Opoademia

GUIA D'ESTUDI COMPLETA

ACTIC · Certificat avançat (competències digitals)

Generalitat de Catalunya · Competències digitals (ACTIC)

Grup ACTIC nivell 3 (avançat) · 5 temes amb apunts explicats

250 preguntes d'examen disponibles

Material original, redactat per Opoademia

AVÍS LEGAL

Drets d'autor i condicions d'ús

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

TEMA 1

Àrea 1. Alfabetització informacional i de dades

Cerca avançada: anar més enllà de l'operador AND

A nivell avançat ja no n'hi ha prou amb saber que Google entén cometes o el signe menys. El que es demana és combinar operadors per construir consultes precises i saber quan una cerca genèrica queda curta. Un usuari mitjà escriu quatre paraules i es conforma amb els primers resultats; un usuari avançat pensa la consulta abans d'escriure-la, com si negociés amb el cercador les condicions exactes del que vol trobar.

Booleans i parèntesis: construir la lògica de la cerca

La combinació d'operadors funciona per parèntesis i booleans, igual que en una base de dades: `("funció pública" OR oposicions) AND Catalunya -privada` filtra resultats que continguin qualsevol de les dues primeres expressions, que a més parlin de Catalunya, i que descarti tot allò que inclogui la paraula privada. El parèntesi agrupa les alternatives (OR) perquè el cercador les tracti com un bloc únic abans d'aplicar-hi la resta de condicions; sense parèntesis, la consulta es tornaria ambigua i el motor de cerca prioritzaria termes de manera diferent a la que volem.

Val la pena dominar també l'operador `OR` en majúscules, que és l'únic que el cercador interpreta com a disjunció lògica: si s'escriu en minúscules ("o"), Google el tracta com una paraula normal de la cerca i no com un connector lògic. Aquest és un dels punts que més sovint es demanen a l'examen perquè no és intuïtiu: sembla un detall menor, però canvia completament el resultat.

Operadors de camp: afinar per domini, format, títol i URL

Els operadors de camp afinen encara més la cerca:

- `site:` restringeix els resultats a un domini concret, per exemple `site:gencat.cat`.
- `filetype:` busca només documents en un format determinat, com `filetype:pdf`.
- `intitle:` obliga que el terme aparegui al títol de la pàgina.
- `inurl:` obliga que el terme aparegui a l'adreça web mateixa.

Un exemple real i molt útil a la pràctica: per trobar convocatòries oficials en PDF sense passar per portals de tercers que en fan resums (i que sovint pengen la informació desactualitzada), la consulta `intitle:convocatòria filetype:pdf site:caib.es` dona resultats molt més nets que escriure la mateixa frase a la caixa de cerca normal. El mateix principi funciona per a qualsevol tràmit administratiu: si es vol la instància oficial de sol·licitud d'un ajut municipal en PDF, `filetype:pdf inurl:tramits site:ajuntament.cat` (substituint pel domini real de l'ajuntament) evita haver de navegar deu pàgines de menú fins arribar-hi.

Procediment pas a pas: construir una cerca combinada eficaç

1. Identifica el domini de confiança on hauria d'estar la informació (una administració, una universitat, un mitjà consolidat) i anota'l per fer-lo servir amb `site:`.
2. Decideix si necessites un format concret (un PDF descarregable, per exemple) i afegeix `filetype:pdf`.
3. Si la informació es pot trobar amb paraules alternatives (sinònims, noms antics i nous d'un mateix tràmit), agrupa-les amb parèntesis i `OR`: `(empadronament OR "certificat de residència")`.
4. Exclou amb el signe menys (`-`) les paraules que saps que et portaran soroll, com `-oposicions` si vols

excloure convocatòries de feina d'una cerca sobre un tema diferent.

5. Executa la cerca i, si el primer intent no dona el resultat esperat, retoca un únic operador cada vegada (no tots alhora) per entendre quin canvi ha millorat o empitjorat els resultats.

