmules matemàtiques i no per píxels, de manera que es veu igual de nítid en una targeta de visita que en una lona de tres metres, cosa que no passa mai amb un JPG o un PNG ampliats més enllà de la seva mida original (es "pixelen").

Propietats i metadades

Cada fitxer, a banda del seu contingut, guarda un conjunt de propietats visibles des de l'explorador sense necessitat d'obrir-lo: mida, data de creació, data de darrera modificació, i sovint també l'autor o el programa amb què es va crear. Es poden consultar fent clic dret sobre el fitxer i triant "Propietats" (Windows) o "Obtenir informació" (Mac), i són la base de moltes cerques avançades: ordenar una carpeta per data de modificació, per exemple, permet trobar de seguida el darrer document en què s'ha treballat sense recordar-ne el nom.

Més enllà de les propietats bàsiques, les metadades són informació encara més detallada "amagada" dins del fitxer, que no es veu directament quan l'obres però hi queda registrada: en un document de text poden incloure l'autor original i el temps total d'edició; en una fotografia feta amb mòbil, sovint la ubicació GPS exacta on es va prendre. Són rellevants per dos motius: primer, perquè permeten cercar documents sense obrir-los un per un; segon, perquè són un risc de privadesa, ja que abans de penjar una foto a internet convé saber que pot revelar on es va fer, motiu pel qual moltes xarxes socials eliminen aquesta informació automàticament (però no tots els mitjans de compartir ho fan). Per revisar (i si cal esborrar) aquestes metadades abans de compartir una imatge des del mòbil:

1. A Android, en obrir la foto a la galeria, sol haver-hi una opció "Detalls" o una icona d'informació (i) que mostra la ubicació i altres dades tècniques; algunes aplicacions de missatgeria (com WhatsApp) ja eliminen aquestes dades automàticament en enviar la imatge per xat, però no ho fan totes ni sempre.
2. A iPhone, dins l'aplicació Fotos, en compartir una imatge apareix l'opció "Opcions" a la part superior de la pantalla d'enviament, amb un interruptor per a "Ubicació"; desactivant-lo, la foto es comparteix sense les coordenades GPS.
3. Al PC o Mac, a les propietats avançades d'una imatge (pestanya "Detalls" a Windows, "Informació general" i "Més informació" a la vista prèvia del Mac) sol haver-hi una opció per eliminar propietats i informació personal abans d'enviar el fitxer.

Emmagatzematge local i al núvol

Guardar un fitxer "al disc dur" i guardar-lo "al núvol" no és el mateix, i l'examen sol posar situacions on cal triar l'opció adequada. L'emmagatzematge local (el disc de l'ordinador, un pendrive, un disc extern) és ràpid i no depèn de tenir connexió, però si es perd o s'espatlla el dispositiu, es perd la informació si no hi ha còpia. L'emmagatzematge al núvol (Google Drive, Dropbox, OneDrive, o alternatives com Nextcloud, que moltes administracions catalanes fan servir per tenir el control de les dades en servidors propis) permet accedir als fitxers des de qualsevol dispositiu i compartir-los fàcilment, però requereix connexió i implica confiar les dades a un tercer.

L'avantatge clar del núvol enfront del disc dur local és precisament aquest: es pot accedir des de qualsevol dispositiu i compartir-lo fàcilment, cosa que un disc local, per definició, no pot oferir (cal ser físicament davant d'aquell ordinador o portar-lo a sobre).

Sincronització versus còpia de seguretat

La sincronització és el mecanisme que manté actualitzada la còpia local i la del núvol alhora: quan modifiques un document al portàtil, el canvi puja automàticament i queda disponible al mòbil o a un altre



ordinador. Cal distingir sincronitzar de fer una còpia de seguretat: la sincronització reflecteix els canvis a totes bandes, inclosos els esborrats (si elimines un fitxer sincronitzat, desapareix a tot arreu), mentre que una còpia de seguretat (backup) és una fotografia congelada d'un moment concret, pensada precisament per recuperar informació si s'esborra per error o s'infecta amb un virus.

Si esborres per error un fitxer d'una carpeta sincronitzada amb el núvol (per exemple Google Drive), el fitxer també desapareixerà al núvol, perquè la sincronització reflecteix els esborrats a totes bandes. Aquest és, probablement, el malentès més comú i perillós sobre el núvol: molta gent pensa "com que és al núvol, sempre hi és", quan en realitat és un mirall en temps real del que tens local, no una còpia de seguretat independent. L'única via per recuperar-lo és la paperera del propi servei (amb un termini limitat, típicament 30 dies) o l'historial de versions, que veurem tot seguit.

Compartir amb permisos

Un dels usos més habituals del núvol és compartir un document sense haver-lo d'enviar per correu com a adjunt, i aquí l'ACTIC espera que sàpigues que compartir no és una acció única sinó que admet nivells de permís diferents. El més comú és triar entre "només lectura" (la persona pot veure el document, i com a molt descarregar-se'n una còpia, però no alterar l'original) i "edició" (pot modificar-lo directament, amb els canvis visibles per a tothom que hi tingui accés). Hi ha també nivells intermedis, com "comentari", que permeten afegir-hi anotacions sense tocar el text original. Tria el permís equivocat és un error freqüent a la feina real (compartir en edició un document que només s'havia de consultar, i que algú acaba modificant sense voler), i per això apareix com a pregunta de situació: si vols que diverses persones opinin sobre un esborrany sense arriscar-te que algú l'esborri per error, el permís adequat no és "edició" sinó, com a molt, "comentari" o "lectura".

Pas a pas per compartir un document de Google Drive amb un permís concret:

1. Obre el document a Google Drive, o fes clic dret sobre el fitxer a la llista.
2. Selecciona "Compartir" (o la icona d'una persona amb un "+").
3. Escriu l'adreça de correu de la persona a qui vols donar accés.
4. Al desplegable que apareix al costat (per defecte sol dir "Editor"), tria el nivell adequat: "Lector" (només lectura), "Comentarista" (pot afegir comentaris però no editar el text) o "Editor" (pot modificar-lo directament).
5. Fes clic a "Enviar" o "Fet".

Si vols que diversos companys opinin sobre un informe abans de tancar-lo, el permís de "Comentari" és el que evita el risc: amb edició, algú pot esborrar sense voler un paràgraf sencer; amb comentari, poden marcar suggeriments (Google Docs té, a més, una funció de "suggeriments" que és una variant encara més controlada, visible com a proposta de canvi) sense tocar mai el text original.

Historial de versions

Un altre avantatge del núvol davant del disc local és que la majoria de serveis (Google Drive, OneDrive, Dropbox) guarden un historial de versions anteriors d'un document cada cop que es desa: si algú esborra per error un paràgraf sencer, o es vol recuperar com estava el document fa tres dies, es pot obrir l'historial i restaurar una versió anterior sense haver-ho previst amb una còpia manual. No substitueix una còpia de seguretat completa (l'historial sol tenir un límit de temps o de versions), però converteix el núvol en una xarxa de seguretat afegida per als errors del dia a dia.

Algú esborra per error un paràgraf sencer d'un document compartit a Google Drive fa tres dies: la funció que permet recuperar-lo sense haver previst una còpia manual és l'historial de versions del document. Pas



a pas per consultar-lo a Google Docs:

1. Amb el document obert, ves a Fitxer > Historial de versions > Mostra l'historial de versions (o l'accés directe des de la icona del rellotge, si és visible a la barra d'eines).
2. Al lateral apareix una llista de versions anteriors, agrupades per data i hora, i sovint amb el nom de qui hi va fer canvis.
3. Fes clic sobre una versió anterior per previsualitzar-la.
4. Si és la que vols recuperar, fes clic a "Restaura aquesta versió" a la part superior.

Espai disponible i treball sense connexió

Els comptes gratuïts dels serveis al núvol tenen un espai limitat (per exemple, 15 GB compartits entre correu, fotos i documents en el cas de Google), i quan s'exhaureix cal ampliar-lo de pagament o alliberar espai esborrant fitxers pesants. Val la pena saber consultar quant espai queda disponible abans que un error de "no hi ha espai" interrompi una pujada important.

Un compte gratuït de Google (Gmail, Fotos i Drive) té un espai d'emmagatzematge limitat i compartit entre tots aquests serveis, i aquest espai sol ser de 15 GB, una xifra que val la pena recordar perquè apareix literalment en algunes preguntes d'examen. Entendre que és un espai compartit (no 15 GB només per al Drive) ajuda a entendre per què de vegades el compte "es queda sense espai" encara que la carpeta de documents sembli petita: sovint el culpable és el correu amb adjunts acumulats durant anys, o les fotos i vídeos del mòbil.

Per consultar l'espai disponible a un compte de Google:

1. Ves a Google Drive, One.google.com, o directament a la icona d'engrenatge dins de Drive.
2. Al menú lateral esquerre de Drive, a la part de baix, sol aparèixer una barra amb l'espai utilitzat sobre el total (per exemple, "8,2 GB de 15 GB utilitzats").
3. Fent-hi clic accedeixes a un desglossament per servei (Gmail, Drive, Fotos), útil per identificar què ocupa més espai abans de decidir què esborrar.

Pel que fa a la connexió, la majoria d'eines al núvol permeten marcar carpetes o fitxers concrets per fer-los disponibles sense connexió: es descarreguen localment, es poden consultar i editar encara que no hi hagi internet, i els canvis es tornen a sincronitzar sols quan es recupera la connexió. Aquesta funció és clau per a qui treballa sovint fora de cobertura, i un altre dels punts on l'examen distingeix qui coneix el núvol només com "on hi ha els meus fitxers" de qui en sap treure profit real. A Google Drive, per exemple, es marca fent clic dret sobre un fitxer o carpeta i triant "Disponible fora de línia"; a OneDrive i Dropbox, l'opció equivalent sol dir "Fer disponible sense connexió" o "Mantenir sempre en aquest dispositiu".

La regla 3-2-1

La regla pràctica que es fa servir a l'àmbit professional per a les còpies de seguretat és la 3-2-1: com a mínim tres còpies de la informació important, en dos suports diferents (per exemple disc dur i núvol), i una d'aquestes fora del lloc físic habitual (per si hi ha un robatori o un incendi a l'oficina). No cal memoritzar-ho com a fórmula matemàtica per a l'examen, però sí entendre la lògica: no n'hi ha prou amb un sol lloc, encara que sigui "al núvol", perquè un compte bloquejat o un error de sincronització també pot fer perdre dades.

Segons la pràctica habitual de còpies de seguretat coneguda com a regla 3-2-1, la informació important s'hauria d'organitzar en almenys tres còpies, en dos suports diferents, amb una d'elles fora del lloc físic habitual: per exemple, el document original al portàtil (còpia 1, local), una còpia sincronitzada al núvol (còpia 2, suport diferent i ja fora del lloc per definició), i una tercera en un disc extern guardat a casa d'un



familiar o a la feina (còpia 3). Si hi ha un incendi o robatori a casa, sobreviuen les còpies 2 i 3; si el compte del núvol falla, sobreviuen l'1 i la 3.

A escala personal, aquesta idea es tradueix sovint en un gest molt senzill: activar la còpia de seguretat automàtica del mòbil (fotos i vídeos que es pugen soles a Google Fotos, iCloud o similar en connectar-se a wifi), de manera que perdre o trencar el telèfon no signifiqui perdre anys de fotografies. És l'aplicació més quotidiana de la regla 3-2-1 i, per això mateix, un dels exemples que l'examen fa servir per comprovar si entens el concepte més enllà de la teoria. Per activar-ho a un mòbil Android: obre l'aplicació Google Fotos, ves al teu perfil (la icona de la cantonada superior dreta), tria "Configuració de Google Fotos" i activa "Còpia de seguretat"; a iPhone, ves a Configuració, toca el teu nom, entra a iCloud i activa "Fotos".

Consells per a la prova

Les preguntes d'aquesta àrea acostumen a plantejar-se com a situació pràctica ("vols trobar X, quina cerca fas") més que com a teoria pura, així que val la pena practicar operadors de cerca reals abans de l'examen, no només llegir-los. Fixa't també en les preguntes que combinen dos conceptes (avaluar la fiabilitat d'un resultat trobat amb un operador concret), perquè és el tipus d'ítem que l'ACTIC fa servir per diferenciar el nivell mitjà del bàsic. Repassa bé la diferència entre sincronització i còpia de seguretat, entre compartir amb permís de lectura o d'edició, i entre un percentatge i un punt percentual: són els tres punts on més gent falla perquè assumeix que "ja ho sap" sense haver-hi parat mai atenció de manera explícita. I si una pregunta et mostra un gràfic o una xifra "sorprenent", desconfia per sistema: mira primer els eixos i la font abans de valorar si la conclusió que suggereix és la que diuen realment les dades.

Un altre patró molt habitual és la pregunta que et dona un domini concret (site:girona.cat, per exemple) i et demana quina cerca faries per trobar informació publicada només al web d'aquell ajuntament: la resposta correcta combina sempre paraules clau amb l'operador site:, mai una sola cosa. Practica muntar aquest tipus de cerca de memòria (tràmit o paraula clau + site:domini.cat) fins que et surti automàtic, perquè és el patró de pregunta que més es repeteix en aquest bloc.

Finalment, no et quedis només amb la teoria dels formats de fitxer (PDF, DOCX, CSV, ZIP, JPG, PNG, SVG): l'examen sol formular-ho com un cas d'ús ("necessites enviar X perquè es vegi igual a tot arreu", "necessites que t'editin un document", "necessites un logotip que s'ampliï molt"), no com una pregunta directa "què és un PDF". Repassa cada format associant-lo a la situació on és la millor opció, no a la seva definició tècnica, perquè així és exactament com et preguntaran per ell el dia de l'examen.

**2****TEMA****Àrea 2. Comunicació i col·laboració****Què avalua aquesta àrea**

L'Àrea 2 del nivell mitjà d'ACTIC no busca que sàpigues on és cada botó de Gmail o de Meet, sinó que entenguis com comunicar-te de manera correcta i segura amb eines digitals, com compartir informació sense posar en risc dades ni intimitat de ningú, i com relacionar-te amb l'administració pública per via electrònica. El nivell mitjà pressuposa que ja domines l'ús bàsic d'aquestes eines i afegeix un pas més: saber configurar-les amb criteri (una resposta automàtica, un filtre de correu, la privadesa d'un perfil) i triar en cada situació el canal i el format adequats. A l'examen hi trobaràs tant preguntes de conceptes (què és Cl@ve, per a què serveix el CCO, què és una regla de correu) com preguntes de criteri: què faries en una situació concreta.

Val la pena tenir present, abans d'entrar en matèria, que aquesta àrea barreja dos mons que a la pràctica van sempre junts: les eines de comunicació i col·laboració que fem servir cada dia a la feina o a casa (correu, xat, videotrucada, documents compartits, calendari) i la relació digital amb l'administració pública, que a Catalunya i a l'Estat ja és, per a molts tràmits, l'única via disponible o com a mínim la preferent. Un bon truc per estudiar aquest bloc és no memoritzar definicions soltes sinó imaginar-te fent realment cadascuna de les tasques que es descriuen: convocar una reunió de veïns, revisar un document d'un company, demanar cita al metge de capçalera. Si t'imagines el procediment pas a pas, la resposta correcta sol sortir sola.

El correu electrònic amb ofici

El correu electrònic continua sent el canal formal per excel·lència, i el nivell mitjà espera que en treguis més partit que un simple enviar i rebre. No n'hi ha prou amb saber redactar un missatge: cal conèixer les funcions que el converteixen en una eina de treball eficient i respectuosa amb la privadesa d'altri, i saber-les activar quan convé.

CC i CCO: la diferència que més es pregunta

Convé dominar la diferència entre **CC** (amb còpia, visible per a tothom) i **CCO** (còpia oculta, els destinataris no es veuen entre ells): quan escris a un grup de persones que no es coneixen entre si, per exemple convocant una reunió veïnal o enviant una circular a famílies, el CCO evita exposar adreces de correu alienes, que és una dada personal. Un assumpte clar i concret, evitar adjunts innecessàriament pesats i revisar els destinataris abans d'enviar (el clàssic "respondre a tots" per error) són bones pràctiques que l'examen sol preguntar en forma de cas pràctic.

Pensa en un exemple molt real: ets la persona delegada de classe d'una escola i has de convocar 40 famílies a una reunió de final de trimestre. Si poses les 40 adreces al camp "Per a" o al camp "CC", totes les famílies rebran un correu on hi apareixen els correus electrònics de la resta, cosa que no toca a ningú de decidir per elles: potser algunes no volen que la seva adreça circuli entre desconeguts. La solució correcta és posar la teva pròpia adreça (o l'adreça de l'escola) al camp "Per a" i totes les 40 adreces de les famílies al camp "CCO". Així cada família rep el correu com si l'haguessis enviat només a ella, sense veure qui més l'ha rebut.



El procediment pràctic a Gmail és senzill:

1. Prem "Redacta" per obrir un correu nou.
2. Al costat del camp "Per a" hi ha l'opció "CCO"; clica-hi per fer-lo visible.
3. Escriu-hi (o enganxa-hi) totes les adreces separades per comes.
4. Deixa el camp "Per a" amb la teva pròpia adreça o una adreça genèrica.
5. Redacta el missatge i envia'l amb normalitat.

A Outlook el procediment és equivalent: en un missatge nou, la pestanya "Opcions" té el botó "CC i CCO" per mostrar aquests camps si no hi surten per defecte.

Un error habitual que cal evitar és l'invers: fer servir CC quan en realitat calia CCO, o al contrari, ocultar amb CCO un destinatari que en realitat hauria de ser visible perquè tothom sàpiga qui més ha rebut el missatge (per exemple, quan es respon formalment a un grup de treball on tothom ja es coneix i té sentit que es vegin entre ells). El criteri és sempre el mateix: CCO quan els destinataris no es coneixen entre si o quan protegir la seva adreça és rellevant; CC quan té sentit que tothom sàpiga qui rep còpia del missatge.

Signatura de correu i resposta automàtica

La signatura de correu és aquell bloc de text (nom, càrrec, telèfon, potser un logotip) que s'afegeix automàticament al final de cada missatge nou; un cop configurada, estalvia haver de repetir les dades de contacte en cada enviament i dona un aire més professional a la correspondència. Per configurar-la a Gmail cal anar a la icona d'engrenatge de dalt a la dreta, triar "Veure tota la configuració", quedar-se a la pestanya "General" i baixar fins a l'apartat "Signatura": des d'allà es pot crear una signatura nova, escriure-hi el text i el format (negreta, mida, un logo si cal) i triar si s'ha d'afegir als correus nous, a les respostes, o a totes dues coses. A Outlook el camí és similar: "Arxiu" > "Opcions" > "Correu" > botó "Signatures".

Molt relacionada hi ha la resposta automàtica d'absència (el clàssic "estic fora de l'oficina fins al dia..."): es configura des dels ajustos del correu, s'activa i es desactiva sola entre les dates que indiquis, i informa qui t'escriu que trigarà a respondre, sovint amb un contacte alternatiu. És una eina de cortesia professional que l'examen pot preguntar en forma de cas: si te'n vas de vacances i vols que qui t'escrigui ho sàpiga sense haver-li de respondre un per un, la resposta automàtica és la solució.

Imagina't la situació concreta: te'n vas de vacances dues setmanes i no vols contestar cada correu un per un ni deixar la gent sense resposta durant quinze dies. A Gmail, el camí és: engranatge > "Veure tota la configuració" > pestanya "General" > apartat "Resposta automàtica d'absència"; s'activa el commutador, s'omplen les dates d'inici i final, un assumpte ("Fora de l'oficina") i el text del missatge (per exemple, indicant que tornaràs el dia tal i, si és urgent, a qui es pot escriure mentrestant). Un cop passada la data final, Gmail la desactiva sol, sense que hakis de recordar-ho. A Outlook l'opció equivalent es diu "Respostes automàtiques" i es troba a "Arxiu" > "Informació".

Regles i filtres, etiquetes i carpetes

Les regles i filtres de correu permeten automatitzar què passa amb els missatges entrants segons condicions que defineixes tu: per exemple, que tot el que arribi d'un remitent concret es marqui com a llegit, s'arxivi directament en una carpeta o s'etiqueti amb un color determinat, sense que hakis de fer-ho manualment cada vegada. A Gmail es creen des de la icona de "Cerca avançada" (la fletxa cap avall dins el cercador de dalt) o des de "Configuració" > "Filtres i adreces bloquejades" > "Crea un filtre nou": s'hi indica la condició (remitent, assumpte, paraules concretes) i, en un segon pas, l'acció que cal fer-hi (arxivar, etiquetar, marcar com a llegit, suprimir, o fins i tot reenviar-lo a una altra adreça). A Outlook



l'equivalent són les "Regles", dins "Configuració" > "Correu" > "Regles", amb un funcionament molt semblant: es defineix la condició i l'acció associada.

Això es combina amb les etiquetes i carpetes, que serveixen per organitzar la safata d'entrada per temes o projectes en lloc de deixar-ho tot barrejat en un únic llistat cronològic; un mateix missatge pot tenir diverses etiquetes alhora, cosa que no passa amb les carpetes tradicionals, on un correu només pot estar en un lloc. Per exemple, un correu que parla d'una factura d'un projecte concret es pot etiquetar alhora com "Factures" i com "Projecte Nord", i aparèixer als dos llistats sense haver-lo duplicat; en canvi, si l'organitzessis amb carpetes tradicionals, hauries de triar en quina de les dues el desis. A Gmail les etiquetes es creen des del menú lateral esquerre, a l'opció "Crea etiqueta nova"; a Outlook, que treballa amb carpetes, es crea una carpeta nova amb el botó dret sobre la safata d'entrada i "Carpeta nova".

Un truc que sovint apareix a l'examen: si el que necessites és que un mateix missatge pugui aparèixer classificat sota diversos criteris alhora, la resposta correcta sol ser "etiquetes", no "carpetes".

Trobar un correu antic: el cercador intern

Quan la bústia acumula anys de missatges, el cercador intern del correu permet trobar un missatge concret filtrant per remitent, per paraules del text o de l'assumpte, per data o per si té adjunts, i és molt més eficient que baixar amunt i avall repassant missatges un per un. Posem el cas d'algú que ha de trobar un correu de fa dos anys del qual només recorda que portava un fitxer adjunt i que parlava d'un pressupost: en lloc d'anar desplaçant-se manualment per centenars de missatges antics, cal obrir el cercador i fer servir els operadors de cerca avançada. A Gmail, clicant la fletxa cap avall del cercador s'obre un formulari amb camps per "De", "Assumpte", "Conté les paraules" i una casella "Té adjunt"; combinant "pressupost" al camp de text amb la casella d'adjunts marcada, el resultat es redueix a molt pocs missatges. També es pot escriure directament a la barra de cerca amb operadors com "from:", "subject:" o "has:attachment" seguits del terme desitjat.

Adjunts grans i enviament programat

Per als adjunts grans, hi ha un límit tècnic (habitualment al voltant dels 25 MB) a partir del qual el correu no els deixa enviar directament. La solució pràctica és pujar el fitxer a un servei al núvol (Google Drive, WeTransfer, OneDrive) i enviar per correu només l'enllaç de descàrrega, en lloc de l'arxiu en si; així el destinatari el descarrega quan vulgui i tu no satures ni la teva bústia ni la seva. Un exemple habitual: vols enviar a un company un vídeo de 300 MB d'una presentació gravada. El correu et donarà error o directament no et deixarà adjuntar el fitxer perquè supera el límit; el que has de fer és pujar el vídeo a Google Drive (arrossegant-lo a la carpeta corresponent o amb el botó "Nou" > "Puja un fitxer"), un cop pujat fer-hi clic amb el botó dret i triar "Obtenir enllaç", i finalment enganxar aquest enllaç dins del cos del correu en lloc d'intentar adjuntar el vídeo directament.

Programar l'enviament d'un correu perquè surti en un moment determinat (per exemple, redactar-lo un diumenge a la nit però que arribi dilluns a primera hora) és una altra funció habitual que evita enviar missatges de feina fora d'horari, un detall de cortesia professional que també entra dins la netiqueta. A Gmail, en lloc de prémer el botó "Enviar" cal clicar la fletxa petita que hi ha al costat (una fletxa cap avall) i triar "Programa l'enviament"; apareix un desplegable amb opcions habituals (demà a primera hora, dilluns a primera hora) o l'opció de triar data i hora exactes. A Outlook l'equivalent es fa des de "Opcions" > "Retard en el lliurament", indicant la data i l'hora en què s'ha d'enviar.

Llistes de distribució

Finalment, les llistes de distribució (una única adreça que reenvia el missatge a tots els membres d'un



grup, com podria ser "claustre@escola.cat") permeten escriure una sola vegada a un col·lectiu sencer sense haver d'afegir cada adreça manualment, i solen ser gestionades per un administrador que hi dona d'alta o de baixa les persones. Aquesta és precisament la diferència amb un simple "grup de contactes" personal: la llista de distribució té una sola adreça pública que qualsevol pot fer servir per escriure a tot el col·lectiu, mentre que una llista de contactes és una comoditat privada de qui l'ha creada, per no haver de teclejar cada adreça cada vegada.