Comodins i intervals numèrics

El comodí (representat amb un asterisc) serveix per a frases de les quals no recordem una paraula exacta, per exemple "la llei * de la funció pública": el cercador entén que hi falta una paraula concreta dins d'una frase que, per la resta, es recorda amb precisió, i la substitueix per qualsevol terme que completi un resultat real. L'interval numèric (escrit com `2020..2026`, amb dos punts seguits sense espais) és útil per acotar per anys sense haver de repetir la cerca cada vegada, per exemple per trobar convocatòries publicades entre dos anys concrets sense haver de fer una cerca diferent per a cadascun.

Truc per a l'examen: l'interval numèric es reconeix perquè sempre porta els dos punts seguits (`..`) entre dues xifres, mai un guionet; amb un guió (`2020-2026`) no és l'operador d'interval, és només text normal.

Font primària i font secundària

Un usuari expert sap, a més, distingir entre fer una cerca i verificar-la amb una segona via independent. Si l'objectiu és trobar el text vigent d'una norma, la cerca es pot acotar per domini oficial (`site:boe.es` o `site:dogc.gencat.cat`), però la confirmació final s'ha de fer contra la font primària: el diari oficial, no un resum periodístic. Aquesta distinció entre font primària (el document original, l'acta, la sentència, el butlletí oficial) i font secundària (qui l'interpreta o en fa un resum) és una de les competències que més distingeix un usuari avançat d'un usuari mitjà: la secundària és còmoda de llegir, però només la primària té valor probatori si cal citar-la en un informe, en una al·legació o en un recurs administratiu.

A la pràctica, això vol dir que si es llegeix a la premsa que "s'ha publicat una nova taxa municipal", el pas final abans de donar-ho per fet -i abans, per exemple, de fer-hi referència en una reclamació- és anar directament al Butlletí Oficial de la Província (BOP) o al Diari Oficial de la Generalitat de Catalunya (DOGC) i llegir el text exacte de la publicació, amb la data i el número d'edicte concrets.

Cerca acadèmica i especialitzada

La cerca acadèmica i especialitzada té les seves pròpies regles del joc. Google Scholar indexa citacions i permet ordenar per rellevància o per data, però no ho indexa tot: bases com Dialnet, Scopus, Web of Science o el Portal de la Recerca de Catalunya (PRC) donen accés a literatura revisada per parells que Scholar sovint no arriba a cobrir, perquè el seu rastreig és automàtic i no discrimina entre una revista amb revisió científica rigorosa i un document penjat sense cap control de qualitat.

Saber llegir un DOI (identificador digital d'objecte, amb un format del tipus 10.1000/xyz123) permet localitzar un article de manera inequívoca encara que hagi canviat d'URL, cosa que no passa amb un enllaç normal, que es pot trencar si la revista canvia de servidor o de plataforma. Per això, en una bibliografia acadèmica seriosa, sempre és preferible citar pel DOI que per l'adreça web del moment.

Procediment pas a pas: localitzar un article a partir del seu DOI

1. Copia el DOI complet (per exemple, 10.1000/xyz123).
2. Afegeix-lo darrere de l'adreça `https://doi.org/`, de manera que quedi `https://doi.org/10.1000/xyz123`.
3. Enganxa aquesta adreça al navegador i prem Retorn: el sistema redirigeix automàticament a la ubicació actual de l'article, sigui quina sigui la revista o el servidor on estigui allotjat en aquell moment.

Wayback Machine i hemeroteques

Quan un contingut ha desaparegut d'internet o s'ha modificat sense avís, l'eina de referència és la

Wayback Machine de l'Internet Archive: guarda instantànies històriques de milions de pàgines i permet comprovar exactament què deia un lloc web en una data concreta, imprescindible quan algú nega haver publicat una cosa que ara ha esborrat. Les hemeroteques digitals de diaris i biblioteques fan la mateixa funció per a la premsa històrica, i sovint són l'única manera de contrastar com es va informar en el seu moment d'un fet que avui es reinterpreta amb una narrativa diferent.