Recorda per a l'examen: si la pregunta parla d'una adreça del tipus "algú@organització.cat" a la qual escriu qualsevol persona i que reparteix automàticament el missatge entre un col·lectiu gestionat per un administrador, la resposta és "llista de distribució".

Missatgeria instantània i videotrucades amb criteri

La missatgeria instantània (WhatsApp, Telegram, o eines corporatives com Teams o Slack) ha guanyat terreny al correu per a comunicacions ràpides, però no serveix igual per a tot: un contracte, una queixa formal o una notificació amb valor administratiu s'han de fer per correu o pel canal oficial corresponent, no per WhatsApp. Aquesta és una de les distincions de criteri que més agrada a l'examen: el fet que una eina sigui còmoda i ràpida no vol dir que sigui l'adequada per a qualsevol contingut. Un missatge de WhatsApp no deixa el mateix rastre formal ni la mateixa validesa que un correu institucional; per això, per exemple, una reclamació formal a una empresa, un avís de baixa laboral o la confirmació d'un acord de feina s'han de fer sempre pel canal formal (correu, seu electrònica, registre), reservant el xat per a allò informal i urgent del dia a dia.

Videoconferència: funcions que el nivell mitjà exigeix conèixer

La videoconferència (Meet, Zoom, Teams) té les seves pròpies normes, i el nivell mitjà espera que en coneguis les funcions amb una mica més de detall que el simple "entrar a la reunió".

Silenciar el micròfon. Silenciar el micròfon quan no es parla és l'etiqueta bàsica de qualsevol reunió amb diverses persones, perquè el soroll de fons d'un micròfon obert (una porta, un tecleig, una conversa de fons) molesta i interromp qui parla. A Google Meet la icona del micròfon és a la barra inferior de controls, al centre de la pantalla; a Zoom és també a la barra inferior, a l'esquerra; en tots dos casos un sol clic el silencia i un altre el torna a activar, i sol acompanyar-se d'una drecera de teclat (per exemple, la barra espaiadora mantinguda premuda a Zoom permet parlar momentàniament sense desactivar el silenci).

Compartir pantalla. Compartir pantalla serveix per mostrar a la resta un document, una presentació o qualsevol finestra del teu ordinador tal com la veus tu, cosa molt útil per explicar un procediment o revisar un text conjuntament sense haver-lo d'enviar abans. El procediment habitual és: prémer el botó "Presentar ara" (Meet) o "Compartir pantalla" (Zoom, Teams) a la barra inferior, triar si es vol compartir tota la pantalla, una finestra concreta (per exemple, només el document de Word obert) o una pestanya del navegador, i confirmar. Quan s'acaba, es prem "Deixa de presentar" o "Atura la compartició" per tornar a la vista normal de la reunió. Un cas pràctic típic d'examen: durant una videotrucada de feina, vols que la resta vegi un document que tens obert al teu ordinador tal com el veus tu, sense enviar-lo abans; la resposta és "compartir pantalla".

Fons difuminat o virtual. El fons difuminat (o un fons virtual) emborriona o substitueix l'entorn real que hi ha darrere teu, útil per mantenir una imatge professional o simplement per privacitat quan es truca des de casa. A Meet s'activa des dels tres punts o des de la icona d'"Aplica efectes visuals" abans o durant la trucada; a Zoom, des de la fletxa al costat de la icona de la càmera es tria "Fons virtual". És una funció



merament estètica i de privacitat, no de seguretat de la trucada.

Sala d'espera. La sala d'espera reté els participants abans que l'amfitrió els doni pas a la reunió, cosa que serveix per controlar qui hi entra i evitar interrupcions no desitjades, especialment en reunions amb persones externes a l'organització. Es configura des de les opcions de seguretat de la reunió (a Zoom, dins el menú "Seguretat" durant la trucada, o en configurar-la prèviament; a Meet, l'amfitrió pot activar l'opció que cal la seva aprovació perquè algú entri). El cas pràctic típic: organitzes una videotrucada amb persones externes a l'organització i vols controlar qui hi entra abans que comenci la reunió; la resposta és la sala d'espera.

Xat de la reunió. El xat de la reunió permet escriure missatges, enllaços o preguntes sense interrompre qui parla, i sovint queda disponible per repassar-lo després que la trucada hagi acabat. Si durant una videotrucada vols compartir un enllaç amb la resta sense tallar qui està parlant, la funció que has de fer servir és el xat, no aixecar-te a parlar per damunt de ningú.

Gravar la reunió. Gravar una reunió és una funció habitual per a qui no hi pot assistir o per deixar constància d'allò acordat, però comporta una obligació clara: cal avisar prèviament els participants que la sessió es gravarà i, en molts contextos, demanar-ne el consentiment explícit abans de començar, ja que la gravació inclou la imatge i la veu de persones identificables. Comprovar càmera i so abans que comenci la reunió també forma part de la bona pràctica, per no fer perdre temps a la resta resolent problemes tècnics en directe. Recorda-ho com una parella indestriable: gravar sí, però sempre avisant abans; comprovar el so i la càmera abans, no durant.

Un error habitual que cal evitar a l'examen és confondre "silenciar el micròfon" amb "tallar la càmera": són dues accions independents, i silenciar el so no impedeix que et vegin, ni desconnectar la càmera impedeix que se senti el que dius.

Compartir fitxers i recursos

Quan un fitxer és petit, adjuntar-lo al correu és senzill, però per a fitxers grans (vídeos, carpetes senceres) el més pràctic és pujar-los a un núvol -Google Drive, OneDrive, Dropbox- i compartir un enllaç. Aquí és clau entendre els nivells de permís: **només lectura** (pot veure però no tocar), **comentaris** (pot fer anotacions) i **edició** (pot modificar el document). I sobretot, distingir entre compartir amb persones concretes (per correu) i generar un enllaç obert a "qualsevol persona que el tingui": aquesta segona opció és còmoda però arrisca que el fitxer acabi circulant més enllà del previst, especialment si conté dades personals o sensibles.

El procediment habitual a Google Drive per compartir un fitxer o carpeta amb persones concretes és:

1. Fes clic amb el botó dret sobre el fitxer o la carpeta (o obre'l i clica la icona "Comparteix" a dalt a la dreta).
2. Tria "Comparteix".
3. Al camp "Afegeix persones i grups" escriu les adreces de correu de qui hi ha de tenir accés.
4. A la dreta de cada adreça, tria el nivell de permís: "Lector" (només veure), "Comentarista" (pot afegir comentaris però no editar el contingut) o "Editor" (pot modificar-lo).
5. Prem "Envia" per notificar-los per correu que tenen accés al fitxer.

Si en canvi el que es vol és un enllaç obert, dins el mateix quadre de "Comparteix" hi ha l'apartat "Accés general", on es pot canviar de "Restringit" (només les persones afegides) a "Qualsevol persona amb l'enllaç", triant també si aquest enllaç dona permís de lector, comentarista o editor.



Pensa en el cas pràctic típic: vols compartir una carpeta de fotos amb tota la teva família a Google Drive perquè hi puguin afegir imatges, però que ningú de fora hi tingui accés. La resposta correcta és compartir la carpeta amb les adreces de correu concretes de cada familiar, amb permís d'edició; no té sentit fer servir un enllaç obert perquè "qualsevol persona amb l'enllaç" inclou, de fet, qualsevol persona a qui el reenviïn per error o expressament, i el propòsit era precisament limitar-ho a la família.

L'exemple contrari també és habitual a l'examen: quin és el risc principal de generar un enllaç del tipus "qualsevol persona amb l'enllaç pot editar" per a un document amb dades personals? El risc és que el document pot circular i ser modificat per persones no previstes, sense cap control d'accés individual, perquè qualsevol que rebí l'enllaç (encara que no sigui a qui anava dirigit originalment) hi pot entrar i fer canvis.

Un error habitual a evitar: deixar per defecte l'accés "Qualsevol persona amb l'enllaç" en documents de treball intern (nòmines, dades d'alumnes, informes mèdics) només perquè és més ràpid que anar afegint adreces una per una. La comoditat mai ha de guanyar a la protecció de dades personals: quan el contingut és sensible, sempre val més invertir el minut extra a afegir les adreces concretes.

Col·laboració en temps real: documents, comentaris i historial

Google Docs, Sheets o els equivalents de Microsoft 365 permeten que diverses persones editin un mateix document alhora, cadascuna des del seu propi ordinador, i vegin en temps real els canvis que fa la resta, sovint amb el cursor de cada persona identificat per un color o un nom. Aquesta és, de fet, la resposta habitual quan l'examen pregunta quina eina permet que diverses persones editin un mateix document de text a la vegada, en temps real, des de navegadors diferents.

Edició, comentaris i mode de suggeriments

Dins d'aquesta edició conjunta convé distingir dues maneres de proposar canvis: escriure directament sobre el text (edició) o afegir un comentari al marge que assenyalava un problema sense modificar el contingut. Per afegir un comentari a Google Docs, cal seleccionar el fragment de text sobre el qual es vol comentar i clicar la icona de "+" amb un requadre (afegeix comentari) que apareix al marge dret, o bé anar al menú "Insereix" > "Comentari". El comentari queda enllaçat a aquell fragment concret i qualsevol persona amb accés pot respondre-hi, formant un petit fil de conversa al marge del document sense tocar el text principal.

Encara més precís és el mode de suggeriments (a vegades anomenat "mode de revisió"), en què els canvis que fas no s'apliquen directament sinó que queden marcats com a proposta perquè la persona propietària del document els accepti o els rebutgi; és la manera adequada de revisar el text d'algú altre sense imposar-hi canvis, i l'examen ho sol plantejar com el cas d'un company que revisa un informe que no és seu. Per activar-lo a Google Docs, cal clicar la icona amb forma de llapis que hi ha a dalt a la dreta del document (al costat de la icona de compartir) i triar l'opció "Suggeriments" en lloc de "Edició"; a partir d'aquí, qualsevol text que s'esborri apareixerà ratllat i qualsevol text nou apareixerà subratllat i en un altre color, amb el nom de qui ho proposa, fins que la persona propietària del document accepti o rebutgi cada suggeriment amb els botons de tick verd o creu vermella que apareixen al marge. A Word i al Word en línia de Microsoft 365 la funció equivalent es diu "Control de canvis" i s'activa des de la pestanya "Revisió".

Un cas pràctic per fixar-ho bé: un company t'ha de revisar un informe, però no vols que els canvis que proposi s'apliquen directament al text, sinó que quedin marcats perquè tu els acceptis o els rebutgis un a un. Has de demanar-li que activi el mode de suggeriments (o de revisió), no que editi el document



directament.

Historial de versions

L'historial de versions és la xarxa de seguretat d'aquesta manera de treballar: guarda automàticament versions anteriors del document a mesura que es va editant, de manera que si algú esborra per error un paràgraf important, o si cal recuperar com estava el text ahir a la tarda, es pot obrir l'historial i tornar a aquell punt sense haver de refer res de memòria. A Google Docs, Sheets o Slides s'hi accedeix des del menú "Arxiu" > "Historial de versions" > "Veure historial de versions", que obre un panell lateral amb totes les versions guardades ordenades per data i hora, indicant sovint qui ha fet cada canvi; des d'allà es pot restaurar qualsevol versió anterior amb el botó "Restaura aquesta versió". A Word en línia l'opció equivalent es troba al títol del document, clicant la data de l'última modificació, o des de "Arxiu" > "Historial de versions".

El cas pràctic típic d'examen: un company esborra per error un paràgraf important d'un document compartit a Google Docs; per recuperar-lo cal consultar l'historial de versions del document, no intentar refer-lo de memòria ni demanar-li a l'altra persona que ho recordi.

Espais de treball en línia

Els espais de treball en línia (una carpeta compartida d'equip, un canal de Teams o Slack) centralitzen documents i converses perquè no calgui anar-los buscant en cadenes de correu, i sovint incorporen també eines senzilles de gestió de tasques: llistes o taulers on s'assigna qui ha de fer què i per quan, de manera que tothom pot veure l'estat d'una feina sense necessitat de preguntar-ho per correu. Per exemple, un equip que vol centralitzar en un mateix lloc els documents, les converses i el seguiment de qui ha de fer cada tasca, en lloc d'anar-ho buscant disperses en cadenes de correu, hauria de crear un espai de treball en línia amb gestió de tasques integrada (una carpeta compartida amb un canal de Teams o Slack associat), en lloc de continuar treballant amb correus solts que es van perdent.

Calendaris compartits i convocatòria de reunions

Els calendaris compartits mereixen atenció especial a l'examen: es pot compartir la disponibilitat (mostrar només si estàs lliure o ocupat, sense detalls) o el detall complet dels esdeveniments, i cada opció té el seu context. Compartir només la disponibilitat és habitual entre companys d'equips diferents que necessiten quadrar una hora sense veure el contingut de les reunions de l'altre; compartir el detall complet té sentit dins d'un mateix equip de treball molt cohesionat.

A Google Calendar, la configuració d'aquest permís es fa des de l'engranatge > "Configuració" > el nom del calendari propi al menú de l'esquerra > "Permisos per als esdeveniments"; des d'allà es pot triar, per a cada persona amb qui es comparteix, si veurà "Només ocupat/lliure (oculta els detalls)" o "Veure tots els detalls dels esdeveniments". Aquesta distinció és exactament la que pregunta l'examen quan planteja quina diferència hi ha entre compartir la "disponibilitat" o el "detall complet" d'un esdeveniment: la disponibilitat mostra si estàs lliure o ocupat, sense mostrar el motiu ni els detalls de la reunió, mentre que el detall complet mostra també el títol, la descripció i els assistents.

Convidar algú a una reunió a través del calendari envia automàticament una notificació i permet confirmar assistència (sí, no, potser), cosa que estalvia el clàssic intercanvi de correus per quadrar una hora i, a més, deixa constància de qui ha confirmat i qui no. El procediment és senzill: en crear un esdeveniment nou a Google Calendar, dins l'apartat "Convidats" s'hi escriuen les adreces de correu de les persones convocades; en desar l'esdeveniment, cadascuna rep una invitació al seu propi correu i calendari, amb



botons per respondre "Sí", "No" o "Potser", i l'organitzador pot veure en tot moment, dins del mateix esdeveniment, qui ha confirmat i qui encara no ha respost.

El cas pràctic: vols convidar 8 companys de feina a una reunió i que puguin confirmar la seva assistència automàticament. L'eina més adequada és crear l'esdeveniment en un calendari compartit i convidar-los des d'allà, en lloc d'enviar un correu preguntant la disponibilitat de cadascú un per un.

Un detall que sol confondre: el calendari compartit no serveix només per convocar reunions, també és útil per veure d'un cop d'ull la disponibilitat de tot un equip abans de proposar cap hora, evitant l'intercanvi típic de correus de "a mi em va bé dimarts" que es repeteix persona per persona.

Identitat i reputació digital

Tot el que fem a internet -comentaris, fotos, publicacions, però també allò que altres publiquen sobre nosaltres- configura la nostra **identitat digital**, i la percepció que en resulta és la **reputació digital**. Aquesta distinció és exactament la que planteja l'examen: la identitat digital és el conjunt del que fem i publiquen sobre nosaltres a internet; la reputació digital és la percepció que en resulta, és a dir, com ens perceben els altres a partir d'aquesta identitat.

Configurar la privadesa d'un perfil

Configurar bé la privadesa d'un perfil de xarxa social vol dir decidir, publicació per publicació o de manera general, qui pot veure què: només amistats, amics d'amics o qualsevol persona d'internet. A la majoria de xarxes socials aquesta configuració es troba dins un menú anomenat "Configuració i privadesa" (o similar), amb apartats específics per triar qui pot veure les publicacions futures, qui pot veure les publicacions passades, qui pot etiquetar-te en fotos o qui pot enviar-te sol·licituds de contacte.

És una bona pràctica preguntar-se de tant en tant què veuria de tu una persona completament desconeguda que et cerqués pel nom: si el perfil és públic, hi pot arribar qualsevol, des d'un futur cap de recursos humans fins a algú amb males intencions, i això inclou fotos, opinions publicades fa anys o dades com la ciutat on vius. Aquest exercici mental -imaginar-se el propi perfil des dels ulls d'un desconegut- és precisament la bona pràctica que l'examen espera que reconeguis quan pregunta com comprovar si has configurat bé la privadesa del teu perfil.

Perfil personal versus perfil professional

En aquest sentit, val la pena separar el perfil personal del professional quan les xarxes ho permeten: a LinkedIn té sentit mostrar-se amb el nom real, la trajectòria laboral i un to més formal, mentre que altres xarxes es poden reservar per a l'àmbit privat amb una configuració de privadesa més restrictiva. Barrejar-ho tot en un sol perfil obert acaba exposant a un possible ocupador, o a un client, continguts que no tenien res a veure amb la feina. Per exemple, si algú té un perfil professional a LinkedIn amb el seu nom real i la seva trajectòria laboral, i alhora un perfil més personal en una altra xarxa social, la pràctica recomanada per a aquest segon perfil és configurar-hi una privadesa més restrictiva que la del perfil professional: no cal que sigui visible per a qualsevol reclutador o client que et busqui, perquè el seu contingut pertany a un àmbit diferent de la vida.

El dret a l'oblit

El dret a l'oblit permet, en determinades condicions, demanar que un cercador o una plataforma deixi d'enllaçar o elimini informació personal que ja no és rellevant, és inexacta o s'ha fet pública sense el consentiment de la persona afectada; no és un dret absolut ni automàtic (s'ha de sol·licitar i pot ser



denegat si hi ha un interès públic legítim més gran), però és una eina real davant de continguts antics que perjudiquen la reputació d'algú. Aquesta darrera precisió -que pot ser denegat si hi ha un interès públic legítim més important- és el matís que més sol confondre a l'examen: no n'hi ha prou de sol·licitar-ho perquè s'apliqui automàticament, cal que es valorin els drets en conflicte.

És una bona pràctica, en general, cercar el propi nom periòdicament per saber què hi ha publicat, revisar la configuració de privadesa de les xarxes socials i pensar abans de publicar que allò pot quedar-hi molt de temps i ser vist per persones que no eren el públic previst, la coneguda "petjada digital". Precisament, quan l'examen pregunta què s'entén per petjada digital, la resposta és el conjunt de rastres i dades que una persona deixa a internet amb la seva activitat: cada publicació, cada comentari, cada "m'agrada" i cada cerca formen part d'aquest rastre acumulat, encara que la persona no en sigui del tot conscient en el moment de generar-lo.

Assetjament i comportament cívic

El comportament cívic també implica no participar en assetjament, difusió de rumors o suplantació d'identitat, i denunciar-ho quan es detecta. Si es detecta que algú, per exemple un company d'una xarxa social professional, està rebent missatges d'assetjament reiterats d'un altre usuari, l'actitud cívica correcta és recomanar-li que ho denunciï a la plataforma i, si cal, ho documenti (fent captures de pantalla dels missatges, per exemple), en lloc de mirar cap a una altra banda o respondre amb un altre atac que només empitjoraria la situació.

Identificació i signatura electrònica

Per fer tràmits amb l'administració cal identificar-se digitalment, i aquí hi ha diversos sistemes que conviuen i que l'examen tendeix a confondre expressament perquè en sàpigues distingir les diferències. Aquest és, probablement, el bloc de conceptes que més es confon a l'examen, així que val la pena parar-hi especial atenció.

idCAT Mòbil

idCAT Mòbil: sistema d'identificació de la Generalitat de Catalunya vinculat al mòbil; un cop registrat, rebre un codi per SMS és suficient per signar tràmits, sense necessitat de cap targeta ni lector. És, de tots quatre, el més senzill de fer servir del dia a dia perquè no requereix instal·lar res al dispositiu, només tenir el mòbil a mà. Per donar-se d'alta, cal fer el registre una única vegada -normalment a través de la mateixa seu electrònica, aportant el DNI i el número de mòbil, o presencialment en alguna oficina d'atenció ciutadana si es prefereix- i, a partir d'aquí, cada vegada que cal identificar-se en un tràmit de la Generalitat n'hi ha prou d'introduir el DNI i esperar rebre per SMS un codi numèric que es tecleja a la pantalla per confirmar la identitat i signar.

Cl@ve

Cl@ve: sistema d'identificació electrònica de l'Estat, vàlid a la majoria d'organismes públics espanyols (Seguretat Social, Agència Tributària...), que inclou diverses modalitats (Cl@ve PIN, d'ús puntual i codi renovat cada vegada; Cl@ve Permanent, amb una contrasenya duradora i un segon factor per SMS; i l'opció d'entrar-hi amb certificat electrònic). La diferència pràctica entre Cl@ve PIN i Cl@ve Permanent és exactament la que sol preguntar l'examen: Cl@ve PIN és d'ús puntual amb un codi renovat cada vegada (útil per a algú que fa tràmits esporàdicament i no vol recordar cap contrasenya fixa), mentre que Cl@ve Permanent fa servir una contrasenya duradora amb un segon factor per SMS (més pràctica per a qui fa tràmits sovint, perquè no cal tornar a demanar un codi cada vegada des de zero, encara que igualment



calgui el segon factor per confirmar).

DNI electrònic (DNle)

DNI electrònic (DNle): requereix un lector de targetes intel·ligents (o un mòbil amb NFC compatible) i un PIN; permet signar amb el mateix valor legal que una signatura manuscrita. Per signar tràmits amb el DNle des d'un ordinador, normalment cal connectar un lector de targetes intel·ligents compatible a l'ordinador, introduir el DNle al lector, instal·lar el programari corresponent del fabricant del lector (o, en alguns sistemes operatius, els drivers ja hi són integrats) i, en el moment de signar, introduir el PIN personal que es va establir en obtenir el DNle a la comissaria. Alternativament, alguns mòbils moderns permeten llegir el xip del DNle per contacte NFC (apropant el DNle a la part posterior del telèfon) sense necessitat de lector físic.

Certificat digital

Certificat digital: un fitxer instal·lat a l'ordinador o al mòbil (per exemple el de l'IdCat o la FNMT) que identifica una persona o una empresa de manera unívoca i que, a diferència de l'IdCAT Mòbil, cal instal·lar prèviament i sol utilitzar-se per a tràmits més complexos o de volum, com la gestoria d'una empresa. El certificat digital és una afirmació correcta a tenir present: és un fitxer que identifica de manera unívoca una persona o una empresa i permet signar electrònicament tràmits, i és el sistema preferit quan s'ha de fer molts tràmits seguits o d'una certa complexitat (com la gestió fiscal d'una empresa o d'una assessoria), perquè un cop instal·lat a l'ordinador no cal tornar a demanar codis per SMS cada vegada.

Diferències pràctiques que cal retenir

Val la pena retenir la diferència pràctica: l'IdCAT Mòbil i Cl@ve serveixen per identificar-te i signar tràmits puntuals de manera còmoda des del mòbil, mentre que el certificat digital i el DNle requereixen una instal·lació o un lector previ però ofereixen un nivell de seguretat i formalitat superior, adequat per a operacions de més transcendència. Formulats com sol aparèixer a l'examen: la diferència pràctica principal entre l'IdCAT Mòbil i el certificat digital com a sistemes d'identificació electrònica és que l'IdCAT Mòbil no requereix instal·lar res al dispositiu, mentre que el certificat digital cal instal·lar-lo prèviament i sol usar-se per a tràmits més complexos o de volum.

Tipus de signatura electrònica

És important saber que la signatura electrònica no és sempre el mateix: n'hi ha de simple (per exemple, marcar una casella o escriure el nom), avançada (vinculada de manera única al signant i que permet detectar si el document s'ha modificat després de signar-lo) i qualificada, i només aquesta última té exactament el mateix valor legal que la signatura manuscrita en qualsevol context, perquè es fa amb un certificat qualificat i un dispositiu de creació de signatura reconegut. Les altres dues poden ser vàlides per a molts tràmits (acceptar unes condicions, confirmar una comanda) però no tenen la mateixa força jurídica davant de qualsevol tribunal.

Un exemple senzill per fixar el concepte de signatura simple: quan acceptes les condicions d'un servei en línia marcant una casella amb el text "Accepto els termes i condicions", en general aquesta acció és una signatura simple: prou per a la majoria de tràmits quotidians, però sense la mateixa força que una signatura avançada o qualificada. En canvi, quan signes una declaració de la renda amb Cl@ve o amb certificat digital, o presentes una instància a un registre electrònic amb DNle, sol tractar-se ja de signatura avançada o qualificada, amb plena validesa legal.

Un truc per a l'examen: si la pregunta parla del "mateix valor legal que la signatura manuscrita en



qualsevol context", la resposta sempre és la signatura qualificada; les altres dues (simple i avançada) poden bastar per a molts usos, però mai s'igualen explícitament així a la manuscrita en qualsevol context.

L'administració electrònica: seu, registre, notificacions i tràmits habituals

La **seu electrònica** és la "oficina virtual" d'un ajuntament, departament o organisme: des d'allà es presenten instàncies, es consulta l'estat d'un expedient i es reben notificacions. És, doncs, l'equivalent digital de la finestra física, però disponible les 24 hores i sense necessitat de desplaçar-se.

El procediment habitual d'un tràmit en línia

Per fer un tràmit en línia normalment cal seguir aquests passos:

1. Entrar a la seu electrònica de l'organisme corresponent (ajuntament, Generalitat, Seguretat Social...) i localitzar el tràmit concret, sovint mitjançant un cercador de tràmits o un catàleg per temes.
2. Identificar-se digitalment (amb idCAT Mòbil, Cl@ve, certificat digital o DNle, segons quins accepti l'organisme).
3. Emplenar el formulari corresponent amb les dades sol·licitades.
4. Adjuntar la documentació requerida (normalment en format PDF o imatge escanejada).
5. Revisar les dades introduïdes abans de continuar.
6. Signar electrònicament l'enviament amb el mètode d'identificació triat.
7. Descarregar o guardar el justificant de registre que es genera en confirmar l'enviament.

El registre electrònic i el justificant

El **registre electrònic** és el punt d'entrada oficial de qualsevol document adreçat a una administració: quan presentes una instància, una sol·licitud o un recurs per via telemàtica, en realitat queda registrat d'entrada de la mateixa manera que si l'haguessis presentat en paper a una finestra, però sense horaris ni desplaçaments. Un cop presentat, el sistema genera un **justificant de registre** amb data, hora i número d'entrada, que té el mateix valor que el segell d'un registre presencial i que convé guardar com a prova. Aquest és precisament el document que l'examen anomena quan pregunta com es diu el paper (o fitxer) que el sistema genera en confirmar una instància, amb data, hora i número d'entrada: el justificant de registre.

Un error habitual (i un truc útil per a l'examen): molta gent pensa que un tràmit "no compta" fins que rep resposta de l'administració, però en realitat el que fa fe de la data i hora de presentació és el justificant de registre, no la resposta posterior; a efectes de terminis, el que importa és quan es va registrar d'entrada la instància.

Notificacions electròniques i carpeta ciutadana

Moltes administracions notifiquen electrònicament (per exemple via e-NOTUM a Catalunya): la notificació queda dipositada a la carpeta ciutadana i s'envia un avís per correu o SMS perquè la persona sàpiga que ha d'entrar a consultar-la; és responsabilitat de la persona anar a buscar-la dins el termini, encara que no obri l'avís, i el termini legal per respondre corre igualment des que la notificació queda a disposició, no des que l'usuari efectivament l'obre. Aquest matís -que el termini corre igualment encara que no s'obri l'avís- és exactament el que planteja l'examen amb el cas pràctic de rebre un avís per correu que diu que hi ha una notificació electrònica pendent a la carpeta ciutadana de l'Ajuntament, però no obrir el correu ni entrar a consultar-la: el que passa és que el termini per respondre corre igualment, encara que no s'obri l'avís, cosa que fa molt recomanable revisar sovint la bústia de correu i la carpeta ciutadana per no perdre terminis per descuit.



La funció d'e-NOTUM, quan l'examen la pregunta directament, és gestionar les notificacions electròniques oficials i avisar la ciutadania que en tenen una de pendent: no és el mateix que la carpeta ciutadana (que centralitza tots els tràmits), sinó el sistema concret encarregat de les notificacions.

La **carpeta ciutadana** o "el meu espai" centralitza tots els tràmits fets amb un organisme: expedients en curs, notificacions rebudes i documents presentats, en un sol lloc consultable en qualsevol moment. Formulats com sol aparèixer a l'examen: la carpeta ciutadana (o "el meu espai") és un espai personal en línia on es centralitzen tots els tràmits i notificacions fetes amb aquell organisme, de manera que no cal anar buscant per correus solts o papers guardats per saber en quin punt es troba un expedient.

Tràmits habituals que un ciutadà fa per via electrònica

Entre els tràmits més habituals que un ciutadà fa per via electrònica hi ha l'empadronament o un canvi de domicili al padró municipal, la sol·licitud de cita prèvia per a gestions que encara requereixen atenció presencial (com renovar el DNI o una consulta a la Seguretat Social), i la presentació de la declaració de la renda a través de la seu electrònica de l'Agència Tributària, on es pot consultar l'esborrany, modificar-lo si cal i presentar-lo signat electrònicament sense sortir de casa.

Val la pena veure amb una mica més de detall un parell d'aquests tràmits, perquè l'examen sol plantejar-los com a cas pràctic:

Empadronar-se o canviar de domicili al padró municipal es fa des de la seu electrònica de l'ajuntament corresponent: cal identificar-se (per exemple amb idCAT Mòbil), localitzar el tràmit "Alta o canvi de domicili al padró municipal", emplenar les dades del nou domicili, adjuntar la documentació que acredita la residència (un contracte de lloguer o d'escriptura, per exemple) i signar l'enviament; el sistema genera el corresponent justificant de registre.

Demandar cita prèvia per renovar el DNI, per exemple, es fa des de la seu electrònica de la Policia Nacional o des del portal de cites de l'administració corresponent: es tria la comissaria o oficina, es consulten les hores disponibles i es reserva un dia i una hora concrets, evitant haver-se de presentar sense cita i esperar torn. El mateix principi s'aplica a moltes gestions de la Seguretat Social que encara requereixen presència física per a determinats tràmits.

Presentar la declaració de la renda es fa a través de la seu electrònica de l'Agència Tributària: la persona s'identifica (amb Cl@ve, certificat digital o número de referència), accedeix a l'esborrany que l'Agència ja té preparat amb les dades fiscals conegudes, el revisa i el modifica si cal (afegint deduccions, corregint dades incorrectes) i finalment el presenta signant-lo electrònicament, sense necessitat de moure's de casa ni de portar cap paper a cap oficina.

La Meva Salut

En l'àmbit sanitari català, **La Meva Salut** és el portal que permet consultar l'historial clínic, els resultats de proves, demanar hora amb el metge de capçalera i gestionar receptes, tot amb la mateixa lògica d'identificació digital que la resta de tràmits. Per demanar cita amb el metge de capçalera del CAP, per exemple, cal entrar a La Meva Salut, identificar-se (amb idCAT Mòbil, Cl@ve o certificat digital), anar a l'apartat de "Cites" o "Demanar visita", triar l'especialitat o el professional (metge de família, infermeria...) i seleccionar entre les hores disponibles; el sistema confirma la cita i sol enviar un recordatori per correu o SMS els dies previs.

Participació ciutadana digital

La **participació ciutadana digital** inclou eines com consultes públiques, pressupostos participatius o



plataformes de debat (per exemple Decidim), que permeten opinar, votar propostes o fer el seguiment d'iniciatives sense haver d'anar presencialment a cap oficina. Un exemple molt clar de participació ciutadana digital, tal com el planteja l'examen, és votar una proposta de pressupostos participatius en una plataforma com Decidim: la ciutadania proposa i vota en quines partides es destina una part del pressupost municipal, tot des d'una plataforma en línia oberta a qualsevol veí empadronat.

Netiqueta professional

La netiqueta és el conjunt de normes de bon comportament a internet, i en un context professional adquireix matisos propis segons el canal que facis servir. El to no és el mateix a un correu institucional, més formal i complet, que a un missatge de xat intern, més breu i directe; adaptar el registre al canal és una habilitat que l'examen valora especialment.

Assumpte, temps de resposta i horaris

Posar un assumpte clar i concret que resumeixi el contingut del missatge és una de les bones pràctiques més bàsiques i alhora més preguntades de la netiqueta de correu professional: permet que qui rep el missatge sàpiga de què tracta sense haver-lo d'obrir, i facilita trobar-lo després amb el cercador.

Respondre en un temps raonable, sense fer esperar dies una resposta senzilla però tampoc sentir-se obligat a contestar de matinada o en cap de setmana, forma part d'aquest mateix criteri, i per això existeixen eines com la resposta automàtica o els missatges programats, precisament per gestionar les expectatives sense haver d'estar sempre disponible. En un grup de treball a Teams o Slack, la pràctica recomanada és utilitzar els canals o converses temàtiques adequades, evitant missatges que no aportin informació, en lloc d'escriure-ho tot en un únic canal general barrejat sense cap ordre.

"Respondre a tots" i el soroll dels grups

"Respondre a tots" és pràctic quan de debò tothom necessita veure la resposta, però és un error habitual quan el missatge només interessa a l'emissor original: respondre "gràcies" o una qüestió personal a una llista de 40 persones satura innecessàriament totes les bústies. Abans de prémer aquest botó val la pena preguntar-se si la resta de destinataris realment necessiten llegir això. En un grup de treball s'ha d'evitar el soroll (missatges que no aporten, com un simple "ok" a tothom) i respectar els horaris de la resta, sense esperar resposta immediata fora de l'horari laboral.

Cadenes, majúscules i verificació

Cal pensar-s'ho dues vegades abans de reenviar una cadena de missatges sense contrastar-la: molts són bulos o hoaxes dissenyats per generar alarma o aconseguir que es reenviïn massivament (el típic "reenvia'l o perdràs..."), i la pràctica correcta és no reenviar-los i, si es pot, contrastar la informació en una font fiable abans de dir-ho a ningú més. Un cas pràctic típic: reps un missatge de WhatsApp que et demana reenviar-lo a 10 contactes perquè, diu, "l'aplicació deixarà de ser gratuïta si no ho fas"; l'actitud correcta és no reenviar-lo, ja que és un patró típic de cadena falsa (hoax). Aquest tipus de missatge sempre segueix el mateix esquema: una amenaça exagerada ("perdràs el compte", "et cobraran"), una petició de reenviament massiu i cap font verificable que ho sustenti; reconèixer aquest patró és l'habilitat clau que avalua l'examen.

Escriure en majúscules equival a cridar, i és una altra d'aquelles normes que sembla de sentit comú però que l'examen sol formular com a pregunta concreta: en un correu de feina, escriure un paràgraf sencer en majúscules s'interpreta habitualment com cridar o alçar la veu al destinatari, encara que la intenció de qui



l'escriu no fos aquesta, i per això s'aconsella reservar les majúscules només per remarcar una paraula puntual, mai un text sencer.

Consells per a la prova

Moltes preguntes d'aquesta àrea són de criteri pràctic més que de memorització: pensa sempre "què faria una persona prudent i respectuosa amb la privadesa dels altres, i que sap treure profit de les eines que té a mà". Repassa bé les diferències entre els sistemes d'identificació digital (idCAT Mòbil, Cl@ve, DNIe, certificat) i entre els tipus de signatura electrònica, perquè són els conceptes que més es confonen. Repassa també les funcions menys evidents del correu i de la videotrucada (regles, resposta automàtica, sala d'espera, fons difuminat), que el nivell mitjà dona per fetes.

Fixa't especialment en els casos pràctics de l'administració electrònica: el termini corre encara que no obris l'avís de notificació, el justificant de registre és la prova que val, i la carpeta ciutadana centralitza tot allò que has fet amb un organisme. I recorda, com a resum d'actitud més que de continguts: CCO per protegir adreces de tercers, enllaç restringit millor que obert quan hi ha dades sensibles, avisar sempre abans de gravar una reunió, i verificar abans de reenviar qualsevol cosa. Si a l'examen dubtes entre dues opcions i una implica exposar dades d'altri sense necessitat i l'altra no, la resposta correcta gairebé sempre és la que protegeix més la privadesa aliena.

**3**

TEMA

Àrea 3. Creació de continguts digitals**Processadors de text: estils, estructura i format llarg****Per què "posar-ho bonic a mà" surt car**

Quan algú escriu un treball de deu pàgines per primera vegada sol fer el mateix: selecciona el títol de cada apartat, li posa negreta, puja la mida a 16 i canvia de tipografia. Funciona... fins que cal canviar tots els títols de color o afegir un capítol nou a la meitat del document. Aleshores toca repassar pàgina per pàgina, i és fàcil deixar-se'n un. Això és exactament el que reflecteix el material d'examen: en un document llarg (una memòria, un treball, un informe de varies pàgines) aplicar format "a mà" és un error que es paga car quan cal reorganitzar el document.

La solució professional és treballar amb **estils**. Un estil és una etiqueta que agrupa un conjunt de característiques (tipografia, mida, color, espaiat) sota un nom, de manera que aplicar l'etiqueta aplica totes les característiques alhora, i modificar l'etiqueta una sola vegada actualitza tots els paràgrafs que la porten.

Aplicar i modificar estils, pas a pas**A LibreOffice Writer:**

1. Obre la galeria d'estils amb la tecla **F11** (o Estils>Gestiona els estils).
2. Selecciona el paràgraf que vulguis convertir en títol.
3. Fes doble clic sobre "Títol 1" (per a un apartat principal) o "Títol 2" (per a un subapartat) a la galeria.
4. Per canviar l'aspecte de TOTS els títols 1 de cop: clic amb el botó dret sobre "Títol 1" a la galeria>Modifica>ajusta tipografia, mida o color>Acceptar. Automàticament es reformaten tots els paràgrafs que porten aquest estil.

A **Microsoft Word** el concepte és idèntic amb el panell "Estils" de la pestanya Inici: selecciona el text i clica l'estil "Títol 1" o "Títol 2" a la galeria d'estils ràpids; per modificar-lo, botó dret sobre l'estil>Modifica.

Un matís que confon molta gent i que l'examen aprofita: aplicar directament "negreta + mida 16" a un text no el converteix en un títol per al programa, encara que visualment ho sembli. Només l'estil "Títol 1" el marca com a tal, i és aquesta marca invisible la que permet construir un índex automàtic o navegar pel document amb el panell de navegació.

La taula de continguts, la recompensa dels estils

Aquest és un dels avantatges que l'ACTIC sol preguntar amb més insistència: si els títols estan marcats amb estils en comptes de format manual, es pot generar automàticament una **taula de continguts** (índex).

Pas a pas per crear-la:

1. Assegura't que tots els títols del document tenen aplicat "Títol 1" / "Títol 2" (no negreta manual).
2. Situa el cursor a la pàgina on vols l'índex.
3. A Word: pestanya Referències>Taula de continguts>tria un estil.
4. A Writer: Inserir>Índex i taules>Índex i taules...>Acceptar.
5. Si després afegeixes un capítol o canvies l'ordre de les seccions, fes clic dret sobre l'índex>Actualitza el camp (Writer) o Actualitza taula (Word), i es recompon sol, sense repassar-lo a mà.



Truc per a l'examen: si et pregunten per què un índex "no surt bé" o "no apareix un apartat", la resposta gairebé sempre és que aquell títol no té aplicat l'estil de títol corresponent, sinó format manual.

Capçaleres, peus de pàgina i numeració

Un document professional també es reconeix per com gestiona capçaleres, peus de pàgina i numeració. Es defineixen una sola vegada, des d'Inserir>Capçalera i peu de pàgina (a Writer) o la pestanya Inserció>Capçalera/Peu de pàgina (a Word), i es repeteixen a totes les pàgines sense haver-les de retocar full a full. El número de pàgina no s'escriu mai a mà: s'insereix com a camp (Inserir>Camp>Número de pàgina), i així s'actualitza sol si més endavant s'afegeixen o s'eliminen pàgines.

Es pot configurar una capçalera diferent per a la primera pàgina (útil perquè la portada no dugui número ni logotip repetit), o alternar-ne el contingut entre pàgines parells i imparells en documents pensats per imprimir-se a doble cara, com un llibret o una memòria enquadernada.

Interlineat i salts de pàgina

L'**interlineat** es controla des del format de paràgraf (Format>Paràgraf>pestanya Sagnats i espaiat), no afegint línies en blanc a mà prement Retorn diverses vegades. Un interlineat d'1,5 o doble és habitual en treballs acadèmics perquè el corrector hi pugui anotar comentaris entre línies.

Per començar un capítol sempre en una pàgina neta, sense comptar quantes vegades cal prémer Retorn fins arribar-hi, s'utilitza un **salt de pàgina: Ctrl+Retorn**. És un salt "dur" que es manté fix encara que s'afegeixi o s'esborri text abans, de manera que el capítol nou continua començant a la pàgina següent, sense desquadrar-se. Aquesta és, de fet, la pregunta típica d'examen: quan et demanen que un capítol comenci sempre a l'inici d'una pàgina encara que hi afegeixis o esborris text abans, la resposta correcta és el salt de pàgina, mai Retorn repetit.

Taules i imatges dins del text

Amb **taules**, cal saber-ne inserir de noves (Taula>Insereix taula, indicant files i columnes), combinar o dividir cel·les, i aplicar un estil de taula predefinit (colors alterns per fila, vores) des de les eines de disseny de taula.

Amb les **imatges**, l'ajust del text al voltant sol generar dubtes, i és un dels punts que més es pregunta a examen perquè la teoria i la pràctica xoquen sovint:

- **En línia amb el text:** és el mode per defecte en inserir una imatge. El programa la tracta com si fos un caràcter més dins de la línia, tan alta com sigui la imatge. És la causa més freqüent que un paràgraf "es desmunti" en enganxar-hi una imatge gran: la línia s'estira i tot el text queda desplaçat.
- **Ajust quadrat o estret:** el text flueix al voltant del contorn (quadrat) o de la forma (estret) de la imatge, com en una revista.
- **Davant o darrere del text:** la imatge queda superposada, independent del flux del paràgraf, útil per a marques d'aigua o decoracions, però poc pràctic per il·lustrar un text explicatiu.

Per canviar-ho: clic dret sobre la imatge>Ajusta el text (Writer) o Disposició del text (Word), i triar l'opció adequada.

Plantilles: un document base, no una còpia

Una **plantilla** (extensió .dotx a Word, .ott a Writer) és un document base amb estils, capçaleres, marges i sovint un logotip ja definits, pensat perquè molts documents diferents en surtin amb el mateix aspecte (una factura, un informe corporatiu, un treball acadèmic amb la portada de la universitat).



No és el mateix que "un document que després guardo amb un altre nom": en obrir una plantilla amb doble clic, el programa crea automàticament un document nou, sense tocar mai l'arxiu original de la plantilla, per molts cops que es faci servir; si en canvi obres un document normal i l'edites, existeix el risc de sobreescrivre l'original si t'oblides de canviar-ne el nom en desar-lo.

Combinació de correspondència: una carta, molts destinataris

La **combinació de correspondència** (mail merge) enllaça un document base (una carta, unes etiquetes, uns certificats) amb una font de dades, per generar automàticament una versió personalitzada per a cada destinatari, sense escriure cada carta a mà.

Pas a pas orientatiu a Writer (Eines>Auxiliar de combinació de correspondència) o Word (pestanya Correspondència>Inicia la combinació de correspondència): prepara la font de dades (una fila per registre, una per persona, amb els noms de camp a la primera fila: Nom, Cognoms, Adreça...); redacta el document base amb el text fix; insereix els camps combinats allà on han de variar (per exemple, "Benvolgut/da «Nom»,"); vincula el document amb la font de dades; i genera el resultat, amb una còpia personalitzada per cada fila de la font.

Aquest és un punt molt preguntat: si la font de dades no té una fila per registre amb els noms de camp ben definits a la capçalera (per exemple, si les dades estan escampades en cel·les soltes sense estructura de taula), la combinació no funciona correctament o assigna malament els camps.

Control de canvis i comentaris: dues eines que no s'han de confondre

El **control de canvis** (Revisar>Control de canvis, o Ctrl+Maj+C) marca en colors qui ha afegit, esborrat o modificat cada fragment de text, sense perdre mai el text original fins que algú accepta els canvis explícitament (Revisar>Accepta) o els rebutja (Revisar>Rebutja). És l'eina adequada quan diverses persones corregeixen un mateix document i cal poder desfer una correcció.

Els **comentaris** (Inserir>Comentari) permeten anotar un dubte, un suggeriment o una pregunta al marge, associat a un fragment de text seleccionat, sense tocar ni una lletra del contingut.

La diferència que pregunta l'examen és precisa: el control de canvis modifica el contingut del document, de manera reversible i marcada visualment, mentre que el comentari és una nota externa, al marge, que no altera absolutament res del text.

Fulls de càlcul: referències, fórmules i funcions

Referències relatives, absolutes i mixtes

El nucli del nivell mitjà en fulls de càlcul és entendre com es comporta una referència a una cel·la quan es copia o s'arrossega la fórmula a altres cel·les.

- **Referència relativa** (A1): canvia proporcionalment quan arrossegues la fórmula a una altra cel·la. Si a B2 escries =A2 i ho arrossegues a B3, es converteix automàticament en =A3.
- **Referència absoluta** (\$A\$1): es manté sempre fixa, apunti on apunti la còpia de la fórmula. El símbol de dòlar davant de la lletra i davant del número "ancora" tant la columna com la fila.
- **Referència mixta** (\$A1 o A\$1): només una part queda fixada. \$A1 fixa la columna (sempre A) però deixa variar la fila; A\$1 fixa la fila (sempre 1) però deixa variar la columna.

Exemple resultat, el mateix que apareix al banc de preguntes: escries la fórmula =A1+\$B\$1 a la cel·la C1 i l'arrossegues cap avall fins a C5. A cada fila, la referència relativa avança (a C2 queda =A2+\$B\$1, a C3



=A3+\$B\$1, i així fins a C5, =A5+\$B\$1), mentre que \$B\$1 es manté sempre igual perquè els símbols de dòlar l'ancoren. Aquest tipus d'exercici, predir com queda una fórmula després d'arrossegar-la, és l'estil de pregunta més habitual sobre referències.

Per convertir una referència de relativa a absoluta ràpidament, sense escriure els símbols de dòlar a mà: selecciona la referència dins la fórmula i prem **F4** (en molts fulls de càlcul), que va alternant entre A1, \$A\$1, A\$1 i \$A1 cada vegada que es prem.

Funcions bàsiques i condicionals

Les funcions que cal saber utilitzar de manera pràctica, no només reconèixer de nom, són:

- **SUMA**: suma un rang de cel·les. Exemple: =SUMA(B2:B20) suma totes les vendes de la columna B entre les files 2 i 20.
- **MITJANA** (o PROMITJA, segons el full de càlcul): calcula la mitjana aritmètica d'un rang.
- **MÀXIM** i **MÍNIM**: retornen el valor més alt o més baix d'un rang.
- **COMPTAR**: compta quantes cel·les d'un rang contenen un número.
- **COMPTA.SI** (COMPTAR.SI): compta només les cel·les que compleixen una condició. Exemple pràctic: tens una columna amb les notes d'un grup d'alumnes i vols saber quants han tret un 5 o més, sense sumar-ne els valors: =COMPTA.SI(B2:B30;">=5"). Aquesta funció no suma res, només compta quantes cel·les compleixen la condició.
- **SI(condició; valor_veritable; valor_fals)**: la funció condicional bàsica, la més preguntada de totes. Exemple: =SI(B2>=5;"Apte";"No apte"): si la nota de B2 és 5 o més, la cel·la mostra "Apte"; si no, mostra "No apte".
- **SUMA.SI**: suma només les cel·les que compleixen un criteri. Exemple resultat: tens una llista de vendes amb la botiga a la columna A i l'import a la columna B, i vols saber quant ha venut només la botiga "Girona": =SUMA.SI(A2:A50;"Girona";B2:B50). La funció recorre la columna A buscant "Girona" i, quan la troba, suma l'import corresponent de la columna B a la mateixa fila.
- **PROMITJA.SI**: igual que SUMA.SI però fa la mitjana en lloc de sumar.
- **BUSCARV** (o CONSULTAV, VLOOKUP en anglès): busca un valor a la primera columna d'una taula i retorna un valor d'una altra columna de la mateixa fila (per exemple, buscar un codi de producte i que et retorni el seu preu). Comença a aparèixer en algun examen de nivell mitjà, tot i que és més pròpia del nivell avançat; n'hi ha prou de conèixer-ne l'existència i la idea general.

Format de nombre: canvia l'aspecte, no el valor

El **format de nombre** d'una cel·la no canvia mai el valor real que conté, només com es mostra en pantalla. La xifra 1500 es pot presentar com a moneda (1.500,00 euros), com a data o com a percentatge, sense que el número guardat internament canviï.

Aquest matís genera dos errors clàssics d'examen:

1. Confondre format amb valor: si una cel·la mostra "1.500,00 euros" i en fas referència des d'una fórmula, la fórmula treballa amb el número 1500, no amb el text "euros".
2. El parany del percentatge. Si en una cel·la escrius el número 15 amb la intenció que representi un 15%, i després li apliques el format de percentatge, el resultat que es mostra és 1500%, no 15%. Això passa perquè el format de percentatge multiplica per cent el valor que ja hi ha escrit. Per obtenir un 15% real cal escriure el número en tant per u, és a dir 0,15, i aplicar-hi després el format de percentatge, que el mostrarà correctament com a 15%. Canviar el format a percentatge sense haver escrit abans el número en tant per u és, doncs, l'error que desquadra els resultats en cadena si aquella cel·la s'utilitza en més fórmules.



Ordenar, filtrar i immobilitzar

Ordenar i filtrar dades és una habilitat pràctica de cada dia: ordenar una llista per una columna (per exemple, per import de més gran a més petit) i aplicar un filtre des de Dades>Filtre (o l'autofiltre, que afegeix unes fletxetes desplegable a la capçalera de cada columna) per mostrar només les files que compleixen un criteri concret, sense esborrar mai la resta de dades, que simplement queden ocultes fins que es treu el filtre.

En una taula llarga, on la capçalera desapareix de la vista en baixar avall, **immobilitzar files i columnes** (Visualitza>Immobilitzar files i columnes, triant si es vol immobilitzar només la primera fila, la primera columna o una combinació) manté sempre visibles les capçaleres mentre es navega per la resta de la taula amb la barra de desplaçament.