Procediment pas a pas: recuperar una versió antiga d'una pàgina web

1. Obre `web.archive.org` al navegador.
2. Enganxa l'adreça exacta de la pàgina que vols consultar a la caixa de cerca.
3. El servei mostra un calendari amb els dies en què es va fer una còpia; els dies marcats amb un cercle indiquen que hi ha instantània disponible.
4. Fes clic sobre la data que t'interessa (per exemple, la més propera al dia dels fets que vols verificar) i navega per la còpia com si fos la pàgina original en aquell moment.

Alertes i sindicació de contingut

Les alertes i la sindicació de contingut permeten automatitzar el seguiment: en lloc de tornar a cercar cada setmana, es configura una alerta a Google Alerts amb el terme exacte que interessa, o se subscriu un lector de canals RSS a la font oficial d'un butlletí, i la informació nova arriba sola sense haver de recórrer manualment cap pàgina.

Procediment pas a pas: configurar una alerta a Google Alerts

1. Entra a `google.com/alerts` amb el teu compte de Google.
2. Escriu a la caixa superior el terme exacte que vols vigilar (per exemple, el nom d'una convocatòria d'oposicions).
3. Fes clic a "Mostra opcions" per triar la freqüència (a mesura que passi, com a màxim una vegada al dia o una vegada per setmana), la font (notícies, blogs, tot el web...), l'idioma i la regió.
4. Tria on vols rebre l'avís (normalment "Per correu electrònic") i prem "Crea alerta".
5. Cada vegada que aparegui contingut nou que coincideixi, arribarà un correu automàtic sense haver de tornar a cercar res.

La diferència pràctica entre alertes i RSS és importable a l'examen: l'alerta notifica per correu quan apareix contingut nou que coincideix amb una cerca (una paraula clau), mentre que l'RSS sindica tot el contingut nou d'una font concreta que ja s'ha triat de seguir, sense necessitat que hi hagi una paraula clau de per mig. Dit d'una altra manera: l'alerta vigila un tema a través de tot internet, l'RSS vigila una font sencera.

Errors habituals: confondre l'operador `OR` en minúscules amb el connector lògic (no funciona), oblidar els dos punts seguits sense espais en l'interval numèric, i pensar que `site:` només serveix per a dominis oficials -també funciona amb qualsevol domini, com un blog concret o una xarxa social.

Avaluació crítica de fonts i dades

El nivell avançat exigeix un pas més enllà de "mirar qui ho ha escrit": cal saber verificar-ho de manera activa, amb eines i mètodes concrets, no només amb intuïció.

Qui hi ha darrere una pàgina: la consulta whois

Davant d'una notícia dubtosa, la primera pregunta tècnica és qui és el titular del domini i des de quan existeix. Una consulta whois (o eines web com who.is) revela la data de registre d'un lloc web: una pàgina creada fa tres setmanes que es fa passar per un mitjà consolidat és un indici clar de manipulació.

Procediment pas a pas: fer una consulta whois

1. Obre un navegador i ves a `who.is`.
2. Escriu el domini exacte que vols investigar (per exemple, `nomdelapagina.com`), sense `www` ni `https://`.
3. Prem Retorn: el servei mostra la data de creació del domini, el registrador, i en molts casos el país des d'on s'ha registrat.
4. Compara aquesta data amb el que la pàgina diu ser: si es presenta com un mitjà "de tota la vida" però el domini té tres setmanes, ja tens un primer indici sòlid de manipulació.

Cerca inversa d'imatges i metadades EXIF

La cerca inversa d'imatges (Google Lens, TinEye, Yandex Images) permet saber si una fotografia que circula com a "actual" en realitat és d'un altre esdeveniment o d'un altre any: és la tècnica bàsica per desmuntar bulos visuals durant catàstrofes o conflictes.