Triar el gràfic adequat

Pel que fa als **gràfics**, l'ACTIC valora que sàpigues triar el tipus adequat segons què es vol comunicar, no només saber-ne inserir un des del menú Inserir>Gràfic:

- **De columnes o barres:** per comparar valors entre categories diferents en un moment donat, com les vendes de cada botiga d'una cadena el mateix mes.
- **De línies:** per mostrar una evolució al llarg del temps, com les vendes mensuals d'una empresa durant un any sencer; el que interessa aquí és veure la tendència, pujada o baixada, i les línies connecten visualment un mes amb el següent.
- **De sectors** (o de pastís): per veure quina proporció representa cada part respecte d'un total, com el repartiment del pressupost d'un ajuntament entre educació, sanitat i urbanisme. Aquest tipus de gràfic només té sentit si les dades sumen un total coherent (el 100% del pressupost, per exemple); no s'ha d'utilitzar per comparar magnituds que no formen part d'un mateix conjunt.

Truc per a l'examen: si l'enunciat parla d'"evolució" o "al llarg del temps", pensa en línies; si parla de "proporció", "percentatge del total" o "repartiment", pensa en sectors; si parla de "comparar" categories independents, pensa en columnes o barres.

Imprimir un full de càlcul gran

Un aspecte que sovint es descuida fins que cal imprimir de veritat un full gran: un full ample o llarg que no cap en una sola pàgina. Passos a seguir:

1. Revisa la previsualització de salt de pàgina (Visualitza>Salt de pàgina) per veure com quedaran repartides les dades entre fulls.
2. Ajusta l'àrea d'impressió (Format>Àrees d'impressió>Defineix) si només vols imprimir una part concreta del full.
3. Defineix files o columnes que es repeteixin a cada full imprès (Format de pàgina>Fulls>Files/columnes a repetir), perquè la capçalera amb els noms de les columnes surti a totes les pàgines impreses i no només a la primera.
4. Si cal, escala el contingut a un nombre determinat de pàgines d'ample (Format de pàgina>Escala>Ajusta a) perquè totes les columnes càpiguen en l'amplada d'una sola pàgina, encara que el full continuï en diverses pàgines de llargada.

Presentacions que no s'improvisen

El patró de diapositives, la base de tot



A Impress o PowerPoint, el nivell mitjà valora que la presentació estigui construïda amb el **patró de diapositives** (Visualitza>Patró de diapositives) i no diapositiva a diapositiva, retocant cadascuna a mà. El patró defineix, d'una tirada, el fons, la tipografia i la posició dels marcadors (on va el títol, on va el contingut) de tota la presentació.

El gran avantatge pràctic és aquest: si més endavant vols canviar la tipografia del títol a totes les diapositives, o el color de fons, no cal entrar diapositiva per diapositiva. N'hi ha prou de modificar-ho una sola vegada dins del patró perquè totes les diapositives que en depenen s'actualitzin automàticament.

Pas a pas per editar-lo: Visualitza>Patró de diapositives (Impress) o pestanya Visualització>Patró de diapositives (PowerPoint); selecciona el patró principal (o un dels dissenys derivats, si n'hi ha diversos); modifica la tipografia del títol, el color de fons o la posició dels quadres de text; i tanca la vista de patró per tornar a la vista normal i comprovar el resultat.

Transició i animació: no són la mateixa cosa

Cal distingir dos conceptes que sovint es confonen:

- La **transició** és l'efecte amb què es passa d'una diapositiva a la següent (una esvaïda, un desplaçament lateral). S'aplica des de la pestanya Transicions.
- L'**animació** és un efecte aplicat a un element concret dins d'una mateixa diapositiva: un text que entra lletra a lletra, una imatge que apareix en fer clic, una llista de punts que va sortint un a un. S'aplica des de la pestanya Animacions, seleccionant primer l'element i després l'efecte.

L'ACTIC sol preguntar més per l'ús adequat que per la simple existència de l'efecte: abusar d'animacions distreu l'audiència i alenteix la presentació. El criteri de nivell mitjà és la regla del "menys és més": poques diapositives amb poc text, una idea per diapositiva, i animacions només quan aporten claredat (per exemple, fer aparèixer els punts d'una llista un a un perquè l'audiència no llegeixi per davant allò que encara no s'ha explicat).

Notes de l'orador i el mode de dues pantalles

També s'espera saber utilitzar les **notes de l'orador**: un text associat a cada diapositiva (s'escriu a la zona inferior de la vista normal, o a Visualitza>Notes) que no es projecta mai davant del públic, però que qui presenta pot consultar mentre parla, a manera de guió de suport.

Aquesta funció enllaça amb **presentar amb dues pantalles**: quan l'ordinador es connecta a un projector i s'activa el mode de presentador, es reparteix la informació de manera diferent segons qui la mira:

- El **públic**, a través del projector, veu únicament la diapositiva actual, a pantalla completa, sense cap element addicional.
- Qui **presenta**, al monitor propi de l'ordinador, veu la diapositiva actual, però també les notes de l'orador, un rellotge o cronòmetre, i una previsualització de la diapositiva següent, cosa que li permet preparar la transició sense sorpreses.

Exportar la presentació

La presentació es pot exportar de diverses maneres segons l'ús:

- Com a **PDF**, per repartir-la sense que ningú en pugui alterar el contingut ni desmuntar-ne el disseny en obrir-la amb un altre programa o una altra versió.
- Com a **vídeo**, que incorpora els temps de transició i les animacions ja gravades, útil quan es vol que la presentació es reproduïxi sola, sense algú passant les diapositives.

Plantilla de presentació vs. duplicar una diapositiva



Un matís que surt sovint a examen: una **plantilla de presentació** (extensió .potx a PowerPoint, .otp a Impress) inclou el patró de diapositives, l'esquema de colors i les disposicions de diapositiva (títol i contingut, només títol, dues columnes...) per a tota la presentació sencera. En canvi, "**duplicar una diapositiva**" (botó dret sobre una diapositiva al panell lateral > Duplica la diapositiva) només replica el contingut d'una diapositiva concreta, sense aportar cap dels avantatges d'una plantilla ni permetre reutilitzar el disseny en un altre document.

Imatge: formats, resolució i edició bàsica

Rasteritzada vs. vectorial

Cal distingir amb precisió dos mons molt diferents dins de les imatges digitals:

- **Imatge rasteritzada** (o de mapa de bits): formada per una graella de píxels, cadascun amb un color fix. Formats habituals: JPG, PNG, GIF, WebP. Una fotografia sempre és rasteritzada.
- **Imatge vectorial**: formada per línies i corbes definides matemàticament (punts, angles, colors de farciment), no per píxels. Formats habituals: SVG, EPS.

La diferència pràctica és clau i és exactament el que pregunta l'examen: un logotip vectorial es pot ampliar a la mida d'una lona publicitària sense perdre gens de qualitat, perquè el programa simplement recalcula les fórmules matemàtiques a la mida nova. Una fotografia JPG ampliada, en canvi, es pixel·la (es veuen quadradets), perquè cada píxel és una dada fixa i el programa ha d'"inventar" píxels intermedis que no existien a l'original per omplir l'espai extra.

Formats rasteritzats, un per un

Dins del món rasteritzat, cada format té un ús preferent i unes característiques que l'examen distingeix amb precisió:

- **JPG/JPEG**: pensat per a fotografies. Fa servir compressió amb pèrdua (descarta informació que l'ull difícilment nota per reduir el pes del fitxer) i no admet transparència: el fons sempre és opac.
- **PNG**: pensat per a gràfics, captures de pantalla i logotips que necessiten fons transparent. Fa servir compressió sense pèrdua (no descarta informació), per això sol pesar més que un JPG de mida similar.
- **GIF**: paleta limitada a 256 colors i animació senzilla (fotogrames encadenats). Avui pràcticament desplaçat pel vídeo curt per a animacions, tot i que encara s'utilitza en missatgeria per la seva lleugeresa.
- **WebP**: format més modern, pensat específicament per a web, que comprimeix millor que JPG i PNG mantenint una qualitat semblant. A diferència de JPG, admet tant compressió amb pèrdua com sense pèrdua, i també admet fons transparent, com el PNG. És, per tant, l'únic dels quatre que combina bona compressió amb la possibilitat de transparència.

Resolució: ppp/dpi

La **resolució** es mesura en píxels per polzada (ppp, o dpi en anglès): quants punts de color caben en una polzada lineal d'una imatge. 72 ppp és suficient per a pantalla (un monitor no és capaç de mostrar més detall del que ja ofereix aquesta densitat a la mida habitual de visualització), mentre que 300 ppp és l'estàndard per a impressió de qualitat, perquè l'ull, de molt a prop d'un paper imprès, sí que distingeix més detall.

L'error clàssic d'examen, i també un error real molt habitual en el dia a dia, és pujar una imatge pensada per a pantalla (72 ppp, sovint descarregada directament d'una pàgina web) per imprimir-la en un cartell gran, i que surti borrosa o pixelada perquè la impressora necessita molta més densitat de punts de la que



la imatge conté.

Redimensionar vs. retallar

Un altre parell de conceptes que l'examen distingeix amb cura perquè sovint es confonen col·loquialment:

- **Redimensionar**: canvia la mida global d'una imatge (amplada i alçada en conjunt), mantenint tot el contingut original però fent-lo més gran o més petit, com si s'ampliés o reduís una fotocòpia sencera.
- **Retallar** (crop): elimina part de la imatge original per quedar-se només amb una zona concreta, canviant l'enquadrament (què es veu i què no) però sense canviar la resolució de la part que es conserva.

Exemple resultat: tens una fotografia de grup i només vols la cara d'una persona per fer-ne un carnet: això és retallar. Si tens la mateixa fotografia i la vols fer més petita perquè ocupi menys a la web sense canviar què es veu: això és redimensionar.

Redimensionar cap amunt una imatge petita no en millora mai la qualitat, sinó que sovint l'empitjora: si tens una fotografia petita de baixa resolució i l'amplies molt amb un editor d'imatges perquè ocupi tot un cartell, el resultat es pixel·la, perquè el programa ha d'inventar píxels intermedis que no existien a l'original, exactament pel mateix motiu que explica per què una fotografia JPG ampliada perd qualitat.

El pes del fitxer

El **pes** d'un fitxer d'imatge depèn de tres factors combinats: la resolució (com més píxels, més pes), el nombre de colors i la compressió aplicada. Cal trobar l'equilibri: una imatge massa comprimida mostra artefactes visibles (blocs, pèrdua de detall en vores), mentre que una de massa pesada carrega lentament en una pàgina web.

Eines d'edició: GIMP i Canva

Per a edició bàsica-mitjana, **GIMP** (programari lliure, equivalent funcional de Photoshop) permet retallar, redimensionar, ajustar nivells i contrast, i treballar amb capes (elements superposats que es poden editar per separat) i filtres (efectes que es poden aplicar sobre una capa o una selecció).

Passos habituals a GIMP per a una edició bàsica: Fitxer>Obre per carregar la imatge; Imatge>Escala la imatge per redimensionar-la indicant la nova amplada i alçada; l'eina de retallada (dreuera Maj+C) per retallar la zona que es vol conservar; Colors>Brillantor-Contrast o Colors>Nivells per ajustar-ne l'exposició; i finalment Fitxer>Exporta com a per desar en el format final (JPG, PNG...), ja que GIMP treballa amb el seu propi format natiu (.xcf) mentre s'edita.

Canva, per a qui no vol entrar en capes ni eines de selecció detallades, ofereix plantilles ja dissenyades i una edició guiada especialment pensada per a xarxes socials (mides predefinides per a Instagram, cartells, targetes), amb molt menys control fi que GIMP però amb una corba d'aprenentatge molt més ràpida.

Àudio i vídeo: nocions bàsiques

Formats d'àudio: sense pèrdua vs. amb pèrdua

En àudio, la distinció clau, igual que passava amb les imatges, és entre compressió sense pèrdua i amb pèrdua:

- **Format sense pèrdua** (WAV, FLAC): conserva tota la informació de l'enregistrament original, amb fidelitat total, però genera arxius grans.
- **Format amb pèrdua** (MP3, AAC): comprimeix eliminant informació que l'oïda humana difícilment



distingeix (freqüències que es perceben pitjor, sons emmascarats per altres de més forts), i produeix arxius molt més petits, ideals per compartir o emmagatzemar grans quantitats de música.

Audacity és l'eina de referència, programari lliure, per treballar amb àudio a nivell d'usuari: gravar, retallar fragments, eliminar soroll de fons (seleccionant una mostra només de soroll i aplicant Efectes>Reducció de soroll), normalitzar el volum i exportar-ho en el format que calgui, ja sigui WAV per conservar la màxima qualitat o MP3 per compartir-ho fàcilment.

Contenidor vs. còdec en vídeo

En vídeo, el nivell mitjà espera que sàpigues distingir dos conceptes que es confonen constantment perquè tots dos "sonen" a format de fitxer:

- **Contenidor** (MP4, MKV, AVI): l'embolcall del fitxer, la capsula que agrupa el flux de vídeo, el d'àudio, els subtítols i els metadades.
- **Còdec** (H.264, VP9): el mètode concret amb què es comprimeixen les dades de vídeo (i d'àudio) dins d'aquell contenidor.

Un mateix contenidor MP4 pot dur a dins vídeo comprimit amb còdecs diferents, i per això de vegades un vídeo "no es reproduïx" en un aparell (una televisió, un reproductor antic) encara que l'extensió .mp4 sembli compatible: l'aparell entén el contenidor MP4 en general, però no sap desxifrar aquell còdec concret amb què s'ha comprimit el vídeo per dins.

Edició bàsica de vídeo

L'edició de vídeo que es demana a l'examen de nivell mitjà no requereix programari professional de muntatge:

1. **Tallar un clip**: seleccionar l'inici i el final del fragment útil i descartar la resta.
2. Afegir **transicions** entre tallats, perquè el canvi d'un pla a un altre no sigui sec.
3. Incorporar **subtítols**, ja sigui escrivint-los sincronitzats amb el diàleg dins del mateix editor, o important-los d'un fitxer extern amb els temps ja marcats.

Finalment, cal exportar amb una resolució i un pes adequats al canal on es publicarà el vídeo: no té sentit exportar en la màxima qualitat possible (i amb el pes de fitxer corresponent) un vídeo que només es veurà en una pantalla de mòbil, perquè el temps de càrrega i l'ús de dades no compensen una millora de qualitat que ningú notarà en una pantalla petita.

Integrar i reelaborar continguts de fonts diferents

Un document real rarament és cent per cent original de principi a fi: combina text propi, una imatge trobada en una recerca prèvia, un gràfic exportat d'un full de càlcul. L'ACTIC avalua que sàpigues combinar aquestes fonts sense que el document en surti perjudicat.

Enganxar sense format

Quan copies text d'una pàgina web (per exemple, un fragment de la normativa d'un ajuntament que vols citar) i l'enganxes directament amb Ctrl+V dins d'un document ja format, sol arrossegar-hi el format original de la pàgina web: una altra tipografia, una altra mida, enllaços de color blau subratllat, que trenquen l'estil del document destí i s'han d'anar netejant a mà.

La solució és **Enganxar sense format** (o Enganxament especial), amb la drecera **Ctrl+Maj+V**: en comptes d'enganxar directament, obre un petit menú on es pot triar "text sense format", de manera que el



fragment adopta automàticament l'estil del paràgraf on s'enganxa, sense arrossegat res de l'origen.

Incrustar vs. vincular

Aquesta parella de conceptes és una de les que més confusió genera, i alhora una de les més preguntades: en inserir un objecte d'un programa dins d'un altre (per exemple, un full de càlcul d'Excel dins d'una presentació de PowerPoint), hi ha dues maneres diferents de fer-ho, amb conseqüències molt diferents.

- **Incrustar** un objecte el copia sencer dins del document destí i el fa completament independent de l'arxiu original: si algú modifica el full de càlcul original després, el que s'ha incrustat a la presentació NO canvia, perquè ja n'és una còpia autònoma.

- **Vincular**, en canvi, manté una connexió activa amb l'arxiu font: cada cop que s'obre el document destí (o es demana actualitzar-lo), es va a buscar les dades més recents de l'original i les mostra actualitzades. L'inconvenient és que el vincle es trenca si l'arxiu original es mou, es renomena o s'esborra: llavors el document destí ja no pot recuperar les dades.

Exemple d'ús: si prepares una presentació trimestral amb dades de vendes que canvien cada mes, val la pena vincular el full de càlcul perquè s'actualitzi sola; si vols que quedi congelada tal com estava, per exemple per arxivar-la com a acta d'una reunió passada, val més incrustar-la.

Convertir formats

De vegades cal convertir el format d'un contingut perquè s'adapti al seu ús final: exportar un document a PDF per compartir-lo sense que es pugui editar fàcilment, o convertir una imatge de PNG a JPG per reduir-ne el pes quan no cal mantenir-hi la transparència de fons, com passa amb una imatge PNG destinada a una pàgina web que no necessita fons transparent.

Documents PDF: formularis i signatura

El PDF s'ha convertit en el format de referència per compartir documents que han de veure's exactament igual en qualsevol dispositiu i qualsevol sistema operatiu, sense dependre del programa amb què es van crear originalment. Més enllà de "convertir un document a PDF" (Fitxer>Exporta com a PDF, o Fitxer>Imprimeix i triar una impressora virtual PDF), el nivell mitjà demana saber-hi interactuar de dues maneres més avançades.

Emplenar un formulari en PDF

Molts formularis administratius (una sol·licitud a l'ajuntament, una instància genèrica, un imprès de la seguretat social) es distribueixen amb **campus interactius**: caselles de text on escriure, caselles de verificació per marcar amb un clic, llistes desplegable per triar una opció. Aquests camps es poden clicar i omplir directament amb un lector de PDF com Adobe Acrobat Reader, sense necessitat d'imprimir el document, escriure-hi a mà i tornar-lo a escanejar per enviar-lo.

Pas a pas: obre el PDF amb Adobe Acrobat Reader (o un lector equivalent que admeti formularis); clica sobre cada camp de text i escriu-hi la informació; marca les caselles de verificació i tria les opcions de les llistes desplegable que corresponguin; i desa el document (Fitxer>Desa) o exporta'l amb les dades ja incorporades, abans d'enviar-lo o imprimir-lo.

Quan el PDF no té aquests camps interactius (per exemple perquè és una imatge escanejada d'un full imprès), l'única manera d'omplir-lo digitalment és amb eines d'anotació que hi superposen text a sobre, sense que aquest text quedi realment "estructurat" com un camp de formulari: el programa no sap que allò



és un nom o una adreça, només veu una capa de text flotant sobre una imatge.

Signar un PDF: nivells de validesa molt diferents

Signar un document en PDF admet mètodes amb un nivell de garantia molt diferent, i confondre'ls és un dels errors més habituals a examen:

- **Inserir una imatge escanejada de la signatura manuscrita:** és la manera menys segura, perquè no garanteix la identitat de qui signa (qualsevol pot copiar aquella imatge i enganxar-la en un altre document) ni que el document no s'hagi alterat després de "signar-lo".
- **Signatura digital** pròpiament dita: es basa en un certificat electrònic (el DNI electrònic o un certificat emès per una entitat de certificació reconeguda) que xifra el document i vincula matemàticament la signatura a la identitat del signant. Qualsevol modificació del document després de signar-lo invalida automàticament la signatura, cosa que la fa fiable per a tràmits oficials (presentar una instància, signar un contracte amb validesa legal).

Confondre "posar una imatge de la signatura escanejada" amb "signar digitalment" és un error habitual a examen: només la signatura digital basada en certificat electrònic ofereix garanties legals reals d'autenticitat i integritat del document; la imatge escanejada és, en el millor dels casos, una formalitat visual sense cap validesa tècnica que la sustenti.

Codis QR: crear-ne i llegir-ne

Un **codi QR** (Quick Response) és un codi de barres bidimensional que emmagatzema informació (una adreça web, un text, les dades d'accés a una xarxa Wi-Fi) i es llegeix en una fracció de segon apuntant-hi la càmera d'un mòbil.

A diferència d'un codi de barres tradicional, que codifica una sèrie numèrica en una sola direcció (una línia de barres més primes o més amples), el codi QR aprofita les dues dimensions del quadrat (amplada i alçada) per emmagatzemar molta més informació en el mateix espai físic, i a més incorpora correcció d'errors: un sistema matemàtic que permet reconstruir la informació encara que una part del codi estigui tapada, ratllada o feta malbé, fins a un cert percentatge de dany.

Crear un codi QR és senzill amb qualsevol generador en línia gratuït: n'hi ha prou d'introduir el contingut que es vol codificar (una URL, un text) i l'eina genera automàticament la imatge del codi, llesta per baixar i imprimir en un cartell, una targeta de visita o un tríptic.

Llegir un codi QR només requereix apuntar la càmera del mòbil cap al codi: la majoria de càmeres actuals de mòbil (Android i iPhone) el reconeixen directament des de l'aplicació de càmera nativa, sense necessitat d'instal·lar cap aplicació addicional específica.

A nivell de seguretat, un codi QR pot amagar un enllaç maliciós tan fàcilment com qualsevol enllaç de text: com que el contingut codificat no es veu a simple vista fins que s'escaneja, cal aplicar el mateix criteri de prudència en escanejar un QR d'origen desconegut (per exemple, un adhesiu enganxat sobre el QR oficial d'un aparcament) que en clicar qualsevol enllaç rebut per correu electrònic.

Blogs i pàgines web senzilles

Blog vs. pàgina web fixa

Per publicar contingut a internet sense necessitat de programar, existeixen dues grans famílies d'eines, i l'examen espera que sàpigues triar quina correspon a cada necessitat.



Les plataformes de **blog** (WordPress, Blogger) ofereixen una estructura ja feta i pensada per a contingut que es va publicant amb el temps: entrades ordenades cronològicament (la més recent primera), categories i etiquetes per classificar-les, un espai de comentaris perquè els lectors hi participin, i una plantilla visual personalitzable sense tocar codi. És l'eina adequada per publicar contingut sovint (un diari personal, el butlletí d'una associació amb entrades noves cada setmana ordenades cronològicament i amb categories), més que per a un lloc amb una estructura de pàgines fixa que canvia poc.

Per a una **pàgina web senzilla** (la presentació d'un negoci local, un currículum en línia, la fitxa d'un esdeveniment puntual), els constructors visuals "what you see is what you get" (Wix, Google Sites) permeten dissenyar-la arrossegant blocs de text, imatges i botons directament sobre un llenç visual, sense escriure ni una línia de codi, i publicar-la després amb un domini propi (comprat a banda) o amb un subdomini gratuït que ofereix la mateixa plataforma.

Què hi ha per sota, encara que no es vegi

El nivell mitjà no demana saber programar, però sí entendre que tot el que es veu en una pàgina web és, al fons, un fitxer **HTML** (que en defineix l'estructura: on va cada títol, cada paràgraf, cada imatge) combinat amb un full d'estils **CSS** (que en defineix l'aspecte visual: colors, tipografies, marges), encara que el constructor visual amagui completament aquest codi darrere d'una interfície gràfica d'arrossegar i deixar anar.

Contingut generat amb intel·ligència artificial

Cada cop és més habitual generar text, imatges o resums amb eines d'intel·ligència artificial (ChatGPT, Gemini, generadors d'imatge com Midjourney o DALL·E), i l'ACTIC ja incorpora aquest ús dins de les competències digitals bàsiques que cal dominar amb criteri. Dos principis en resumeixen l'ús responsable, i tots dos apareixen sovint a examen formulats com a situació pràctica.

Revisar-ho sempre

El primer principi és **revisar-ho sempre** abans de donar-ho per bo. Una IA generativa pot produir informació incorrecta amb tota la confiança d'una que és certa, un fenomen que es coneix com a "al·lucinació": inventa una xifra, una data o una referència legal amb el mateix to segur amb què donaria una dada real, sense cap avís que allò podria ser fals.

Per això, si s'utilitza una eina d'intel·ligència artificial generativa per redactar un informe amb dades i xifres concretes, la bona pràctica abans de publicar-lo és contrastar sempre aquestes dades concretes amb una font fiable, precisament perquè la IA pot equivocar-se amb tota la confiança d'una que encerta. Delegar la redacció en una IA no eximeix mai la persona que la fa servir de la responsabilitat sobre allò que finalment es publica o es lliura.

Citar-ho quan correspongui

El segon principi és **citar-ho** quan correspongui. Si un treball incorpora de manera significativa text o imatges generats per una eina d'intel·ligència artificial, la bona pràctica és indicar-ho, exactament igual que se citaria qualsevol altra font externa. Presentar com a producció íntegrament pròpia un contingut generat majoritàriament per una eina externa es considera una forma de manca d'honestedat acadèmica o professional, comparable a no citar un llibre del qual s'ha copiat un fragment.

Drets d'autor i llicències



Aquest bloc pesa molt a l'examen perquè no és gens intuïtiu si no s'ha estudiat expressament: barreja conceptes legals que en el llenguatge del carrer s'utilitzen de manera imprecisa.

Drets morals i drets patrimonials

La propietat intel·lectual d'una obra es divideix en dos grans blocs de drets, de naturalesa molt diferent:

- Els drets **morals**: irrenunciables i intransferibles, és a dir, l'autor no els pot cedir ni vendre mai a ningú, per molt que ho vulgui. Inclouen coses com ser reconegut com a autor de l'obra, o decidir si l'obra es divulga o no.
- Els drets **patrimonials** o d'explotació: la reproducció, la distribució, la comunicació pública i la transformació de l'obra. A diferència dels morals, aquests sí que es poden cedir, vendre o llicenciar a tercers, i a l'Estat espanyol duren, amb caràcter general, tota la vida de l'autor més 70 anys després de la seva mort.