Procediment pas a pas: fer una cerca inversa d'imatges amb Google Lens

- Al mòbil (Android o iPhone): obre l'aplicació de fotos o el missatge on hi ha la imatge, comparteix-la a l'aplicació Google, i tria l'opció "Cerca amb Google Lens" (o obre directament l'app Google, toca la icona de la càmera dins la caixa de cerca i selecciona la imatge de la galeria).
- Al navegador d'ordinador (Chrome): fes clic amb el botó dret sobre la imatge i selecciona "Cerca imatge amb Google Lens"; s'obrirà una barra lateral amb resultats visualment semblants i les pàgines on apareix la mateixa imatge, amb dates de publicació que permeten comprovar si és realment recent.

Anant un pas més enllà, les metadades EXIF d'una imatge (model de càmera, data, i de vegades coordenades GPS) es poden consultar amb eines com Jeffrey's Exif Viewer, tot i que cal tenir present que moltes xarxes socials les eliminen en pujar el fitxer, precisament perquè redueixen el pes de la imatge i, de retruc, també eliminen informació que podria comprometre la privacitat de qui l'ha fet.

Procediment pas a pas: consultar les metadades d'una foto sense sortir de l'ordinador (Windows)

1. Localitza el fitxer d'imatge a l'Explorador de fitxers.
2. Fes clic amb el botó dret sobre la imatge i selecciona "Propietats".
3. Ves a la pestanya "Detalls".
4. Baixa fins a l'apartat "Càmera" i "Origen": si hi ha dades de model de càmera, data de captura o coordenades GPS, apareixeran aquí; si el fitxer les ha perdut (per exemple, perquè s'ha descarregat d'una xarxa social), aquests camps sortiran buits.

Geolocalització d'imatges quan no hi ha EXIF

Quan la imatge no porta EXIF útil, la geolocalització d'imatges es fa per mètode indicial: es comparen elements de l'escena (la vegetació, l'alfabet dels rètols, el sentit de circulació, la posició de les ombres a una hora determinada, la silueta d'un edifici de fons) amb imatges de satèl·lit i panoràmiques de carrer per confirmar on i quan es va prendre realment la fotografia.

És la tècnica que fan servir de manera sistemàtica els col·lectius d'investigació en codi obert (OSINT, sigles de open source intelligence), que treballen només amb informació disponible públicament, sense accedir a res privat ni piratejar res: la seva força ve de creuar fonts obertes de manera metòdica, no d'intrusió il·legal. Fer-ho amb finalitats de verificació periodística o acadèmica és legítim; fer-ho per localitzar o assetjar una persona concreta no ho és mai, i aquesta línia ètica hi és sempre present en aquest bloc de la certificació. L'examen sol plantejar precisament aquest matís: no és la tècnica el que fa lícita o il·lícita una cerca OSINT, és la finalitat i el fet que la informació sigui pública.

Detecció de deepfakes i text generat per IA

La detecció d'imatges i vídeos manipulats amb intel·ligència artificial (deepfakes) i de text generat automàticament és una de les competències més noves d'aquest nivell, i també una de les més limitades: no existeix cap detector infal·lible. Alguns indicis visuals ajuden -parpelleig poc natural, dents o dits mal renderitzats, il·luminació inconsistent entre la cara i el fons-, però els models milloren tan ràpid que aquests indicis caduquen en pocs mesos: el que avui delata un vídeo generat per IA, d'aquí a un any pot estar corregit.

Els detectors automàtics de text generat per IA tenen el mateix problema estructural: donen falsos positius amb text escrit per una persona (sobretot si té un estil molt uniforme o correcte) i falsos negatius amb text d'IA que s'ha reescrit o "humanitzat" a posteriori, de manera que cap resultat s'ha de donar per definitiu sense corroborar-lo amb una altra via, com la procedència de l'arxiu, l'historial de versions del document o el context de publicació. Saber explicar aquest límit -que la detecció automàtica és una ajuda, mai una prova concloent- és en si mateix un contingut d'examen que apareix formulat de maneres diferents però que sempre demana la mateixa idea de fons.