Passat aquest termini de vida de l'autor més 70 anys, l'obra passa a **domini públic** i es pot utilitzar lliurement, sense necessitat de demanar permís ni de pagar res a ningú: qualsevol pot reproduir-la, distribuir-la o adaptar-la.

El copyright existeix des del primer instant

Per defecte, qualsevol obra creada (un text, una fotografia, una il·lustració, una cançó) està protegida per **copyright** des del moment mateix de la seva creació, encara que no dugui cap símbol ni avís explícit: no cal registrar-la enlloc ni escriure-hi "tots els drets reservats" perquè la protecció existeixi.

Aquest és un punt que a la pràctica es passa per alt constantment: agafar una imatge trobada per internet i utilitzar-la sense permís vulnera els drets del seu autor, encara que la pàgina on es trobava no hi digués res al respecte. El silenci d'una pàgina web sobre els drets d'una imatge no vol dir mai que sigui d'ús lliure.

Creative Commons: quatre lletres, sis combinacions

Les llicències **Creative Commons** permeten a l'autor cedir voluntàriament alguns dels seus drets d'explotació, sense renunciar-hi del tot, combinant quatre condicions bàsiques:

- **BY** (Reconeixement): cal citar sempre l'autor original. Present a totes les llicències Creative Commons sense excepció; és l'única condició que mai es pot ometre.
- **NC** (No Comercial): prohibeix explícitament un ús amb finalitat comercial de l'obra.
- **ND** (Sense obra derivada): no es pot modificar l'obra ni fer-ne remescles ni adaptacions; només es pot compartir tal qual, sense tocar-la.
- **SA** (Compartir igual): les obres derivades que se'n facin s'han de llicenciar amb la mateixa llicència original, el que es coneix com a "copyleft". Aquesta condició és incompatible amb ND, perquè no es pot alhora prohibir modificar l'obra (ND) i exigir que les modificacions es comparteixin amb la mateixa llicència (SA): si no es pot modificar, mai n'hi haurà de "modificacions" a compartir.

Combinant aquestes quatre condicions s'obtenen les sis llicències Creative Commons habituals, de la més oberta a la més restrictiva. Una llicència **CC BY-SA**, per exemple, permet usar i modificar l'obra, fins i tot amb finalitat comercial, sempre que es citi l'autor i que les obres derivades es comparteixin amb la mateixa llicència. Una **CC BY-NC-SA** hi afegeix la restricció comercial: permet usar i adaptar l'obra citant l'autor, sempre que no sigui amb finalitat comercial i que el resultat es comparteixi amb la mateixa llicència.

La més oberta de totes és **CC BY**: només cal citar l'autor, i es permet tant l'ús comercial com la modificació sense cap altra restricció. La més restrictiva de les que encara permeten compartir l'obra és **CC BY-NC-ND**: es pot compartir tal qual, citant l'autor, sense finalitat comercial i sense modificar-la gens ("pots



compartir-ho tal qual, citant-me, i prou").

Bancs d'imatges i citació correcta

Per il·lustrar un document o una presentació sense infringir cap dret, els **bancs d'imatges gratuïts** com Unsplash o Pixabay ofereixen fotografies amb llicències molt permissives (sovint equivalents a domini públic o CC0, la variant de Creative Commons que renuncia a tots els drets possibles), pensades per utilitzar-se sense pagar ni, sovint, haver de citar l'autor.

Citar correctament una font vol dir indicar, com a mínim, l'autor, el títol de l'obra i, si escau, l'any i on es va publicar, prou clarament perquè qualsevol lector pugui localitzar l'original. No fer-ho, i fer passar per pròpia una idea, un text o una imatge d'una altra persona, constitueix **plagi**, amb independència de la llicència que protegís l'obra.

Programari lliure vs. propietari

Les quatre llibertats

El programari **lliure** (free software, en el sentit de llibertat, no necessàriament de gratuïtat, un matís que confon molta gent en castellà i en català) garanteix quatre llibertats bàsiques a qui l'utilitza: usar-lo per a qualsevol finalitat, estudiar-ne el codi font per entendre com funciona, modificar-lo per adaptar-lo a les pròpies necessitats, i redistribuir-lo, amb o sense modificacions, a qui vulgui.

LibreOffice, GIMP, Audacity o Linux en són exemples habituals, distribuïts sota llicències com la **GPL** (General Public License), que a més de garantir aquestes quatre llibertats imposa el concepte de **copyleft**: si algú redistribueix una versió modificada d'un programa amb llicència GPL, aquesta versió modificada també ha de mantenir-se lliure, amb el codi font disponible i les mateixes quatre llibertats per a qui la rebí. Aquest mecanisme evita que algú agafi programari lliure, hi afegeixi millores i el torni a vendre com a propietari tancat.

El programari **propietari** (Microsoft Office, Adobe Photoshop) restringeix aquestes quatre llibertats: el codi font no és públic, no es pot estudiar ni modificar legalment, i l'ús es regeix per una llicència que sol requerir el pagament d'una quota, única o periòdica.

Gratuït no és el mateix que lliure

Un matís que l'examen distingeix amb molta cura, i que sovint és font d'error: **gratuït** (freeware) no vol dir lliure. Un programa pot ser completament gratis de descarregar i utilitzar, i tenir alhora el codi tancat, com passa amb molts lectors de PDF que es poden baixar sense pagar però que ningú pot estudiar-ne ni modificar-ne el funcionament intern.

I a l'inrevés: el programari lliure no sempre és gratuït. Es pot cobrar legítimament pel suport tècnic, per la instal·lació o per una còpia física concreta, encara que qui la rep en pugui fer còpies i redistribuir-la lliurement sense cap restricció legal, cosa que mai passaria amb programari propietari de pagament: preu i llibertat són dos eixos independents entre si.

Algorismes i automatització

Què és un algorisme

Un **algorisme** és una seqüència finita i ordenada de passos per resoldre un problema concret o completar una tasca determinada. No cal saber programació per parlar-ne: una recepta de cuina n'és un bon



exemple quotidià, perquè indica passos concrets, en un ordre concret, que porten des d'uns ingredients inicials fins a un plat acabat.

Representar-lo: pseudocodi i diagrames de flux

Un algorisme es pot representar de dues maneres habituals:

- **Pseudocodi:** un llenguatge proper al natural, però escrit de manera estructurada (amb condicions del tipus "si... aleshores...", bucles del tipus "mentre... fes..."), pensat per descriure la lògica d'un procés sense encara escriure'l en un llenguatge de programació real.
- **Diagrama de flux:** una representació gràfica amb símbols estandarditzats que cal reconèixer:
- **Òval:** marca l'inici o el final del procés.
- **Rectangle:** representa un procés o una acció concreta.
- **Rombe:** representa una decisió o bifurcació (una pregunta amb resposta sí/no que porta el flux per un camí o un altre).
- **Paralelogram:** representa l'entrada o la sortida de dades (per exemple, demanar un valor a l'usuari, o mostrar un resultat).

Macros: automatitzar tasques repetitives

A nivell d'ofimàtica, l'automatització es materialitza sobretot en les **macros**: una seqüència d'accions gravada o programada que s'executa sencera amb un sol clic o una drecera de teclat, en comptes de repetir manualment els mateixos passos cada vegada.

A **LibreOffice** s'escriuen en el llenguatge LibreOffice Basic, accessible des d'Eines>Macros. A **Microsoft Office** s'escriuen en VBA (Visual Basic for Applications), amb un editor propi accessible des de la pestanya Desenvolupador.

Pas a pas per gravar una macro senzilla a LibreOffice: Eines>Macros>Grava una macro; realitza normalment els passos que vols automatitzar (per exemple, seleccionar una taula acabada d'enganxar, aplicar-hi vores, posar la capçalera en negreta i ajustar l'amplada de les columnes); atura la gravació des del quadre flotant que apareix mentre grava; desa la macro amb un nom identificable; i assigna-la a un botó de la barra d'eines o a una drecera de teclat (Eines>Personalitza>pestanya Teclat o Barres d'eines), perquè la propera vegada n'hi hagi prou amb un clic, sense refer els passos manualment. Aquest exemple, formatar automàticament una taula acabada d'enganxar amb una drecera, és el cas típic d'examen sobre automatització ofimàtica amb macros.

**4**

TEMA

Àrea 4. Seguretat**Contrasenyes, identitat digital i comptes robats**

La contrasenya segueix sent el punt més feble de qualsevol compte, i és per aquí per on comença gairebé sempre un disgust digital. Una contrasenya robusta no es defineix només per tenir majúscules, números i símbols barrejats sense sentit -això la fa difícil de recordar i fàcil d'oblidar, i sovint acaba apuntada en un post-it enganxat a la pantalla, que és exactament el contrari de segur-, sinó per la longitud i la manca de patrons previsibles: una frase llarga com "elgosmenjattressandvitxosdimarts" és més segura que "P@ssw0rd1" i molt més fàcil de retenir. Una altra manera de construir-ne una és encadenar tres o quatre paraules que no tinguin cap relació entre elles, com "taronja-bicicleta-37-núvol": no cal que tingui sentit gramatical, només que sigui llarga i que no es pugui deduir de les nostres dades personals (el nom del gos, la data de naixement, el barri on vivim). El problema real no és triar una contrasenya bona, sinó no repetir-la mai entre serveis: si Netflix pateix una fuga i fem servir la mateixa clau al correu, l'atacant ja té accés al correu. Un error molt habitual, i que dona una falsa sensació de seguretat, és fer servir la mateixa contrasenya de base i anar-la variant amb un número al final -Estiu2023, Estiu2024, Estiu2025-: si un atacant en descobreix una, endevinar les altres és qüestió de segons.

Gestors de contrasenyes: com posar-ne un en marxa

Aquí és on entren els gestors de contrasenyes com Bitwarden, 1Password o el gestor integrat del navegador. Funcionen guardant totes les nostres contrasenyes xifrades dins d'una "caixa forta" digital que només es pot obrir amb una única contrasenya mestra; el xifratge es fa al mateix dispositiu, de manera que ni tan sols l'empresa que ofereix el servei pot veure què hi ha desat (és el que s'anomena xifratge de coneixement zero). A partir d'aquí, el gestor pot generar contrasenyes llargues i aleatòries per a cada lloc nou i emplenar-les automàticament, de manera que l'usuari només ha de recordar una contrasenya en lloc de cinquanta. Això elimina el problema de la reutilització sense obligar ningú a memoritzar res impossible.

Posar-ne un en marxa és més senzill del que sembla i val la pena fer-ho amb calma la primera vegada:

1. Obre el navegador (Chrome, per exemple), ves al Chrome Web Store i cerca "Bitwarden - Free Password Manager".
2. Clica "Afegir a Chrome" per instal·lar l'extensió; apareixerà una icona de l'escut a la barra superior.
3. Crea un compte nou amb el teu correu i defineix la contrasenya mestra: llarga, memoritzable, i que no facis servir enlloc més.
4. La propera vegada que et registris en un servei nou -posem per cas l'oficina virtual d'una companyia elèctrica per consultar la factura de la llum-, deixa que Bitwarden et proposi una contrasenya generada (la icona en forma de dau o clau al formulari) en lloc d'escriure'n una de collita pròpia.
5. Al mòbil, instal·la també l'app i activa el desbloqueig per empremta digital o reconeixement facial, perquè no calgui teclejar la mestra cada vegada.
6. De tant en tant, fes una exportació xifrada de la caixa forta com a còpia de seguretat, per si mai perdessis l'accés al compte del gestor.

Per a molts tràmits amb l'Administració catalana i espanyola, la identitat digital va un pas més enllà de la contrasenya del correu: sistemes com Cl@ve o l'idCAT Mòbil permeten identificar-se davant la seu



electrònica de l'ajuntament, la Seguretat Social o el CatSalut sense necessitat de certificat digital instal·lat, fent servir un usuari i contrasenya propis combinats amb un codi que arriba al mòbil. La lògica de fons és la mateixa que la del 2FA: una contrasenya sola no n'hi ha prou per accedir a tràmits sensibles, com demanar un certificat d'empadronament o consultar l'historial mèdic, i per això aquests sistemes hi afegeixen sempre una segona confirmació.

La verificació en dos passos (2FA o MFA)

La verificació en dos passos afegeix una segona prova d'identitat més enllà de la contrasenya: un codi enviat per SMS, una app d'autenticació (Google Authenticator, Authy, o l'autenticador integrat del gestor de contrasenyes) o una clau física (YubiKey). Encara que algú robi la contrasenya per phishing, no podrà entrar sense aquest segon factor. Val la pena entendre per què el SMS és el mètode menys segur dels tres: el codi viatja per la xarxa telefònica i es pot interceptar mitjançant un duplicat fraudulent de la targeta SIM (SIM swapping), en què l'atacant convenç l'operadora que és el titular de la línia i es fa passar la numeració a una SIM pròpia. Una app d'autenticació, en canvi, genera el codi localment al mòbil a partir d'una clau compartida amb el servei, sense passar per cap xarxa que es pugui interceptar, i una clau física encara ofereix més garanties perquè exigeix tenir l'objecte físicament a la mà.

Activar-la a un compte de Gmail, que és el cas més habitual a l'examen i a la vida real, segueix sempre el mateix camí:

1. Obre Gmail des de l'ordinador i clica la icona rodona del compte, a dalt a la dreta.
2. Selecciona "Gestiona el teu Compte de Google".
3. Ves a la pestanya "Seguretat" del menú de l'esquerra.
4. Dins l'apartat "Com iniciés sessió a Google", clica "Verificació en dos passos" i segueix l'assistent.
5. Tria el mètode: si el servei ho permet, val més escollir una app d'autenticació que el SMS.
6. Guarda els codis de recuperació que ofereix Google en un lloc segur diferent del mòbil (per exemple, imprès o dins el gestor de contrasenyes), per si mai perdessis l'aparell.

Passkeys: la contrasenya que ja no cal recordar

La darrera generació d'aquesta idea són les claus d'accés o passkeys, que comencen a substituir la contrasenya directament. En lloc de memoritzar res, el dispositiu genera una parella de claus criptogràfiques: una de pública, que queda al servidor del servei, i una de privada, que es queda guardada i xifrada al mòbil o l'ordinador, protegida per la petjada digital, la cara o el PIN del dispositiu. Com que la clau privada mai surt del dispositiu i està lligada al domini exacte del servei, una passkey no es pot robar per phishing ni reutilitzar en una pàgina falsa, encara que sigui idèntica a l'original. A la pràctica, entrar amb una passkey a una botiga en línia com Amazon es redueix a prémer "Inicia sessió amb una clau d'accés" i confirmar amb el Face ID o l'empremta: no hi ha res a escriure ni res que un atacant pugui pescar.

Compte robat: el protocol dels primers minuts

Si malgrat totes les precaucions un compte acaba robat, els primers minuts compten, i és molt més fàcil actuar bé si ja se sap d'entrada l'ordre dels passos:

1. Canvia la contrasenya immediatament des d'un altre dispositiu de confiança, no des de l'equip que sospites que pot estar compromès.
2. Revisa i tanca les sessions actives que no reconeguis: a Gmail es fa des de l'apartat "Dispositius" de seguretat, i a Facebook des de "Configuració i privadesa > Configuració > Seguretat i inici de sessió > On has iniciat sessió".



3. Activa la verificació en dos passos si encara no hi era.
4. Revisa les dades de recuperació -correu i telèfon alternatiu- per si l'atacant les ha canviat per intentar bloquejar-nos l'accés definitivament.
5. Si el compte robat és de correu o de xarxa social, avisa els contactes que qualsevol missatge estrany dels darrers dies no és nostre. És habitual que l'atacant l'utilitzi per escriure a amics i familiars fent-se passar per nosaltres i demanant-los diners amb una excusa urgent; un missatge d'avís a temps evita que algú proper acabi fent una transferència a una persona que no és qui diu ser.
6. Per saber si les nostres credencials ja circulen en alguna fuga de dades anterior, existeixen serveis com Have I Been Pwned, on n'hi ha prou d'introduir el correu electrònic per comprovar si ha aparegut en alguna filtració coneguda; si la resposta és afirmativa, la contrasenya d'aquell servei s'ha de canviar sense esperar més.

Amenaces amb nom i cognom: el malware que cal saber distingir

Sota el paraigua de "virus" s'hi amaguen programes maliciosos molt diferents entre si, i l'examen sol demanar distingir-los pel que fan, no només pel nom. Val la pena llegir-se aquest apartat pensant en un cas concret per a cada un, perquè és exactament així com es plantegen les preguntes tipus test.

Ransomware: el segrest dels fitxers

El ransomware xifra en silenci tots els fitxers del dispositiu -documents, fotos, bases de dades- i després mostra un avís demanant un rescab, normalment en criptomoneda, a canvi de la clau per desxifrar-los. Un cas típic: una petita empresa o un ajuntament descobreix un matí que centenars de fitxers dels seus servidors han quedat il·legibles i que a la pantalla hi ha aparegut una nota demanant un pagament en bitcoins amb un compte enrere. Pagar no garanteix recuperar res, perquè no hi ha cap obligació legal que l'atacant compleixi la seva part; per això l'única defensa real és tenir còpies de seguretat fetes abans de l'atac, no després. Si l'examen pregunta quina mesura hauria evitat les conseqüències d'un ransomware, la resposta gairebé sempre és aquesta: disposar de còpies de seguretat prèvies i actualitzades.

Troians: el regal enverinat

Un troià es presenta com un programa legítim i útil -un crack de software per activar gratuïtament una aplicació de pagament, una suposada actualització, un fitxer adjunt amb nom de factura pendent- però, un cop executat, obre una porta del darrere que permet a l'atacant controlar l'equip remotament sense que l'usuari se n'adoni. L'error habitual que el fa possible és obrir adjunts executables (.exe) o documents amb macros sense verificar abans qui els envia i per què; si un correu inesperat porta un adjunt amb nom "factura_pendent" o "activador_gratis", el més prudent és no obrir-lo i confirmar per un altre canal que és legítim.

Spyware i adware: la diferència entre espia i molestar

L'espia o spyware treballa de manera encara més discreta: s'instal·la sense avís i vigila l'activitat de l'usuari (pàgines visitades, credencials introduïdes, fins i tot la càmera o el micròfon en els casos més greus) per enviar aquesta informació a tercers. Un exemple habitual és una app gratuïta d'"estalvi de bateria" o de "neteja de mòbil" descarregada d'una botiga no oficial, que en realitat recull dades de l'usuari en segon pla. L'adware és menys perillós però igual de molest: omple el navegador o el mòbil d'anuncis no desitjats, sovint com a "regal" d'una aplicació gratuïta instal·lada d'una font poc fiable, i en molts casos porta associat algun component d'espionatge que rastreja els hàbits de navegació per vendre'ls a anunciants. La diferència que cal recordar per a l'examen és senzilla: l'spyware vigila i informa a tercers en silenci,



l'adware sobretot omple el dispositiu d'anuncis.

Keyloggers: cada tecla, apuntada

El keylogger, finalment, registra cada tecla que es prem al teclat; com que això inclou contrasenyes, números de targeta i missatges sencers, és una de les eines preferides per robar credencials sense necessitat de cap engany previ, només amb la infecció de l'equip. És per aquesta amenaça, entre altres, que alguns bancs ofereixen un teclat virtual en pantalla per introduir el PIN o la contrasenya de l'operació: en clicar amb el ratolí en lloc de teclejar, un keylogger tradicional no pot capturar res.

Com entra el malware a l'equip

Més enllà del cas concret del troià o del ransomware, val la pena tenir clars els camins d'entrada més habituals, perquè coincideixen en la majoria de casos: un adjunt de correu que s'obre sense comprovar el remitent, un enllaç de descàrrega d'un programa "gratuït" obtingut fora de la botiga oficial, un llapis USB d'origen desconegut que es connecta directament sense escanejar-lo abans, o una aplicació mòbil instal·lada des d'una font que no és Google Play ni l'App Store. En tots aquests casos, el patró es repeteix: l'usuari executa alguna cosa -fitxer, programa, aplicació- sense haver-ne verificat prou bé la procedència, i és exactament aquest pas el que cal aturar-se a pensar abans de fer.

Un truc per a l'examen

Quan una pregunta descriu una situació -fitxers xifrats amb missatge de rescat, un "crack" que dona control remot a un desconegut, anuncis que envaeixen el navegador, o un programa que registra tot el que s'escriu- el que es demana és identificar quin tipus de malware hi ha darrere, no recitar la definició de memòria. Val la pena fixar-se sempre en l'acció concreta que fa el programa: xifra i demana rescat (ransomware), s'amaga dins d'un altre programa aparentment útil (troià), vigila i envia dades (spyware), inunda d'anuncis (adware) o registra les tecles (keylogger).

Enginyeria social: per què funcionen els enganys

Cap d'aquests programes maliciosos necessita forçar res si l'usuari li obre la porta ell mateix, i aquí és on entra l'enginyeria social: la manipulació psicològica que porta algú a fer alguna cosa que normalment no faria (clicar un enllaç, revelar una contrasenya, autoritzar un pagament).

Els mecanismes que fa servir

Funciona perquè juga amb reaccions automàtiques: la urgència ("el compte es bloquejarà en 24 hores"), l'autoritat (fer-se passar per un càrrec superior, la policia o el banc) i la por o la cobdícia (un premi, una multa, un paquet retingut). Com més pressió psicològica es genera, menys temps té la víctima per pensar-s'ho, i és exactament això el que busca l'atac: que actuem abans de raonar.

Phishing: com identificar-lo pas a pas

El phishing és, amb diferència, l'engany més habitual: un correu o missatge que suplanta un banc, una empresa de missatgeria o fins i tot un company de feina, i que busca que la víctima cliqui un enllaç i introdueixi credencials en una pàgina falsa idèntica a l'original. Un cas molt típic: arriba un correu que sembla d'Hisenda demanant confirmar les dades bancàries fent clic en un enllaç per rebre una devolució. Davant d'un missatge així, la manera correcta de comprovar-lo és sempre la mateixa:

1. Mira el remitent complet, no només el nom que es mostra en gran: sovint l'adreça real, després del símbol @, no coincideix ni de lluny amb el domini oficial de l'entitat.



2. Passa el punter del ratolí per sobre de l'enllaç sense clicar-hi: el navegador mostrarà a la part inferior l'adreça real a la qual portaria, que sol ser ben diferent de la que diu el text visible.

3. Fixa't en errors d'ortografia, traduccions estranyes o un to genèric ("Benvolgut client" en lloc del teu nom).

4. Si tens qualsevol dubte, no cliquis l'enllaç del correu: obre el navegador tu mateix i escriu directament l'adreça oficial (per exemple, la seu electrònica de l'Agència Tributària), o truca al telèfon d'atenció que ja coneixies d'abans.

5. Si ja has clicat i has introduït dades abans d'adonar-te'n, canvia la contrasenya del servei immediatament i activa la verificació en dos passos.

Els senyals d'alarma solen repetir-se sempre: urgència artificial, un remitent que no coincideix exactament amb el domini oficial, i enllaços que, en passar-hi el ratolí per sobre, mostren una adreça diferent de la que diu el text.

Una variant relativament recent és el quishing, el phishing fet a través d'un codi QR: en lloc d'un enllaç clicable, l'engany arriba com un codi imprès (per exemple, enganxat sobre l'etiqueta legítima d'un parquímetre, o en un fals cartell de "paga aquí" en un aparcament) que, en escanejar-lo amb la càmera del mòbil, porta a una pàgina de pagament falsa. Com que el text de l'adreça no es veu fins després d'escanejar, val la pena parar-se a llegir la URL que mostra el mòbil abans de continuar, exactament igual que es faria amb un enllaç d'un correu.

Smishing i vishing: el phishing que truca i escriu

Les variants per mòbil tenen nom propi: el smishing arriba per SMS, típicament simulant una empresa de paqueteria que reclama un pagament pendent per alliberar un paquet retingut, i el vishing és l'estafa per trucada de veu, sovint fent-se passar pel servei tècnic d'un banc, que fins i tot pot arribar a demanar que es confirmi en veu alta un codi que s'acaba de rebre per SMS -codi que, en realitat, és el que l'atacant necessita per validar una operació que ell mateix ha iniciat. La regla pràctica és la mateixa sempre, per correu, SMS o trucada: cap entitat seriosa demana mai la contrasenya o el codi de verificació per cap d'aquests canals.

Frau del CEO i frau de la doble factura

En l'àmbit laboral, l'enginyeria social pren dues formes clàssiques que val la pena conèixer encara que semblin d'empresa gran. El frau del CEO consisteix a suplantar per correu, i cada cop més també per veu clonada amb intel·ligència artificial, un directiu de l'empresa que demana a algú del departament financer una transferència urgent i confidencial, jugant amb la jerarquia perquè ningú gosi qüestionar l'ordre. El frau de la doble factura, o de canvi de compte, actua sobre una relació comercial real: l'atacant intercepta el correu entre proveïdor i client, i just abans de pagar una factura legítima -imaginem una empresa que ha comprat maquinària a un proveïdor habitual- n'envia una còpia gairebé idèntica amb el número de compte bancari canviat, de manera que el pagament arriba a l'estafador i no al proveïdor real. En tots dos casos, el remei és el mateix: verificar per un canal diferent, com ara una trucada al número ja conegut del proveïdor o del directiu, mai al que apareix al correu sospitos, abans de moure diners.