Tres conceptes que sovint es confonen: desinformació, informació errònia i malinformació

És important distingir amb precisió tres conceptes que sovint es confonen perquè en català quotidià es fan servir com a sinònims, però a l'examen no ho són:

- La **desinformació** és falsa i es difon amb intenció d'enganyar: qui la comparteix sap que és falsa.
- La **informació errònia** (misinformation) també és falsa, però qui la comparteix ho fa de bona fe, sense saber-ho: comparteix un bulo perquè hi creu, no perquè vulgui manipular ningú.
- La **malinformació** és informació certa que es fa servir amb intenció de fer mal, com filtrar dades privades reals fora de context (per exemple, publicar fotografies autèntiques d'algú, però treient-les del seu context original per perjudicar-lo).

Aquesta distinció apareix sovint als exàmens perquè no és intuïtiva: la clau no és si la informació és certa o falsa, sinó la intenció de qui la difon i, en el cas de la malinformació, l'ús que se'n fa d'una dada que en origen és vertadera.

Biaixos: confirmació i bombolla de filtre

Els biaixos no són només dels autors, també dels sistemes que consumim cada dia. El biaix de confirmació ens porta a buscar (i creure) allò que ja pensàvem, ignorant o restant importància a la informació que el contradiu. La bombolla de filtre és l'efecte pel qual els algorismes de personalització (de xarxes socials, de cercadors, de plataformes de vídeo) ens mostren cada cop més del mateix i menys diversitat de punts de vista, perquè el sistema aprèn què fem clic i ens n'ofereix més, en un cercle que es tanca sobre si mateix sense que ho notem.

Detectar-ho passa per contrastar activament amb fonts de fora de la nostra bombolla habitual -llegir un mitjà amb una línia editorial diferent a la que consumim normalment, per exemple- i per revisar la metodologia darrere de qualsevol dada estadística (mida de la mostra, marge d'error, qui ha finançat l'estudi) abans de donar-la per bona. Un estudi finançat per una empresa amb interès directe en el resultat no és automàticament fals, però mereix una lectura més exigent de la metodologia que un estudi independent.

A Catalunya i l'Estat espanyol, els verificadors de referència (Verificat, Maldita.es, Newtral) publiquen la seva metodologia, cosa que en si mateixa és un senyal de fiabilitat: qui amaga com verifica, normalment no verifica gaire. Un bon hàbit, quan es dubta d'una notícia viral, és comprovar si algun d'aquests

verificadors ja l'ha analitzat abans de compartir-la.

Errors habituals: confondre desinformació amb informació errònia pel simple fet que totes dues són falses (la diferència és la intenció, no la veracitat); assumir que un detector d'IA dona sempre resultats fiables; i oblidar que la bombolla de filtre no és culpa exclusiva de l'usuari, sinó del disseny mateix de l'algorisme.

Gestió avançada de dades: metadades, formats i dades obertes

Estàndards de metadades

Les metadades són "dades sobre les dades" i n'hi ha d'estàndards ben establerts, cadascun pensat per a un tipus de contingut concret:

- **Dublin Core** (títol, autor, data, matèria...) s'utilitza a biblioteques i repositoris digitals per descriure documents de manera homogènia.
- **EXIF** és el propi de les imatges (càmera, data, exposició, i de vegades GPS).
- **ID3** etiqueta els fitxers d'àudio MP3 (artista, àlbum, any, gènere).

Saber-les interpretar és clau tant per organitzar un fons documental com per verificar l'origen d'un fitxer, i l'examen sol demanar associar cada estàndard amb el tipus de contingut que descriu.

Format obert i format propietari

La distinció entre format obert i format propietari és més que teòrica: un format obert (ODT, ODS, CSV, PDF/A) té l'especificació publicada i qualsevol programa la pot implementar sense pagar llicència, mentre que un format propietari (DOCX en les seves versions més tancades, o formats antics com el .wpd de WordPerfect) depèn del fabricant. Per a la preservació a llarg termini, els arxius i les administracions prioritzen formats oberts precisament perquè no depenen que una empresa concreta continuï existint d'aquí a vint anys, ni que mantingui la compatibilitat amb els seus propis formats antics.