Estafes entre particulars: Wallapop i Bizum

Les operacions entre particulars, com les de Wallapop, tenen la seva pròpia variant, i sol confondre fins i tot gent atenta. La regla d'or és senzilla: qui envia diners no els sol·licita. Si véns un article i el comprador diu que ja t'ha pagat i que rebràs una notificació de Bizum per "acceptar" o "confirmar" el pagament, en realitat el que t'arriba és una sol·licitud de diners: si la confirmes, series tu qui li envia els diners a ell, no al



revés. Un pagament real de Bizum no necessita cap acceptació per part de qui el rep; només cal comprovar-lo directament dins l'app del banc, mai a través d'una notificació que demana confirmar res. La variant de l'estafa del pagament excessiu (overpayment scam) funciona de manera semblant: el comprador diu que ha enviat més diners dels acordats "per error" i demana que se li retorni la diferència per un altre mitjà, quan en realitat el primer pagament és fals o s'acabarà retirant al cap d'uns dies, i qui ha "retornat" la diferència perd els diners de debò.

Protecció activa del dispositiu

Un ordinador o un mòbil sense manteniment és una porta oberta. Aquest apartat repassa les quatre capes de defensa que treballen millor quan actuen totes alhora: tallafoc, antivirus, actualitzacions i còpies de seguretat.

El tallafoc: la primera barrera

El tallafoc (firewall) filtra les connexions que entren i surten de l'equip i talla per defecte allò que no s'ha demanat expressament; ve activat de sèrie a Windows i macOS, i desactivar-lo només té sentit en xarxes molt controlades. A Windows es pot comprovar que està actiu anant a Configuració, després a Privadesa i seguretat, i finalment a Seguretat de Windows > Tallafocs i protecció de xarxa, on hauria d'aparèixer en verd per a les tres xarxes (de domini, privada i pública).

Comptes d'usuari i permisos: no treballar sempre com a administrador

Un descuit habitual, sobretot en equips familiars compartits, és fer servir el dia a dia amb un compte d'administrador en lloc d'un compte d'usuari estàndard. Un compte d'administrador pot instal·lar programes i canviar qualsevol configuració del sistema sense demanar més confirmació que la contrasenya inicial; si un malware s'executa mentre s'ha iniciat sessió amb aquest tipus de compte, hereta els mateixos permisos i pot modificar el sistema sencer. Crear un compte estàndard per a l'ús diari, i reservar el d'administrador només per a les tasques que realment ho requereixen (instal·lar programari nou, per exemple), fa que qualsevol intent d'instal·lació no autoritzada topi amb una finestra que demana la contrasenya d'administrador, un últim avís abans que passi res.

L'antivirus: signatures i comportament

L'antivirus, en canvi, treballa amb signatures i comportaments: detecta fitxers maliciosos coneguts i, els més moderns, també patrons sospitosos, com un procés que xifra centenars de fitxers de cop, típic d'un ransomware, o un que registra cada tecla premuda, propi d'un keylogger. Tallafoc i antivirus fan feines diferents i complementàries: un vigila el trànsit de xarxa, l'altre vigila el contingut i el comportament dels fitxers i processos, i és per això que cap dels dos substitueix l'altre.

Actualitzacions: el pedaç que ningú instal·la

Cap dels dos serveis de gaire si el sistema operatiu i les aplicacions no s'actualitzen: la majoria d'atacs no exploten vulnerabilitats desconegudes (els anomenats "zero-day"), sinó forats que ja tenen pedaç publicat des de fa mesos i que ningú ha instal·lat. Activar les actualitzacions automàtiques del sistema operatiu, del navegador i de les aplicacions és, a la pràctica, una de les mesures de seguretat més eficaces i menys costoses que existeixen. A Windows es fa des de Configuració > Windows Update, activant "Rebre actualitzacions per a altres productes Microsoft"; a Android, des de la Play Store, tocant la foto de perfil i entrant a Configuració > Preferència de xarxa > Actualitza les apps automàticament; a l'iPhone, des de Configuració > General > Actualització de programari > Actualitzacions automàtiques.



Còpies de seguretat: la regla 3-2-1

I per molt bon sistema de defensa que hi hagi, res substitueix una còpia de seguretat: la regla 3-2-1 (tres còpies dels arxius, en dos suports diferents, i almenys una fora de la ubicació principal, per exemple al núvol) és l'única resposta real davant un ransomware que xifra tots els fitxers o un robatori del dispositiu. Si les còpies estan connectades permanentment a l'equip infectat, el ransomware també les pot xifrar, per això una de les còpies ha d'estar desconnectada o fora de línia de manera habitual. A la pràctica, això es tradueix en tenir, per exemple, els documents originals a l'ordinador, una còpia en un disc dur extern que només es connecta per fer la còpia i després es desconnecta, i una tercera còpia sincronitzada a un servei al núvol com Google Drive o OneDrive, que ja compleix per si sol la condició d'estar "fora de la ubicació principal".

Xifratge, VPN i wifi públic

Xifratge i HTTPS: el cadenat que cal entendre

El xifratge converteix la informació en un galimaties il·legible per a qui no tingui la clau adequada, i és la base de gran part de la seguretat a internet. El senyal més visible del dia a dia és el cadenat que apareix a la barra d'adreces del navegador i el protocol HTTPS (la "s" final vol dir segur): indica que la comunicació entre el navegador i el servidor viatja xifrada, de manera que ningú que intercepti el trànsit pel camí pot llegir contrasenyes, dades bancàries o el contingut de la pàgina. Cal tenir clar, però, que HTTPS xifra el canal, no garanteix que la pàgina sigui legítima: una web de phishing ben feta també pot tenir el seu cadenat, perquè avui dia és fàcil i gratuït obtenir un certificat de xifratge encara que la pàgina sigui falsa. Per comprovar amb qui parlem realment, es pot clicar el cadenat de la barra d'adreces i mirar el nom del certificat: si diu "Banc Sabadell, S.A." té una garantia diferent que si només indica un domini genèric sense cap identificació de l'entitat.

Val la pena distingir dos conceptes que sovint es confonen a l'examen: la navegació privada o "d'incògnit" del navegador no xifra res ni amaga la connexió davant de la resta del món; només evita que el mateix navegador guardi l'historial, les galetes i les dades del formulari en aquell equip. Qui administra la xarxa (per exemple, la wifi de la feina) o el mateix proveïdor d'internet continua veient per on naveguem, encara que ho fem en mode incògnit. Qui de debò xifra i amaga el trànsit davant de tercers és una VPN, no el mode privat del navegador.

VPN: el túnel cap a un altre lloc

Una VPN (xarxa privada virtual) crea un túnel xifrat entre el dispositiu i un servidor intermedi, de manera que tot el trànsit hi passa amagat de la xarxa local per la qual es connecta l'usuari, i surt a internet amb l'adreça IP d'aquell servidor en lloc de la pròpia. Té sentit fer-la servir en connexions poc fiables, com una wifi pública, o per no exposar la ubicació real en determinats serveis; no és, però, una solució màgica que faci invisible ni immune a tota la resta de riscos, com el phishing o la reutilització de contrasenyes: si es cau en un correu fraudulent i s'hi introdueixen les dades, cap VPN evitarà el robatori. Hi ha dos usos habituals que convé distingir: la VPN personal, contractada per un usuari particular per protegir la seva pròpia connexió, i la VPN corporativa, que una empresa fa servir perquè el personal en teletreball es connecti als seus servidors interns com si fos físicament a l'oficina, amb els mateixos permisos i restriccions.

El router de casa, la porta que sovint s'oblida

La seguretat de la xarxa no comença ni acaba al mòbil o a l'ordinador: el router que dona accés a internet



a tota la llar és sovint l'element més descuidat. Molts routers surten de fàbrica amb una contrasenya d'administració genèrica (com "admin/admin") que mai s'arriba a canviar, i amb la xifra de la xarxa wifi configurada amb el protocol antic WEP o el WPA2 en lloc de l'actual WPA3, més robust. Canviar la contrasenya per defecte del router i assegurar-se que la xarxa wifi de casa fa servir com a mínim WPA2 (idealment WPA3 si el router ho permet) és una mesura senzilla i sovint oblidada que redueix molt el risc que un veí o un desconegut proper s'aprofiti de la connexió o intercepti trànsit.

Wifi públiques: un mateix cable per a tothom

Les xarxes wifi públiques -d'un aeroport, una cafeteria, un hotel- comparteixen el mateix medi entre tots els usuaris connectats, cosa que en fa més fàcil, tot i que no trivial, interceptar trànsit no xifrat o muntar un punt d'accés fals amb un nom gairebé idèntic al legítim (per exemple, "Aeroport_WIFI_Free" al costat del real "Aeroport_WiFi") per capturar les dades de qui s'hi connecti per error. Imaginem algú que, esperant un vol, decideix consultar el compte bancari connectat a la wifi de l'aeroport: si la xarxa no és de confiança i no fa servir cap protecció addicional, aquesta operació és exactament el tipus de risc que cal evitar. La recomanació pràctica és evitar operacions sensibles, com la banca en línia o compres amb targeta, en una wifi pública sense VPN, i confiar més en les dades mòbils, o en una VPN de confiança, quan calgui fer alguna gestió delicada fora de casa. Un altre costum senzill és desactivar la connexió automàtica a xarxes wifi obertes que el mòbil recorda d'altres vegades, perquè un aparell configurat per connectar-se sol a qualsevol xarxa coneguda facilita precisament l'atac del punt d'accés fals.

Dades personals i RGPD a la pràctica

El marc normatiu

El Reglament General de Protecció de Dades (RGPD), en vigor a tota la UE des del 2018, i la llei orgànica espanyola que el desplega, la LOPDGDD (Llei Orgànica de Protecció de Dades i Garantia de Drets Digitals), regulen com les empreses i administracions poden tractar les nostres dades. La LOPDGDD no és una llei independent del RGPD, sinó que l'adapta a l'ordenament espanyol i hi afegeix drets digitals nous, com el testament digital, que el reglament europeu no preveia expressament. Qualsevol empresa o administració que tracti dades personals ha de poder explicar, si li ho demanen, amb quina finalitat ho fa, durant quant de temps les conservarà i a qui les podrà cedir; aquesta informació sol trobar-se a la "Política de privacitat" del peu de qualsevol web seriosa, i llegir-la per damunt abans d'acceptar-la és un hàbit que val la pena agafar, sobretot quan es tracta d'una app nova que demana molts permisos.

Les organitzacions que tracten dades a gran escala o dades de categories especials de manera habitual (un hospital, una asseguradora, un ajuntament) han de comptar amb un delegat de protecció de dades (DPD, o DPO per les sigles en anglès), una figura encarregada de vetllar pel compliment de la normativa i que fa d'enllaç entre l'organització, els ciutadans i l'autoritat de control. Aquestes mateixes organitzacions han de mantenir un registre d'activitats de tractament, un document intern on queda anotat quines dades es tracten, amb quina finalitat i quines mesures de seguretat s'apliquen.

Dades ordinàries i categories especials

No totes les dades es tracten igual: la normativa distingeix les dades personals corrents (nom, correu, telèfon) de les categories especials, que mereixen una protecció reforçada perquè un mal ús pot tenir conseqüències greus per a la persona: dades de salut, origen ètnic, ideologia política, creences religioses, orientació sexual o dades biomètriques com l'empremta o el reconeixement facial. El tractament d'aquestes dades exigeix, en general, un consentiment exprés i motius més estrictes que les dades



ordinàries.

El consentiment vàlid

El consentiment és, precisament, l'altre concepte clau: perquè sigui vàlid ha de ser lliure, informat, específic i inequívoc, i cal poder retirar-lo amb la mateixa facilitat amb què es va donar; una casella premarcada per defecte no compleix aquest requisit, perquè no reflecteix una decisió activa de la persona.

Els drets ARCO i la seva ampliació a ARSOPOL

Els drets clàssics es coneixien com a ARCO: Accés (saber quines dades es tenen de nosaltres), Rectificació (corregir-les si són errònies), Cancel·lació (demanar que s'esborrin) i Oposició (negar-nos a un tractament concret, per exemple publicitat). La normativa actual els ha ampliat i reagrupat sota la sigla ARSOPOL, que inclou Accés, Rectificació, Supressió (l'evolució del dret de cancel·lació), Oposició, Portabilitat i Limitació del tractament. A la pràctica, exercir-los és senzill: la portabilitat permet endur-se les dades d'un servei a un altre, per exemple exportar els contactes i correus d'un proveïdor per traslladar-los a un altre; la limitació permet demanar que unes dades es conservin però no es facin servir mentre es resol una discrepància; i drets digitals afegits per la LOPDGDD, com el dret a l'oblit (que un cercador desindexi informació desactualitzada sobre nosaltres) o el testament digital (designar qui podrà gestionar els nostres perfils i comptes després de morir), completen el quadre.

Exercir el dret d'accés davant una administració, per exemple per saber quines dades té l'ajuntament sobre nosaltres al padró municipal, segueix un camí semblant al de qualsevol altre organisme:

1. Localitza el formulari d'"Exercici de drets RGPD" o "Protecció de dades", que sol estar al peu de la web o dins la política de privacitat.
2. Omple'l identificant-te amb el DNI o NIF.
3. Especifica quin dret vols exercir -en aquest cas, l'accés- i, si es demana, adjunta una còpia del document d'identitat per confirmar que ets tu qui ho sol·licita.
4. Envia la sol·licitud i guarda'n el justificant de registre.
5. L'organisme té, amb caràcter general, un mes de termini per respondre.

Exercir el dret d'oposició, per exemple per deixar de rebre publicitat d'una botiga en línia on es va comprar una vegada, sol ser encara més senzill a la pràctica que la resta de drets: la majoria de comunicacions comercials per correu inclouen al final un enllaç de "Donar-se de baixa" o "Deixar de rebre aquests correus", que permet exercir l'oposició amb un sol clic sense necessitat d'omplir cap formulari ni d'esperar cap termini de resposta.

Fuites de dades i reclamacions

Si una empresa pateix una fuga de dades que ens afecta, té l'obligació de notificar-ho a l'autoritat de control en un termini de 72 hores des que en té coneixement, i també als usuaris afectats si el risc per a ells és alt. Com a usuaris, si detectem un ús indegut de les nostres dades o una empresa no atén una sol·licitud de drets en el termini establert, es pot presentar una reclamació davant l'Agència Espanyola de Protecció de Dades (AEPD) o, a Catalunya, davant l'Autoritat Catalana de Protecció de Dades (APDCAT), totes dues gratuïtes i tramitables en línia.

Cookies: petits fitxers que recorden més del que sembla

A la pràctica diària, la privacitat es juga en detalls petits i repetitius. Les cookies són fitxers que les pàgines web guarden al navegador per recordar preferències o, en el cas de les cookies de tercers, per rastrejar la navegació entre webs diferents amb finalitats publicitàries; la normativa obliga a mostrar un avís que



permeti acceptar-les, rebutjar-les o configurar-les per categories abans de navegar, i val la pena parar-hi atenció en lloc de clicar sempre "acceptar totes" per pressa. Al navegador Chrome, es pot ajustar la política de cookies de manera general seguint aquests passos:

1. Obre Chrome i clica les tres línies o els tres punts verticals de dalt a la dreta, i entra a Configuració.
2. Ves a l'apartat "Privadesa i seguretat".
3. Selecciona "Galetes i altres dades de llocs".
4. Tria l'opció de bloquejar les galetes de tercers, en lloc de permetre-les totes per defecte.

Un exemple del dia a dia: en entrar per primer cop a la web d'un diari en línia per llegir una notícia, sol aparèixer un avís amb tres opcions, "Acceptar", "Rebutjar" i "Configurar". Clicar sempre "Acceptar" per pressa vol dir consentir que desenes d'empreses de publicitat que no coneixem rebin dades de la nostra navegació; entrar a "Configurar" i desmarcar les categories que no siguin estrictament necessàries triga uns segons més però és l'única manera real d'exercir el control que la normativa preveu.

Permisos de les aplicacions al mòbil

Als mòbils, revisar quins permisos té concedits cada aplicació -ubicació, contactes, càmera, micròfon, emmagatzematge- i retirar els que no tenen relació amb la funció real de l'app és una tasca de manteniment, no una configuració que es fa un cop i ja està. Una aplicació de llanterna que demana accés als contactes i al micròfon n'és un senyal clar d'alarma, perquè cap d'aquests permisos té res a veure amb encendre una llum. Per revisar-ho a Android, cal anar a Configuració > Aplicacions, triar l'app en concret i entrar a "Permisos"; a l'iPhone, es fa des de Configuració, baixant fins a trobar l'aplicació desitjada i obrint el seu apartat de permisos.

Menors i col·lectius vulnerables

El control parental, sense substituir la conversa

El control parental permet als adults responsables limitar el temps de pantalla, filtrar continguts no adequats per edat i supervisar amb quines aplicacions o contactes interactua un menor, sense que això substitueixi la conversa i l'acompanyament: cap eina tècnica és infal·lible si no va acompanyada d'educació digital. A l'iPhone, es configura des de Configuració > Temps de pantalla, activant l'opció i definint "Restriccions de contingut i privadesa"; a Android, l'eina habitual és Family Link, que s'instal·la com a aplicació, es vincula al compte de Google del menor i permet establir límits d'ús, aprovar aplicacions noves i veure la ubicació del dispositiu.

Grooming: la confiança guanyada per fer mal

El grooming és el procés pel qual un adult s'aproxima a un menor en línia amb intenció d'abús, guanyant-se primer la seva confiança durant dies o setmanes abans de demanar-li contingut íntim o quedar en persona. Sol començar en un joc en línia, una xarxa social o una app de missatgeria, amb un perfil que pot fins i tot fer-se passar per algú de la mateixa edat que el menor; els senyals que haurien d'encendre l'alarma en una família són un adult desconegut que insisteix a passar la conversa a un canal privat, que demana secretisme explícit ("no ho diguis als teus pares") o que regala diners, jocs o crèdits a canvi de fotografies.

Un concepte relacionat, però diferent, és el sexting: l'enviament voluntari d'imatges íntimes pròpies entre persones, sovint dins una relació de confiança entre iguals. No és, en si mateix, un delictes ni un abús, però comporta un risc real si aquell contingut es reenvia sense consentiment o si la relació de confiança es



trenca, perquè un cop una imatge surt del dispositiu original ja no es pot controlar on acaba.

Sextorsió: quan el contingut ja existeix

Quan aquell contingut íntim ja existeix i algú l'utilitza per amenaçar la víctima, exigint més imatges, diners o qualsevol altra cosa a canvi de no difondre'l, es parla de sextorsió. La diferència amb el grooming és, doncs, el punt de partida: el grooming busca aconseguir contingut íntim guanyant-se abans la confiança de la víctima, mentre que la sextorsió parteix d'un contingut que ja existeix per amenaçar i exigir-hi més coses a canvi de no difondre'l. En els dos casos, l'actuació correcta és la mateixa: no cedir mai al xantatge (pagar o enviar més imatges només confirma a l'atacant que la víctima cedeix, i sol demanar-ne més), tallar el contacte, conservar totes les proves (captures de pantalla de les converses, sense esborrar res) i denunciar-ho, tant a la plataforma on ha passat com a les Forces i Cossos de Seguretat.

Ciberassetjament entre iguals

El ciberassetjament o cyberbullying entre iguals, quan es difonen imatges o comentaris humiliants d'algú a través de xarxes o grups de missatgeria, es documenta i es denuncia de la mateixa manera: captures de pantalla amb data i hora visibles, mai respondre a l'assetjador ni esborrar les converses per "no haver de veure-les més", perquè són la prova que després permetrà actuar. A Catalunya, els Mossos d'Esquadra tenen canals específics de denúncia per a delictes tecnològics, i entitats com Internet Segura for Kids (IS4K) o la línia d'ajuda 116111 ofereixen orientació tant a menors com a famílies davant d'aquestes situacions.

Salut digital

Ergonomia i la regla 20-20-20

L'ús intensiu de pantalles té un cost físic que sovint es passa per alt. Una posició de treball correcta situa la part superior de la pantalla a l'alçada dels ulls, l'esquena recolzada i els avantbraços paral·lels al terra; la regla 20-20-20 (cada 20 minuts, mirar 20 segons a 20 peus de distància, uns 6 metres) ajuda a descansar la vista i prevenir la síndrome visual informàtica, que es manifesta amb ulls secs, visió borrosa temporal i mals de cap.

Una cadira amb suport lumbar, els peus recolzats pla a terra (o sobre un reposapeus si la taula és massa alta) i el ratolí a la mateixa alçada que el teclat, sense haver d'aixecar l'espatlla per fer-lo servir, completen una postura de treball correcta i redueixen les molèsties cervicals i d'esquena que apareixen amb hores de pantalla acumulades.

Llum blava, son i desconexió

Més enllà de l'ergonomia, hi ha una dimensió d'ús saludable relacionada directament amb el son: la llum blava de les pantalles interfereix en la producció de melatonina, l'hormona que regula el son, i per això es recomana evitar mòbils, tauletes i ordinadors almenys mitja hora abans d'anar a dormir. La majoria de sistemes operatius inclouen una eina per atenuar aquesta llum blava a les hores de vespre: a Windows es diu "Llum nocturna" i es configura des de Configuració > Sistema > Pantalla, activant l'interruptor i programant l'horari; a l'iPhone s'anomena "Night Shift" i es troba a Configuració > Pantalla i brillantor, on també es pot programar perquè s'activi automàticament de la posta a la sortida del sol. Aquestes eines suavitzen l'efecte, però no el eliminen del tot: l'hàbit que realment ajuda és deixar de mirar pantalles una estona abans de ficar-se al llit, no només canviar-ne el to de color.

Establir límits d'horari i mantenir espais i moments sense connexió -els àpats, per exemple, o la primera



mitja hora del matí- és el que s'entén per desconexió digital, i cada cop es reconeix més com una necessitat, no com un luxe.

Ús problemàtic de la tecnologia

L'ús problemàtic de la tecnologia, com comprovar el mòbil de manera compulsiva sense un motiu concret o sentir ansietat notable en no tenir-lo a mà, es reconeix cada cop més com un problema de salut real, i no només com una manera de dir "hi passo massa estona". Les mateixes eines dels dispositius, com el temps de pantalla o els límits d'ús per app, són un primer pas útil per posar-hi consciència i límits, encara que no substitueixin ajuda professional en els casos més severos.

Sostenibilitat digital: el cost ambiental de la xarxa

La petjada de carboni del que sembla immaterial

El món digital sembla immaterial, però no ho és: cada correu, cada cerca i cada vídeo en streaming consumeix electricitat als centres de dades que els processen i emmagatzemen, i aquesta energia té una petjada de carboni associada. Deixar el vídeo en definició estàndard en lloc de 4K quan no cal veure'l amb tot detall, esborrar correus i arxius que ja no fan falta, sobretot els adjunts pesants duplicats en desenes de carpetes, i limitar l'emmagatzematge automàtic al núvol de fotos i vídeos que mai es tornaran a mirar són gestos petits amb impacte real agregat.

Fer aquesta neteja a Gmail és una tasca senzilla que poca gent fa mai:

1. Obre Gmail i, al camp de cerca, escriu "has:attachment larger:10M" per localitzar els correus amb adjunts de més de 10 MB.
2. Revisa la llista i esborra els que ja no facin falta, com factures o presentacions duplicades que ja es tenen desades en un altre lloc.
3. Buida la carpeta de paperera i la de correu brossa, perquè fins que no es buiden els fitxers segueixen ocupant espai al servidor.
4. A Google Drive, ves a "Emmagatzematge" al menú de l'esquerra per veure quins fitxers ocupen més espai i decidir quins es poden eliminar.

Residus electrònics i obsolescència programada

Els residus electrònics (e-waste) són el tipus de residu que creix més ràpid al món: mòbils, ordinadors i carregadors que es llencen abans d'hora, sovint per obsolescència programada -quan un dispositiu deixa de rebre actualitzacions o una bateria no es pot substituir- més que per avaria real. Un cas habitual: un mòbil que al cap de pocs anys deixa de rebre actualitzacions de seguretat i, a més, té la bateria enganxada de manera que no es pot canviar, cosa que acaba obligant l'usuari a comprar-ne un de nou abans del que seria realment necessari.

Reparar, reacondicionar, reciclar

Davant d'un dispositiu que falla, val la pena preguntar-se primer si es pot reparar -canviar una bateria o una pantalla trencada allarga la vida útil molts anys- abans de substituir-lo directament per un de nou; comprar reacondicionat és una altra manera d'allargar el cicle de vida dels aparells sense generar-ne de nous. Quan un dispositiu ja no té solució, portar-lo a un punt net o a un punt de recollida específic de residus electrònics, mai a la brossa general, és la pràctica que la normativa i els cursos d'ACTIC posen com a exemple de consum digital responsable. Els aparells electrònics contenen metalls pesants i materials tòxics que, si acaben en un abocador convencional, contaminen sòl i aigua; per contra, un bon



reciclatge permet recuperar materials valuosos, com or, coure o liti, que d'altra manera caldria extreure de nou. Estalviar energia també passa per gestos senzills: apagar els dispositius en lloc de deixar-los sempre en repòs, desconnectar carregadors que no s'estan fent servir i aprofitar els modes d'estalvi d'energia que porten de sèrie ordinadors i mòbils.

Per a l'examen

Aquesta àrea combina preguntes de concepte, com què és el RGPD o què significa 2FA, amb preguntes de cas pràctic per identificar un correu de phishing, distingir un troià d'un keylogger o triar la resposta correcta davant un missatge sospitos o una sol·licitud de Bizum estranya. Val la pena fixar-se en els matisos: no és el mateix un antivirus que un tallafoc, ni el phishing que el smishing o el vishing, ni els drets ARCO clàssics que la seva evolució ARSOPOL amb la portabilitat i la limitació. Convé tenir clar també per què una app d'autenticació és més segura que un SMS, per què HTTPS xifra el canal però no garanteix que la web sigui de confiança, i la diferència entre grooming i sextorsió, o entre control parental i simple supervisió. Als exàmens tipus test de l'ACTIC sol aparèixer algun cas concret -un correu, una situació a la feina, una configuració de xarxa social- on cal aplicar el concepte, no només recitar-lo; llegeix sempre l'enunciat pensant "quina acció concreta es descriu aquí" abans de mirar les opcions de resposta.

Una manera senzilla de repassar abans de l'examen és recórrer mentalment un dia normal i identificar, a cada pas, quin concepte d'aquesta àrea hi apareix: obrir el correu al matí (phishing, remitent, enllaços), entrar al banc en línia (HTTPS, 2FA, wifi pública), rebre una trucada estranya (vishing), vendre alguna cosa per Wallapop (Bizum, pagament excessiu), acceptar les galetes d'una web (RGPD, consentiment), instal·lar una app al mòbil (permisos, spyware), i acabar el dia amb el mòbil al llit (llum blava, desconnexió digital). Si per a cada situació es pot explicar amb paraules pròpies què cal fer i per què, la part conceptual de l'àrea 4 ja queda coberta amb escriure.

**5****TEMA****Àrea 5. Resolució de problemes****Diagnosticar l'avaria: separar el problema en capes**

El gran error quan alguna cosa falla és començar a provar coses a l'atzar: desendollar, reiniciar, tornar a instal·lar, tot alhora i sense ordre. Un mètode senzill que funciona sempre és separar el problema en capes: és l'aparell (maquinari), és el programa (programari) o és la connexió (xarxa)? Si l'ordinador no engega, mira primer l'alimentació (endoll, bateria, llum indicadora). Si engega però un programa concret falla, el problema sol ser de programari: reinicia el programa, després l'equip. Si el que falla és Internet, comprova en aquest ordre: el dispositiu (el mòbil amb dades funciona?), el router (llums enceses, cable connectat, reinici del router) i, si res funciona, l'operadora (avaria general a la zona). Aquest ordre, de més proper a més llunyà, és el que et demanaran a la prova: no comences trucant al servei tècnic sense haver reiniciat res.

Separar per capes també vol dir saber quin element és el sospitós més probable abans de tocar res. Un ordinador que no s'engega mai, que no fa ni un so ni encén cap llum quan prems el botó, apunta a maquinari (font d'alimentació, bateria, un cable mal connectat). Un que s'engega amb normalitat, amb el ventilador i les llums funcionant, però un sol programa falla mentre la resta van bé, apunta a programari d'aquell programa concret. I un cas que sol confondre a l'examen és aquest: l'ordinador engega perfectament, sents el ventilador, veus la llum d'encesa, però la pantalla es queda negra i no s'hi veu res. Aquí el dubte no és si l'ordinador funciona (sí que funciona), sinó si la pantalla en si rep senyal: comprova el cable de vídeo, un altre monitor si en tens a mà, o si es tracta d'un portàtil, si la imatge apareix connectant una pantalla externa. Aquest exemple -una pantalla que no s'encén tot i que l'ordinador estigui engegat- és el cas de manual d'un problema clarament de maquinari i no de programari: el sistema operatiu ni tan sols ha pogut arribar a mostrar res, perquè la peça física que hauria de mostrar-ho no rep o no transmet la imatge.

Confondre les capes fa perdre temps: reinstal·lar un programa quan el problema és el router no soluciona res, igual que trucar a l'operadora quan el que falla és només el mòbil (per exemple, perquè té el mode avió activat sense voler). Per això la primera pregunta davant de qualsevol avaria no hauria de ser "què faig ara?" sinó "en quina capa és més probable que estigui el problema?".

Abans de reiniciar: guarda el missatge d'error

Hi ha un reflex molt estès i que sol jugar en contra: en veure una pantalla d'error o una "pantalla blava" (el missatge que a Windows indica una fallada greu del sistema), la reacció automàtica de molta gent és reiniciar l'ordinador de seguida per fer-lo desaparèixer. Abans de fer-ho, val la pena aturar-se un moment i anotar o fotografiar amb el mòbil el codi d'error que apareix en pantalla. Aquest codi (una combinació de lletres i xifres, o un missatge curt com "memòria insuficient" o un nom de fitxer del sistema) és exactament la informació que un servei tècnic necessitarà per identificar la causa real, i que un cop reiniciat l'ordinador és molt més difícil de recuperar. És el mateix criteri que explicarem més endavant per demanar ajuda bé: com més concret siguis sobre què ha passat exactament, més ràpid es resol el problema. Reiniciar sense mirar el missatge no és dolent en si (de fet, sovint cal fer-ho), però fer-ho sense abans llegir què diu la pantalla és perdre una informació que després costa d'obtenir.



Reproduir l'error, entendre'l i el gestor de tasques

Comprovar si l'error es repeteix

Un pas que sovint es passa per alt és intentar reproduir l'error abans de fer res més. Si un programa ha fallat una vegada, val la pena repetir la mateixa acció per veure si torna a passar: si es repeteix sempre igual, el problema és consistent i molt més fàcil de descriure a un tècnic (i normalment també més fàcil de solucionar, perquè es pot aïllar el pas exacte que el provoca); si només passa de tant en tant, probablement hi ha un factor extern (memòria plena, un altre programa obert alhora, una xarxa inestable) que cal identificar. Un error que "de vegades passa i de vegades no" no és menys real que un de constant, però es diagnostica diferent: en el cas consistent, tens una recepta clara ("passa cada vegada que faig X"); en el cas intermitent, cal fixar-se en què és diferent cada vegada que passa (l'hora del dia, quants programes tens oberts, si estàs connectat per Wi-Fi o per cable) per trobar el patró amagat.

El gestor de tasques, pas a pas

Quan un programa deixa de respondre -la pantalla es queda congelada, el ratolí no fa efecte dins la finestra, el cursor potser fins i tot es converteix en una rodeta que gira sense parar-, el primer recurs no ha de ser desendollar l'ordinador ni prémer el botó d'engegada. Existeix una eina feta exactament per a això, el gestor de tasques, que permet veure quins programes s'estan executant en aquell moment i tancar només el que està penjat, sense afectar la resta de feina que tinguis oberta.

A un ordinador amb Windows, els passos són:

1. Prem alhora les tecles Ctrl, Alt i Supr (o directament Ctrl, Maj i Esc, una drecera més ràpida que porta al mateix lloc).
2. Tria l'opció "Administrador de tasques" (o "Gestor de tasques", segons la versió).
3. A la pestanya "Processos", localitza el programa que apareix marcat com "sense resposta".
4. Selecciona'l amb un clic i prem el botó "Finalitza la tasca".

En un ordinador Mac, l'eina equivalent es diu Monitor d'activitat, i es pot obrir des de la carpeta Aplicacions > Utilitats, o prement Ordre + Espai i escrivint "Monitor d'activitat" al cercador Spotlight. Dins seu, es localitza el programa penjat i es prem el botó amb forma d'aspa (o "Surt forçat") per tancar-lo. En tots dos casos, la idea de fons és la mateixa: identificar amb precisió què falla i actuar només sobre allò, en lloc d'apagar-ho tot i perdre feina que altres programes tenien oberta sense guardar.

És l'eina que distingeix un usuari amb criteri d'un que reinicia l'ordinador cada vegada que alguna cosa es queda quieta trenta segons: molts programes que semblen "penjats" simplement estan fent un càlcul llarg i responen al cap d'una estona, així que val la pena esperar uns segons i comprovar si l'indicador d'activitat encara es mou abans de forçar el tancament.

Quan ni això funciona: apagada forçada i mode segur

Quan ni tancar el programa des del gestor de tasques funciona (per exemple, perquè el mateix gestor de tasques també s'ha quedat congelat), el pas següent és reiniciar l'equip amb normalitat des del menú d'engegada/apagada, i només si això tampoc és possible, forçar l'apagada mantenint premut el botó d'engegada uns segons fins que l'aparell s'apagui del tot. Aquesta darrera opció s'ha de fer servir com a últim recurs, perquè un tall brusc pot, en casos rars, malmetre un fitxer que s'estigués desant en aquell moment.

En sistemes que no arrenquen bé existeix també la idea del mode segur: un arrencament amb només els



components mínims del sistema operatiu, sense els programes d'inici automàtic ni els controladors afegits posteriorment, que serveix per determinar si el problema ve d'algun d'aquests elements que s'han anat afegint amb el temps. No cal saber activar-lo de memòria per a la prova (el camí exacte varia segons la versió del sistema i sol implicar prémer una tecla concreta durant l'arrencada, o accedir-hi des de les opcions de recuperació), sinó entendre per què existeix: aïllar el sistema bàsic de tot el que s'hi ha anat instal·lant per veure si l'avaría desapareix. Si en mode segur l'ordinador va bé, la causa és gairebé segur un programa, controlador o element d'inici afegit; si continua fallant fins i tot en mode segur, el problema és més probable que sigui del sistema mateix o del maquinari.

Un ordinador lent: manteniment que evita mals de cap

Per què s'alenteix un equip amb el temps

Un ordinador lent no sempre és per un virus, tot i que és el primer sospitós que molta gent imagina. Les causes més freqüents en la pràctica són tres, i totes es poden comprovar en pocs minuts sense instal·lar res: el disc ple (menys d'un 10-15% d'espai lliure), massa programes carregant-se automàticament a l'inici, o simplement que l'equip fa setmanes que no es reinicia i acumula processos oberts a la memòria. Comprovar l'espai en disc, el gestor de tasques i la data de l'últim reinici resol la majoria de casos sense necessitat de reinstal·lar res ni portar l'ordinador a arreglar.

Alliberar espai en disc, pas a pas

Alliberar espai no vol dir necessàriament comprar més emmagatzematge: sovint n'hi ha prou amb una revisió de deu minuts.

1. Buida la paperera de reciclatge (a Windows, clic dret sobre la icona de la paperera de l'escriptori i "Buida la paperera"; als fitxers d'un Mac, dins la carpeta Paperera, botó "Buida").
2. Revisa la carpeta de Descàrregues, on s'acumulen instal·ladors, PDFs i arxius adjunts que ja no es fan servir mai més. Un ordinador amb anys d'ús pot tenir-hi gigues senceres oblidades.
3. Executa l'eina de neteja de disc del sistema (a Windows, cerca "Neteja de disc" al menú d'inici) per eliminar fitxers temporals que el propi sistema genera i no esborra sol.
4. Repassa la llista de programes instal·lats (a Windows, "Configuració > Aplicacions"; al Mac, la carpeta Aplicacions) i desinstal·la els que vas provar una vegada i no has tornat a obrir.

Cada programa instal·lat ocupa espai encara que no s'utilitzi mai, i molts, a més, es carreguen sols a cada arrencada, cosa que allarga el temps d'engegada sense que l'usuari en sigui conscient.

Programes d'inici automàtic

Revisar la llista de programes d'inici automàtic i desactivar els que no calen cada dia és una millora notable i poc coneguda: un ordinador pot trigar el doble a estar llest només per tenir deu icones innecessàries carregant-se al fons sense que ningú les hagi demanat aquell dia. Per fer-ho a Windows:

1. Obre el gestor de tasques (Ctrl+Alt+Supr o Ctrl+Maj+Esc).
2. Ves a la pestanya "Inici" (o "Startup").
3. Revisa la columna "Impacte a l'inici", que indica quins programes alenteixen més l'arrencada.
4. Selecciona els que no necessites cada dia (per exemple, un editor de fotos que fas servir un cop al mes) i prem "Desactiva".

Això no desinstal·la el programa, només evita que s'obri sol; encara el pots utilitzar quan el necessitis, obrint-lo manualment.



Actualitzar controladors

Les actualitzacions de controladors (drivers), és a dir, el programari que fa que el sistema operatiu sàpiga parlar amb una peça concreta de maquinari (la targeta gràfica, la impressora, la placa de so), no cal entendre-les tècnicament per a la prova, però sí saber que mantenir-les al dia sol resoldre problemes de rendiment o compatibilitat que reinstal·lar el programa que falla no arregla. Un equip que comença a donar problemes amb una peça concreta -per exemple, la imatge que "salta" o els jocs que van molt pitjor que abans- sense que s'hagi instal·lat res de nou, sol tenir aquest origen: el controlador d'aquell component ha quedat desactualitzat respecte a la resta del sistema.

La xarxa no va: com diagnosticar-ho pas a pas

Quan falla la connexió a Internet, el diagnòstic per capes es concreta en passos molt pràctics, i és un dels blocs que més es pregunta a l'examen perquè és una situació que qualsevol persona viu diverses vegades l'any.

Primer, comprova si el problema és només d'aquell dispositiu o de tota la xarxa: si el mòbil, amb les dades mòbils i sense connectar-se al Wi-Fi de casa, navega amb normalitat, el problema no és de l'operadora ni d'Internet en general, és de la xarxa de casa o d'aquell aparell concret. Aquest primer pas -provar amb un altre dispositiu i una altra connexió- és el que separa un problema local d'un de general, i és exactament l'ordre que es demana a l'examen: primer el dispositiu, després el router, i només al final l'operadora.

Segon, mira el router. Les llums indicadores donen molta informació sense necessitat de tocar res: una llum ambre o vermella parpellejant, en comptes de la verda o blava fixa habitual, sol indicar un problema (de connexió amb l'exterior, de configuració, o una avaria del mateix aparell) que val la pena revisar abans de fer res més. Reiniciar el router és el pas següent: apagar-lo, esperar uns deu o quinze segons perquè es descarregui del tot, i tornar-lo a engegar. Aquest gest, tan senzill que sembla mentida que funcioni, soluciona un percentatge molt alt d'incidències domèstiques, perquè neteja errors temporals de memòria de l'aparell, que igual que un ordinador, també pot "penjar-se".

Tercer, val la pena fixar-se en si el problema afecta només el Wi-Fi o també el cable. Si el Wi-Fi falla però un ordinador connectat per cable de xarxa funciona amb normalitat, això és una pista molt clara: un problema només al Wi-Fi sol ser de senyal (l'aparell està massa lluny del router, hi ha parets gruixudes pel mig, o interferències d'altres xarxes properes), mentre que un problema que afecta tant el cable com el Wi-Fi apunta al router mateix o a la connexió que arriba de fora de casa. Imagina una oficina petita on l'ordinador connectat per cable a la recepció funciona perfectament, però els portàtils per Wi-Fi de la sala de reunions del fons van fluixos i es desconnecten sovint: això suggereix un problema de cobertura del senyal Wi-Fi en aquella sala concreta (potser cal un repetidor), no pas una avaria general de la connexió.

Quan la connexió va lenta de manera constant, no puntual, un test de velocitat en línia (hi ha diverses pàgines gratuïtes que ho fan en qüestió de segons) permet comparar-la amb la velocitat que consta al contracte amb l'operadora. Si el resultat és molt inferior de manera repetida i en diferents moments del dia, val la pena documentar-ho (fer captures dels resultats, anotar dates i hores) abans de trucar a l'operadora, amb el mateix criteri de "ser concret" que s'aplica a qualsevol avís de suport tècnic.

Si tot i comprovar el dispositiu, el router i el cable el problema persisteix, l'últim pas és assumir que es tracta d'una avaria general de la zona (que sovint es pot confirmar consultant la pàgina o l'app de l'operadora, que solen informar-ne) i contactar amb el servei tècnic. Un exemple del dia a dia: si vols fer un tràmit urgent a la seu electrònica de l'ajuntament i la pàgina no carrega, abans de donar per fet que la web és qui falla, prova-ho amb les dades mòbils; si tampoc carrega amb dades, el problema pot ser de la



mateixa web de l'ajuntament (que també passa), no de la teva connexió.

Actualitzacions i còpies de seguretat: preveure abans de patir

Quan sí i quan esperar

Les actualitzacions de programari no són un caprici del fabricant per fer-te perdre temps: tapen forats de seguretat (vulnerabilitats) que algú amb males intencions podria fer servir per entrar al teu equip, robar dades o instal·lar programari maliciós sense que te n'adonis. No actualitzar mai deixa l'ordinador o el mòbil exposat de manera innecessària, encara que a simple vista sembli que "tot funciona igual de bé".

Ara bé, això no vol dir instal·lar qualsevol actualització en qualsevol moment, sense pensar-hi. Una actualització important del sistema operatiu, del tipus que canvia de versió sencera i pot trigar mitja hora o més, just abans d'una presentació important, un examen en línia o un lliurament de feina, és una mala idea: pot trigar més del previst, requerir diversos reinicis, o en casos poc freqüents però reals, generar incompatibilitats amb algun programa que necessites just en aquell moment. La pràctica raonable és fer les actualitzacions de seguretat petites (les que arriben sovint i triguen poc) de seguida que apareixen, i deixar les actualitzacions grans de versió per a un moment sense pressa, idealment un vespre o un cap de setmana, havent fet abans una còpia de seguretat de les dades importants.

Còpies de seguretat: on i com

Fer còpies de seguretat periòdiques (al núvol, per exemple amb serveis com Google Drive o iCloud, o en un disc dur extern) no és una tasca per fer quan ja hi ha un problema, és precisament una manera de preveure'l abans que passi. Un ordinador es pot espatllar, un mòbil es pot perdre o robar, un disc dur es pot trencar de cop: cap d'aquestes coses és estrany del tot, i quan passa, la diferència entre "he perdut cinc anys de fotos" i "he perdut el que havia canviat des d'ahir" la marca només tenir un hàbit de còpia de seguretat regular. Per a algú que no en té el costum, una manera senzilla de començar és activar la còpia automàtica al núvol del mòbil (a un Android, dins "Configuració > Google > Còpia de seguretat"; a un iPhone, dins "Configuració > [el teu nom] > iCloud > Còpia de seguretat de l'iCloud") i programar, encara que sigui de manera manual cada pocs mesos, còpiar els documents importants de l'ordinador a un disc extern o una carpeta al núvol.

Aquesta idea de preveure abans que patir connecta amb bona part del que es demana en aquesta àrea: no és fer-ho tot perfecte, és anticipar-se als problemes més habituals abans que et passin a tu.

La bateria: cura del portàtil i del mòbil

Cuidar la bateria també forma part de mantenir un equip en bon estat, i és un dels punts on circulen més mites que fets. Amb les bateries actuals, de ió de liti (llió), no cal esperar que es descarreguin del tot abans de tornar-les a carregar, com passava amb tecnologies més antigues. De fet, és al revés: els cicles de càrrega curts i freqüents (carregar del 40% al 80%, per exemple, diverses vegades al dia) desgasten menys la bateria a llarg termini que deixar-la arribar sistemàticament al 0% abans de tornar-la a endollar.

El que sí que perjudica la bateria a llarg termini és mantenir l'aparell sempre endollat al 100% durant hores i hores (per exemple, deixar el portàtil connectat a la xarxa elèctrica de manera permanent tota la setmana sense mai fer-lo anar amb bateria), o exposar-lo a calor excessiva: dins un cotxe al sol a l'estiu, tapat amb una funda mentre carrega, o sobre un coixí que li impedeixi ventilar-se. La calor és, de fet, l'enemic més gran de qualsevol bateria de llió, més que els cicles de càrrega en si.



Un calibratge ocasional -deixar-la baixar fins gairebé buida i carregar-la del tot de tant en tant- ajuda que el sistema calculi millor el percentatge real que queda, però no cal fer-ho com a rutina diària. Als mòbils, els consells són semblants: evitar temperatures extremes, no forçar sempre el 100% ni el 0%, i vigilar quines aplicacions consumeixen bateria en segon pla. Sovint el problema d'una bateria que "dura poc" no és la bateria en si, sinó una aplicació concreta mal configurada que es manté activa fins i tot amb la pantalla apagada.

Perifèrics i connexions: impressores, pantalles, bluetooth i USB

La impressora que no imprimeix

Si la impressora no imprimeix, seguir un ordre lògic evita perdre temps provant coses sense sentit:

1. Comprova que hi ha paper a la safata i que el nivell de tinta o tòner no és a zero (moltes impressores mostren un avís a la pantalla o des del programa de l'ordinador).
2. Confirma que el cable USB està ben connectat, o si és una impressora en xarxa, que està encesa i connectada al mateix Wi-Fi que l'ordinador.
3. Revisa la cua d'impressió: si un document anterior s'ha quedat encallat, bloqueja tots els següents. A Windows, s'obre des de "Configuració > Bluetooth i dispositius > Impressores i escàners", es tria la impressora i s'entra a "Obre la cua d'impressió"; des d'allà es pot cancel·lar el document encallat amb un clic dret.
4. Si res d'això funciona, reinicia la impressora (apagar-la, esperar uns segons, encendre-la de nou) i després l'ordinador.

Si una impressora que fins ara funcionava bé deixa d'imprimir correctament de sobte, sense que s'hagi fet cap canvi aparent a l'ordinador ni a la impressora mateixa, sovint el motiu és un controlador (driver) que ha quedat desactualitzat després d'una actualització del sistema operatiu, i tornar-lo a instal·lar (des de la web del fabricant, o deixant que el mateix sistema el busqui) sol resoldre-ho sense necessitat de canviar res més.

Pantalla externa: duplicar o ampliar

Connectar una pantalla externa o un projector a un portàtil obre dues opcions que convé distingir bé, perquè confondre-les és un error molt habitual i molt visible:

- Duplicar: la pantalla externa mostra exactament el mateix que la del portàtil. És la que interessa per a presentacions, perquè el públic veu en tot moment el mateix que el ponent té davant.
- Ampliar (o estendre): la pantalla externa afegeix espai de treball nou, com un segon escriptori independent del primer. És útil per treballar amb més finestres obertes alhora, però no per presentar.

A Windows, es canvia prement les tecles Tecla Windows + P, que obre un menú lateral amb les opcions "Només pantalla de PC", "Duplicar", "Ampliar" i "Només segona pantalla". Deixar el mode "Ampliar" quan calia "Duplicar" és un error clàssic -i molt real- que fa que el públic d'una sala vegi una pantalla en blanc, o l'escriptori normal amb les icones, mentre el ponent, mirant només la seva pròpia pantalla, creu que tot va bé i no entén per què ningú el segueix. Comprovar aquest detall abans de començar qualsevol presentació estalvia el moment incòmode de descobrir-ho amb tothom mirant.

Bluetooth i connexions sense fil

El bluetooth permet connectar aparells sense cables (auriculars, altaveus, teclats, o el mòbil amb el sistema del cotxe) mitjançant un procés anomenat emparellament. Per connectar per primera vegada uns



auriculars nous a un mòbil:

1. Activa el bluetooth als dos aparells (al mòbil, des de la barra d'ajustos ràpids o "Configuració > Connexions > Bluetooth"; als auriculars, sol haver-hi un botó que cal mantenir premut fins que una llum comença a parpellejar).
2. Posa els auriculars en mode de detecció (aquest pas sovint coincideix amb el punt anterior).
3. Al mòbil, dins la llista de dispositius disponibles que apareix a la pantalla de bluetooth, tria el nom dels auriculars.
4. Confirma l'emparellament si apareix algun codi a la pantalla (a vegades cal confirmar que el mateix codi apareix als dos aparells).

Un cop fet aquest procés una vegada, l'emparellament queda recordat als dos aparells, i les properes vegades es connectaran automàticament en apropar-se i activar el bluetooth, sense haver de repetir tots els passos.

USB i projectors

Pel que fa als connectors USB, no cal saber-ne les especificacions tècniques per a l'examen, però sí a nivell d'idea general que no tots són iguals: n'hi ha de més antics i lents (adequats per a un teclat o un ratolí, que no necessiten transmetre gaires dades) i de més moderns i ràpids (necessaris per moure grans quantitats de dades, com còpies de vídeos, en poc temps). Un detall que sol confondre: la forma del connector (el rectangular clàssic, anomenat tipus A, o el més petit i reversible tipus C, que es pot endollar per qualsevol dels dos costats) no diu res per si mateixa sobre la velocitat real de transmissió; hi ha connectors tipus C lents i connectors tipus A relativament ràpids, així que la forma i la velocitat són dues coses diferents.