PDF/A: com convertir un document per arxivar-lo

Convertir un document a PDF/A -la variant pensada per a arxivament, que incrusta totes les fonts i no permet elements externs- és una pràctica habitual abans de dipositar-lo en un repositori institucional. Aquesta característica ("no permet elements externs") és important: un PDF normal pot enllaçar a un vídeo, un script o un fitxer extern que amb els anys deixa de funcionar; un PDF/A ho evita perquè tot el que necessita per mostrar-se correctament queda incrustat dins del mateix document.

Procediment pas a pas: desar un document com a PDF/A a Word

1. Amb el document obert, ves a "Fitxer" i tria "Exporta" (o "Desa com").
2. Selecciona "Crea PDF/XPS" o, segons la versió, "Desa com a" i tria el tipus "PDF".
3. Fes clic al botó "Opcions".
4. Marca la casella "Compatible amb ISO 19005-1 (PDF/A)" (aquest és el nom tècnic de l'estàndard PDF/A).
5. Accepta i desa el fitxer.

Procediment pas a pas: desar un document com a PDF/A a LibreOffice Writer

1. Amb el document obert, ves a "Fitxer" > "Exporta com a" > "Exporta com a PDF...".
2. A la pestanya "General" de la finestra que s'obre, marca la casella "Formulari PDF/A-2b" (o l'opció PDF/A disponible segons la versió).
3. Fes clic a "Exporta" i tria on desar el fitxer.

Llicències Creative Commons i dades obertes

Les dades obertes (open data) es publiquen amb llicències que en defineixen l'ús. Les més habituals són:

- **CC BY**: exigeix atribució a l'autor original, però permet gairebé qualsevol altre ús, inclòs el comercial.
- **CC BY-SA**: exigeix atribució i, a més, obliga a mantenir la mateixa llicència en qualsevol obra derivada (SA vol dir "share alike", compartir igual).
- **CC0**: és pràcticament domini públic, sense cap restricció ni tan sols la d'atribuir l'autor.

Distingir CC BY de CC BY-SA és un dels punts que més es demanen a l'examen, perquè la diferència sembla petita però té conseqüències legals reals: si es reutilitza un conjunt de dades amb llicència CC BY-SA per crear un producte propi, aquest producte derivat també ha de quedar sota la mateixa llicència, cosa que no passa amb un CC BY normal.

CSV, JSON i XML: tres formats, tres usos diferents

Portals com dadesobertes.gencat.cat, l'Idescat, l'INE (referència estatal), Eurostat (l'equivalent europeu, amb sèries harmonitzades entre estats membres) o data.europa.eu publiquen conjunts de dades reutilitzables en formats com CSV o JSON, que a diferència del PDF són fàcilment processables per una màquina: un PDF és pensat per llegir-lo una persona, un CSV o un JSON és pensat perquè el processi un programa.

A nivell conceptual, val la pena distingir aquests tres formats sense necessitat de programar:

- Un **CSV** (comma-separated values) és una taula en text pla on cada línia és un registre i cada valor va separat per comes: és el format més senzill i el que s'obre directament amb un full de càlcul (Excel o Google Sheets).
- Un **JSON** (JavaScript Object Notation) organitza la informació en parelles de clau i valor, i permet estructures aniuades (una dada dins d'una altra), cosa que el CSV no pot fer bé; és el format que fan servir la majoria d'aplicacions web per intercanviar dades entre si.
- Un **XML** (Extensible Markup Language) fa una funció semblant al JSON però amb etiquetes obertes i tancades a l'estil de l'HTML, i és habitual en àmbits normatius i d'intercanvi entre administracions perquè permet validar l'estructura del document contra un esquema predefinit, garantint que qui rep el fitxer pot comprovar automàticament que compleix el format acordat abans de processar-lo.