Els projectors es connecten per cable (HDMI és el més habitual avui dia, tot i que encara n'hi ha amb l'antic connector VGA) o per Wi-Fi en alguns models moderns que ho permeten sense fils. Quan es dona la situació de "el projector no detecta l'ordinador" tot i tenir el cable HDMI ben endollat als dos extrems, la causa més habitual no és una avaria, sinó que la font d'entrada seleccionada al projector (que sol tenir diversos ports HDMI numerats, o una entrada VGA a banda) no coincideix amb el port on està físicament connectat el cable. La solució sol ser tan senzilla com prémer el botó "Font" o "Input" del comandament del projector fins que aparegui la imatge correcta.

Demandar ajuda: com fer-ho perquè et resolguin el problema de veritat

Saber quan i com demanar suport tècnic també és una competència digital pròpia d'aquesta àrea, i és un dels aspectes que més es valora a la prova perquè reflecteix si algú sap comunicar un problema de manera útil. Un bon avís a un equip de suport, ja sigui per telèfon, correu o un formulari intern d'una empresa, inclou sempre quatre coses: què estaves fent exactament quan ha passat (obrint un fitxer, enviant un correu, entrant a una pàgina concreta), quin missatge d'error ha sortit, si és possible amb una captura de pantalla, si el problema passa sempre que repeteixes l'acció o només de tant en tant, i què has provat ja per intentar solucionar-ho tu mateix (per exemple, "ho he reiniciat i segueix igual").

Un tècnic que rep un avís del tipus "no em va l'ordinador" o "internet no funciona" perd un temps valuós preguntant el que ja podries haver dit tu des del principi; un que rep aquests quatre punts ben concretats sol poder resoldre el cas en la primera trucada, sense anades i vingudes. Aquest mateix criteri -ser concret, aportar dades, no quedar-se en "no va bé"- és exactament el mateix que fa servir un usuari amb criteri quan documenta una velocitat d'Internet lenta abans de trucar a l'operadora, o quan anota el codi



d'una pantalla d'error abans de reiniciar.

Saber fins on pots diagnosticar tu mateix i quan ja no és cosa teva també forma part de resoldre bé un problema. Un disc dur que fa sorolls estranys (com clics o xiulets metàl·lics) és un símptoma d'una possible fallada física greu, i intentar-hi seguir treballant pot empitjorar les coses; el més sensat és aturar l'ús de l'equip i portar-lo a un servei tècnic, per intentar salvar les dades abans que el disc deixi de respondre del tot. Resoldre bé un problema no vol dir fer-ho tot un mateix, vol dir saber a qui passar la resta.

Seguretat: reconèixer correus i missatges sospitosos

Part de resoldre problemes en l'entorn digital és evitar-ne alguns abans que arribin a passar, i el correu electrònic fraudulent (conegut com a pesca o "phishing") és, avui dia, una de les vies més habituals per les quals algú intenta accedir a dades personals o bancàries d'una persona normal i corrent. Un correu sospitós sol tenir un patró reconeixible: demana "confirmar" o "actualitzar" dades bancàries, una contrasenya o un número de targeta fent clic en un enllaç, sovint amb un to d'urgència ("el teu compte serà bloquejat en 24 hores" o "detectem un moviment sospitós, verifica't ara").

Davant d'un correu així, l'actitud més prudent és desconfiar per defecte, encara que el missatge sembli venir d'un banc, una empresa de missatgeria o un organisme conegut. Els passos raonables són:

1. Comprovar el remitent real del correu (no només el nom que mostra, sinó l'adreça electrònica completa, que a vegades es pot veure fent clic o passant el cursor per sobre del nom), perquè sovint l'adreça real no té res a veure amb l'entitat que diu representar.
2. No fer clic mai en l'enllaç del correu si hi ha el més mínim dubte, i encara menys introduir-hi dades bancàries o contrasenyes.
3. Si cal comprovar alguna cosa amb el banc o l'empresa en qüestió, fer-ho sempre entrant directament a la pàgina oficial escrivint l'adreça al navegador, o trucant al telèfon oficial, mai fent servir l'enllaç o el telèfon que apareix dins el correu sospitós.
4. En cas de dubte raonable, no clicar ni respondre, i si l'entitat ho permet, reenviar-ho al seu departament de seguretat o simplement esborrar-lo.

Aquest mateix criteri de prudència s'aplica a missatges de mòbil (SMS o WhatsApp) que demanen dades semblants, una variant coneguda com a "smishing", cada cop més freqüent suplantant paqueteries o l'Agència Tributària en període de renda. La regla de fons és sempre la mateixa: cap entitat seriosa demana mai una contrasenya completa o el codi d'una targeta per correu o missatge, i com més insisteix un missatge en la urgència, més hauria d'activar-se la desconfiança.

Triar l'eina adequada per a cada tasca

Full de càlcul contra base de dades

Una part important d'aquesta àrea és saber que no tota la tecnologia serveix igual per a tot, i que triar malament fa perdre hores que triar bé hauria estalviat. L'exemple clàssic és full de càlcul contra base de dades. Un full de càlcul (Excel, o la seva alternativa gratuïta Google Sheets) és perfecte per a càlculs, llistes curtes i anàlisis puntuals: el pressupost familiar del mes, les notes d'una classe, el control de despeses de les vacances. Una base de dades es fa necessària quan les dades estan relacionades entre elles i cal evitar duplicats: per exemple, gestionar els 400 socis d'una associació esportiva juntament amb les seves quotes pagades, les activitats en què participen i l'assistència a cadascuna.



Fer això en un full de càlcul obliga a repetir el nom de cada soci a cada fila on apareix una activitat o un pagament, i tard o d'hora algú l'escriurà de manera diferent -"Joan Puig" en una fila, "J. Puig" en una altra- i les dades deixaran de quadrar, perquè el sistema no sabrà que és la mateixa persona. Una base de dades relacional evita això perquè cada soci es registra una sola vegada, amb un identificador únic, i totes les activitats i pagaments s'hi enllacen sense repetir mai les dades de la persona.

Coordinar persones sense saturar el correu

Un altre exemple molt habitual: organitzar una reunió entre deu companys enviant correus del tipus "a mi em va bé dimarts", "jo dimecres no puc" és ineficient i genera una cadena interminable i confusa. Una eina de calendari compartit (on tothom veu la disponibilitat de la resta) o un formulari de disponibilitat (on cada persona marca les franges lliures i l'eina calcula quina va bé a més gent) resol en un sol missatge el que per correu costaria deu missatges i uns quants dies.

Gestionar projectes amb dates i responsables

Quan un equip de treball ha de repartir-se tasques d'un projecte amb dates límit i responsables assignats, el criteri per triar l'eina adequada no és quina és més coneguda o de moda, sinó quina permet fer allò que realment es necessita: assignar una tasca a una persona concreta, posar-hi una data límit visible, i fer-ne seguiment de l'estat (pendent, en curs, feta) perquè tothom sàpiga com va el projecte sense preguntar-ho per correu cada dos dies. Un full de càlcul compartit en pot fer una versió senzilla, però una eina de gestió de tasques pensada per a això (amb targetes, columnes d'estat i avisos de data límit) sol estalviar molt més temps quan hi ha diverses persones i moltes tasques en paral·lel.

Aprofitar el que ja tens: plantilles i macros

Cada mes cal aplicar el mateix format a un informe que es genera a partir d'un full de càlcul: els mateixos colors de capçalera, les mateixes fórmules de totals, el mateix gràfic. Fer-ho manualment cada vegada és perdre temps en una tasca repetitiva. Una manera de fer un ús més intel·ligent de l'eina és crear una plantilla (un full ja formatat que només cal omplir amb les dades noves cada mes) o, un pas més enllà, una macro (una seqüència d'accions gravada que l'eina repeteix automàticament amb un sol clic o una drecera de teclat). Tant Excel com Google Sheets permeten gravar macros senzilles des del menú corresponent (a Excel, dins la pestanya "Visualització > Macros"), sense necessitat de saber programar: n'hi ha prou de fer un cop les accions manualment mentre l'eina les grava, i després reproduir-les sempre que calgui.

El criteri de fons que es demana a la prova en aquesta secció no és memoritzar noms concrets d'eines, sinó saber raonar: quantes dades hi ha, s'han de repetir o estan relacionades entre elles, quantes persones hi participen, i quant de temps val la pena invertir a muntar una solució davant del temps que estalviarà després.

Comparar abans de comprar: criteris que importen de veritat

Triar un aparell nou (un mòbil, un portàtil, una tauleta) amb criteri vol dir saber quines característiques del full de característiques afecten de veritat l'ús diari, i quines són sobretot reclam publicitari que en la pràctica es nota poc.

La memòria RAM determina quants programes o pestanyes del navegador es poden tenir oberts alhora sense que l'equip comenci a alentir-se. Poca RAM és la causa més habitual que un ordinador "nou" ja vagi lent al cap de pocs mesos, no per estar espatllat, sinó perquè l'usuari obre el navegador amb vint pestanyes, un editor de text i un programa de videotrucades alhora, i la memòria disponible no dona per a



tot alhora.

L'emmagatzematge determina quants fitxers, fotos, vídeos i programes hi caben. Un error freqüent en comprar un mòbil nou és triar la versió amb menys emmagatzematge perquè surt més barata, oblidant que les fotos i vídeos actuals (en alta resolució, en format 4K) ocupen molt més espai que fa uns anys; qui compra pensant només en l'estalvi immediat sovint es troba, al cap d'un any, amb l'avís de "espai insuficient" cada vegada que vol fer una foto.

La càmera d'un mòbil, en canvi, és un cas on una xifra gran al full de característiques -els megapíxels- importa menys del que sembla a primer cop d'ull. La qualitat real d'una fotografia depèn més del processament d'imatge que fa el mòbil internament (com combina la llum, com corregeix els colors) i de la qualitat de la lent, que no pas del número de megapíxels anunciat, que sovint és més una xifra de màrqueting que un indicador fiable de qualitat.

Abans d'instal·lar qualsevol programa, tant en un ordinador nou com en un que ja tens, cal comprovar també la compatibilitat: que la versió del sistema operatiu instal·lat és la que demana el programa (moltes aplicacions especifiquen una versió mínima), i que hi ha prou espai en disc i memòria RAM lliure per fer-lo anar amb fluïdesa. Instal·lar un programa incompatible no només fa que aquell programa no funcioni bé, de vegades genera errors que afecten altres programes del sistema que fins aleshores anaven bé.

Programari lliure, versions web i alternatives gratuïtes

Lliure contra propietari

No tot el programari útil s'ha de comprar. El programari lliure (Linux com a sistema operatiu, LibreOffice com a paquet ofimàtic, l'editor d'imatges GIMP) es distribueix de manera gratuïta i, a més, permet que qualsevol persona amb coneixements pugui veure i modificar com funciona per dins, a diferència del programari propietari (Windows, Microsoft Office, Adobe Photoshop), que sol ser de pagament i tancat, sense que ningú fora del fabricant pugui veure'n el codi. Per a moltes tasques quotidianes, LibreOffice fa el mateix que un paquet ofimàtic de pagament: escriure una carta, fer un pressupost, muntar una presentació. GIMP permet retocar fotografies amb un nivell de funcions semblant al d'editors coneguts de pagament, sense cap cost d'entrada.

Web, escriptori o app mòbil

Una altra decisió habitual del dia a dia és triar entre la versió web, la d'escriptori i l'app mòbil d'un mateix servei (per exemple, el correu de Gmail, o un editor de documents). La versió web no requereix instal·lar res i s'actualitza sola cada vegada que hi entres, però pot necessitar connexió constant a Internet per funcionar bé. La versió d'escriptori sol anar més fluida un cop instal·lada i permet treballar sense connexió en molts casos, però ocupa espai al disc i cal actualitzar-la de tant en tant. L'app mòbil està pensada per a pantalles petites i un ús ràpid i puntual (mirar un correu, respondre un missatge curt), no tant per a tasques llargues i complexes com redactar un informe extens. Cap de les tres és millor de manera absoluta: depèn de si cal mobilitat, feina sense connexió, o simplicitat immediata.

Subscripció o llicència única

Finalment, cal distingir entre pagar per subscripció (una quota periòdica, mensual o anual, que dona dret a l'ús del programa mentre es continua pagant, i que sol incloure actualitzacions incloses) i comprar una llicència única (un pagament únic que dona dret a fer servir aquella versió del programa per sempre, però sense actualitzacions futures incloses). La subscripció surt a compte quan l'ús és continuat i es valora tenir



sempre l'última versió; la compra única surt més a compte quan la necessitat és puntual o esporàdica, i no importa quedar-se amb una versió una mica més antiga amb el temps.

Adaptar l'entorn: personalització i accessibilitat

Fer l'entorn còmode

Un sistema operatiu no s'ha d'utilitzar tal com ve de fàbrica si això dificulta la feina de qui l'usa cada dia. Personalitzar el fons de pantalla, la mida de la lletra o activar el tema fosc no és un simple caprici estètic: una lletra més gran facilita la lectura a qui té dificultats de visió, i un tema fosc redueix la fatiga visual en sessions llargues davant la pantalla, especialment de nit. Aquestes opcions es troben, tant a Windows com al mòbil, dins els ajustos de pantalla o d'aparença (a Windows, "Configuració > Personalització"; a un Android, "Configuració > Pantalla"), i adaptar-les al propi gust i necessitat és tan legítim com triar la graduació de les ulleres.

Accessibilitat: eines que fan la tecnologia usable per a tothom

L'accessibilitat va un pas més enllà de la simple comoditat: és el conjunt d'eines pensades perquè una persona amb alguna dificultat concreta pugui fer servir l'ordinador o el mòbil amb normalitat. La lupa de pantalla amplia una zona concreta per a qui té dificultats de visió. El narrador (o lector de pantalla) llegeix en veu alta el contingut de la pantalla per a persones amb discapacitat visual, permetent-los navegar sense necessitat de veure res. Els subtítols automàtics faciliten seguir un vídeo sense so, o a persones amb dificultats auditives. El contrast alt millora la llegibilitat per a persones amb baixa visió o daltonisme, ressaltant els elements de la pantalla. Aquestes opcions es troben dins l'apartat "Accessibilitat" dels ajustos, tant a Windows ("Configuració > Accessibilitat") com a un iPhone o Android ("Configuració > Accessibilitat"). Saber que aquestes opcions existeixen i on trobar-les és part de la competència que avalua aquesta àrea, encara que un mateix no en necessiti cap ara mateix: la utilitat pot sorgir per a un familiar, un company de feina, o un mateix més endavant.

Idioma, teclat i sincronització entre dispositius

Configurar l'idioma del sistema i el del teclat també forma part d'adaptar l'entorn. Un teclat configurat amb l'idioma equivocat fa que certes tecles (els accents, la ç, la dièresi) no funcionin com s'espera, un problema habitual en canviar d'aparell o treballar amb un ordinador prestat configurat per a un altre idioma.

Molts serveis (els comptes de Google, de Microsoft, o d'Apple) permeten sincronitzar la configuració, els documents i les preferències entre diversos dispositius. Això vol dir que en iniciar sessió amb el mateix compte en un ordinador nou, es recuperen automàticament els favorits del navegador, les contrasenyes desades, els documents guardats al núvol i moltes de les preferències, sense haver de configurar-ho absolutament tot de nou des de zero. És un dels avantatges menys visibles però més pràctics de tenir un compte ben configurat: la feina de configuració d'avui es fa servir a tots els aparells futurs.

Ús creatiu i innovador de la tecnologia

Aquesta competència no vol dir "saber programar", vol dir veure una eina que ja coneixes i pensar-hi més enllà del seu ús obvi i habitual. Fer servir les plantilles i les macros d'un full de càlcul perquè una tasca que fas cada mes es faci gairebé sola, com hem vist abans amb l'exemple de l'informe mensual. Combinar un formulari en línia amb un full de càlcul perquè les respostes de les persones que l'omplen s'organitzin automàticament en files i columnes, sense haver de copiar-les una a una a mà: aquest és exactament el



tipus d'exemple que la prova considera un ús innovador dins d'aquest nivell, perquè agafa dues eines senzilles i ja conegudes i les fa treballar juntes per estalviar una feina repetitiva. Usar un gestor de notes compartit per crear una base senzilla de coneixement a la feina, on tothom pot consultar i afegir informació sense dependre d'un sol correu que algú va enviar fa mesos i que ja ningú troba.

La innovació, en aquest nivell, és detectar una tasca repetitiva i preguntar-se si es pot automatitzar o simplificar amb el que ja tens a mà, sense eines noves i cares ni coneixements tècnics avançats.

Intel·ligència artificial: què és i on la trobem cada dia

Què la distingeix de l'automatització clàssica

La intel·ligència artificial és programari capaç de fer tasques que, fetes per una persona, dirien que requereixen "intel·ligència": reconèixer una cara en una foto, traduir un text d'un idioma a un altre, recomanar una sèrie que probablement t'agradarà, o generar un text nou a partir d'una instrucció. La distingeix de l'automatització clàssica el fet que aprèn patrons a partir de grans quantitats de dades, en lloc de seguir només un conjunt de regles fixes escrites d'entrada per un programador. Un exemple molt clar de què NO és intel·ligència artificial, i que és fàcil de confondre a l'examen: una calculadora bàsica que suma dos números seguint sempre la mateixa fórmula matemàtica fixa no aprèn res ni s'adapta a res, simplement aplica una regla exacta i invariable cada vegada; per això no es considera intel·ligència artificial, per molt "intel·ligent" que pugui semblar que resolgui un càlcul.

Usos quotidians, sovint invisibles

La fem servir constantment sense adonar-nos-en: el corrector ortogràfic i el text predictiu del teclat del mòbil, les recomanacions de sèries de Netflix o de cançons de Spotify, el filtre que separa el correu brossa de la resta a la safata d'entrada, el reconeixement facial que desbloqueja el telèfon en mirar-lo, i els assistents conversacionals com ChatGPT, Gemini o Copilot, capaços de redactar, resumir, traduir o fins i tot programar a partir d'una instrucció escrita en llenguatge normal (allò que s'anomena un "prompt").

Els assistents de veu i els traductors automàtics són dos dels usos d'IA més quotidians i, alhora, menys percebuts com a tals. Dir en veu alta "posa una alarma a les set" i que el mòbil ho entengui és intel·ligència artificial funcionant en segon pla, igual que traduir a l'instant un cartell en un idioma desconegut apuntant-hi la càmera del mòbil.

Els chatbots fan bé tasques com resumir un text llarg, generar un primer esborrany, explicar un concepte tècnic de manera senzilla, o traduir amb un nivell prou bo per a l'ús habitual. En canvi, fan malament qualsevol tasca que exigeixi certesa absoluta sobre fets molt concrets o coneixement molt actualitzat que no formava part de les dades amb què es van entrenar, i que per tant poden desconèixer o, pitjor, inventar-se amb tota naturalitat.

Escriure bones instruccions

Usar bé aquests assistents és, en si mateixa, una competència pràctica que es pot millorar: com més context i concreció dones a la instrucció, millor sol ser la resposta. Demanar simplement "escriu un correu" dona un resultat genèric, que gairebé sempre necessita ser reescrit del tot. Demanar, en canvi, "escriu un correu breu i formal per avisar un client que el lliurament s'endarrereix tres dies, sense donar excuses llargues" -és a dir, especificant per a qui és, quin to hi ha de tenir i quina extensió es vol- dona un resultat útil de seguida, molt més a prop del que realment es necessita.

Un bon ús de la IA per aprendre no és copiar directament la resposta que dona, sinó demanar-li que



expliqui un concepte de diverses maneres fins que quedi clar, o que et faci preguntes per comprovar si l'has entès de debò, i contrastar sempre allò rellevant amb una font fiable abans de donar-ho per bo.

Límits, riscos i ètica de la IA

Al·lucinacions: quan la seguretat aparent enganya

Aquí és on la prova sol posar més èmfasi, perquè és el que més s'oblida a la pràctica. Els assistents d'IA generativa no "saben" coses amb certesa com ho faria una persona experta consultant una font: prediuen, paraula a paraula, la continuació més probable a partir dels patrons apresos durant l'entrenament, i això fa que de vegades inventin dades, cites, referències legals o fets sencers, presentats amb tota la seguretat aparent d'una resposta correcta. Aquest fenomen s'anomena "al·lucinació", i el problema de fons no és que la IA s'equivoqui, sinó que ho fa amb el mateix to convincent tant si encerta com si s'inventa alguna cosa. Per això qualsevol informació rellevant que doni una IA -una xifra, una data, una referència legal- s'ha de verificar amb una font fiable abans de fer-la servir, especialment abans d'incloure-la en un informe de la feina.

Biaix: quan les dades porten prejudicis a dins

Un altre límit important és el biaix. Si les dades amb què s'ha entrenat un sistema contenen prejudicis previs (per exemple, associar de manera estadística certes professions més a un gènere que a un altre, perquè històricament ha estat així), el sistema pot reproduir aquests prejudicis en les seves respostes o decisions, sense que ho sembli a primer cop d'ull. No és una qüestió tècnica menor: afecta decisions reals amb conseqüències reals sobre persones. Un cas típic és un sistema d'IA usat per filtrar currículums en un procés de selecció que acaba descartant sistemàticament les candidatures d'un col·lectiu concret sense cap motiu objectiu: el sistema, sense voler-ho ningú expressament, ha après aquest patró de les dades històriques amb què es va entrenar.

Privadesa: què no s'hi ha d'escriure mai

Pel que fa a la privadesa, cal tenir clar que allò que s'escriu en un xat d'intel·ligència artificial pot quedar emmagatzemat pel servei i arribar, segons les condicions de cada eina, a fer-se servir per entrenar futures versions del sistema. Per això no s'hi han d'introduir mai dades confidencials: contrasenyes, dades mèdiques pròpies o d'altres persones, o documents interns d'una empresa, tret que l'eina i el contracte de l'organització ho permetin de manera explícita. Si un treballador vol demanar ajuda a un assistent d'IA gratuït en línia per redactar un informe intern, la pràctica més prudent és descriure el context de manera general, sense incloure-hi dades confidencials ni personals concretes, i completar-ho després amb la informació sensible pel seu compte, fora de l'eina.

Deepfakes i drets d'autor

Finalment, hi ha riscos socials que val la pena tenir en compte, i que apareixen cada cop més sovint en converses quotidianes. Els "deepfakes" són imatges, vídeos o veus falsificats de manera molt realista mitjançant intel·ligència artificial, fins al punt de mostrar una persona coneguda dient o fent coses que mai ha dit ni fet; aquest tipus de contingut pot servir per enganyar, difamar o manipular l'opinió pública, i és cada vegada més difícil de distingir a simple vista d'un contingut real.

Els continguts generats per IA (textos, imatges, música) plantegen també dubtes ètics importants sobre els drets d'autor, en una doble direcció: tant de qui genera el contingut i el fa servir com si fos propi, com de les obres originals de persones creadores amb què el sistema es va entrenar, sovint sense el seu



consentiment explícit. I la facilitat amb què avui es pot generar text de qualitat, amb aparença de credibilitat, pot alimentar la desinformació si es consumeix sense cap sentit crític.

Aprenentatge continu: conèixer els propis límits

La tecnologia canvia més ràpid que qualsevol curs pot seguir-li el ritme, i per això aquesta àrea inclou, com a competència pròpia, saber identificar les pròpies llacunes: no saber-ho tot, sinó saber què no saps i on trobar-ho quan et faci falta de veritat. Els símptomes típics d'una llacuna concreta són evitar sistemàticament una tasca perquè "no se'm dona bé" i buscar sempre una excusa per no fer-la, dependre sempre d'una altra persona per al mateix tipus de gestió repetida, o notar que una eina que fas servir des de fa anys ha canviat de disseny o de funcions i ja no la domines igual que abans. Una persona que sempre depèn d'un company perquè li faci les videotrucades de feina perquè "no se'n surt" amb l'eina no té un problema puntual, té exactament això: una llacuna concreta de competència digital que val la pena identificar i treballar, en lloc de continuar depenent d'algú altre indefinidament.

Un cop identificada una llacuna, hi ha diverses vies per omplir-la sense necessitat d'un curs llarg i car: els cursos en línia oberts i massius (coneguts per les sigles en anglès MOOC), sovint gratuïts, que permeten aprendre al propi ritme des de casa; els tutorials curts en vídeo o en text, útils quan cal una solució concreta i immediata a un problema puntual, sense necessitat d'aprendre tot un tema sencer; i la mateixa acreditació ACTIC, pensada precisament per estructurar i certificar aquest aprenentatge continu en competències digitals. Les comunitats i fòrums en línia també són un recurs valuós per resoldre dubtes, però amb un criteri important que sovint es passa per alt: val la pena llegir primer si algú ja ha tingut i resolt el mateix dubte abans de publicar una pregunta nova, perquè sovint la resposta ja hi és escrita, i preguntar sense buscar abans és una manera de perdre el temps de tots plegats, tant el propi com el de qui hauria de respondre.

Estar al dia amb la tecnologia no vol dir perseguir cada novetat que surt cada setmana. La pràctica raonable és revisar de tant en tant les eines que ja fas servir sovint -el correu, el navegador, el paquet ofimàtic- per veure si han canviat o si n'hi ha una manera millor de treure'ls profit, sense la pressió d'aprendre-ho tot alhora. Reconèixer una llacuna i buscar-hi un tutorial, un curs curt o preguntar a la persona adequada és exactament la competència que avalua aquesta àrea: no fer-ho tot perfecte des del primer dia, sinó saber-se moure amb criteri quan alguna cosa no surt a la primera.