Procediment pas a pas: obrir un CSV de dades obertes en un full de càlcul (Excel o Google Sheets)

1. Descarrega el fitxer CSV des del portal de dades obertes (per exemple, dadesobertes.gencat.cat).
2. A Excel: obre l'aplicació, ves a "Dades" > "Des de text/CSV", selecciona el fitxer i confirma el separador (normalment coma o punt i coma, segons la font).
3. A Google Sheets: obre un full nou, ves a "Fitxer" > "Importa" > "Puja", selecciona el fitxer CSV i tria "Reemplaça el full" o "Insereix un full nou".
4. Un cop importades, les dades queden organitzades en columnes com qualsevol altra taula i es poden filtrar, ordenar o convertir en gràfic.

Qualitat de dades

Tenir accés a un conjunt de dades no vol dir que aquest sigui de qualitat. La qualitat de dades s'avalua per dimensions concretes:

- **Exactitud**: el valor és correcte.
- **Completesa**: no falten registres ni camps.
- **Consistència**: les mateixes dades no es contradiuen entre taules o fonts diferents.
- **Actualitat**: la darrera actualització és recent.

- **Unicitat**: no hi ha registres duplicats.

Una taula amb dates buides, valors impossibles (una edat de 200 anys) o duplicats sistemàtics és de baixa qualitat encara que el format sigui perfectament obert i tècnicament correcte: format obert i qualitat de dades són dues coses independents, i l'examen sol posar-hi paranys precisament aquí.

Gràfics: llegir-los i no deixar-se enganyar

Un cop les dades es converteixen en gràfic, la manera de representar-les pot ser honesta o enganyosa sense canviar cap xifra:

- **Retallar l'eix vertical** perquè no comenci a zero exagera visualment diferències petites entre valors, sense que cap dada s'hagi alterat.
- **Fer servir escales de mida** (àrea o volum) en lloc d'escales lineals distorsiona la percepció, perquè l'ull humà no compara àrees o volums de manera proporcional a la diferència real entre els valors.
- **Triar un interval temporal curt i favorable** pot amagar una tendència contrària que només es veuria mirant un període més llarg.

Saber llegir un gràfic críticament -mirar primer els eixos i les unitats abans de fixar-se en la corba o en les barres- és tan rellevant per a l'examen com saber crear-ne un. Un truc pràctic: davant de qualsevol gràfic de barres, mira on comença l'eix vertical abans de reaccionar a la mida aparent de la diferència.

Correlació i causalitat

Lligat a això hi ha un dels errors d'interpretació més freqüents en l'anàlisi de dades: confondre correlació amb causalitat. Que dues variables es moguin juntes (les vendes de gelats i els ofegaments a la platja augmenten alhora a l'estiu) no vol dir que una provoqui l'altra; en aquest exemple, hi ha una tercera variable (la calor) que explica totes dues, i que els estadístics anomenen variable de confusió. Detectar una correlació és el primer pas d'una investigació, no la conclusió, i l'examen sol presentar exemples similars (paraigües i embussos de trànsit, per exemple) demanant identificar la variable oculta que explica totes dues coses alhora.

Anonimització i risc de reidentificació

La protecció de dades personals dins de conjunts oberts es gestiona amb l'anonimització: eliminar o transformar els camps que identifiquen una persona (nom, DNI, adreça) perquè les dades es puguin publicar sense vulnerar-ne la privadesa.

El problema tècnic seriós és la reidentificació: encara que s'elimini el nom, la combinació d'altres camps aparentment innocus (codi postal, data de naixement i sexe) pot ser prou única per identificar de nou una persona quan es creua amb altres fonts públiques. Per exemple, en un municipi petit, la combinació de "dona, nascuda el 1978, codi postal concret" pot correspondre a una sola persona, encara que el seu nom no aparegui enlloc del conjunt de dades. Per això les bones pràctiques de dades obertes no es limiten a esborrar el nom, sinó que apliquen agregació o generalització -per exemple, publicar franges d'edat en lloc de la data exacta de naixement, o publicar només el districte en lloc del codi postal complet- per reduir aquest risc.

Big data: les tres V i la indexació

A nivell conceptual, el big data es descriu clàssicament amb les tres V:

- **Volum**: la quantitat de dades supera la capacitat d'una base de dades tradicional.
- **Velocitat**: les dades es generen i es processen gairebé en temps real, com un flux de sensors o de transaccions.

- **Varietat**: dades estructurades (com una taula) i no estructurades (com un vídeo o un tuit) conviuen al mateix sistema.

No cal saber programar per a l'ACTIC, però sí entendre que la indexació és el mecanisme que permet cercar dins d'aquest volum sense recórrer tota la base cada vegada: és exactament el mateix principi que fa servir un cercador web quan rastreja pàgines -seguint el que permet o prohibeix el fitxer robots.txt- i les organitza en un índex per respondre en mil·lèsimes de segon. El fitxer robots.txt es col·loca a l'arrel d'un lloc web i indica, mitjançant regles senzilles, quines parts del lloc poden rastrejar els robots dels cercadors i quines no; no és una mesura de seguretat (no impedeix físicament l'accés), és una indicació que els robots ben educats respecten voluntàriament.

Errors habituals: pensar que CSV i JSON són intercanviables (el JSON permet estructures aniuades que el CSV no pot representar bé); confondre format obert amb qualitat garantida; i oblidar que la reidentificació és un risc real fins i tot quan s'han eliminat les dades "evidents" com el nom.

Gestió documental experta

Organitzar bé un fons de documents propis o d'un equip de feina és una competència que a nivell avançat es tradueix en hàbits concrets, no en bona voluntat genèrica.

Convencions de noms de fitxer i control de versions

Una convenció de noms de fitxer coherent -per exemple, AAAAMMDD_projecte_versió (20260726_informe_v2.pdf)- permet que l'ordenació alfabètica coincideixi amb la cronològica i que qualsevol persona de l'equip sàpiga, només llegint el nom, de quin document es tracta sense obrir-lo. El control de versions manual (v1, v2, v2_final, v2_final_definitiu) és precisament l'error que aquesta convenció ha d'evitar: quan cada persona afegeix el seu propi sufix ("_final", "_revisat", "_bo_de_veritat"), ningú sap del cert quin és el document vigent. Cal un criteri únic -número de versió incremental més data- perquè no hi hagi mai dubte de quin és el document que cal fer servir.

Procediment pas a pas: aplicar una convenció de noms senzilla en una carpeta compartida

1. Defineix el format abans de començar a treballar: per exemple, AAAAMMDD_nomprojecte_vX.
2. Renomena els fitxers existents seguint aquest format (a Windows, es pot seleccionar el fitxer, prémer F2, i escriure el nom nou).
3. Cada vegada que es faci una revisió substancial, incrementa el número de versió (v1 a v2) en lloc d'afegir paraules com "final".
4. Si cal indicar que una versió és la definitiva, afegeix-ho com a estat explícit al final ("_APROVAT"), mai com un sufix ambigu que es pugui confondre amb una simple opinió de qui l'ha revisat.

Metadades pròpies i cerca avançada d'escriptori

Més enllà del nom del fitxer, els sistemes operatius i els gestors documentals permeten afegir metadades pròpies -autor, matèria, paraules clau, estat de revisió- que després es poden explotar amb cerca avançada dins del propi ordinador o repositori: la majoria de cercadors d'escriptori i de gestors documentals entenen sintaxi de camp semblant a la dels cercadors web (per exemple, restringir per tipus d'arxiu, per interval de dates de modificació o per autor). Saber fer-ho estalvia haver de navegar carpeta per carpeta quan el volum de documents creix.

Procediment pas a pas: afegir metadades a un document de Word i cercar-lo després

1. Amb el document obert, ves a "Fitxer" > "Informació".
2. A l'apartat "Propietats", fes clic sobre camps com "Etiquetes" o "Comentaris" i afegeix les paraules

clau que et permetran retrobar el document.

3. Desa el document.

4. Més endavant, a l'Explorador de fitxers de Windows, escriu a la caixa de cerca `etiquetes:paraula-clau` (o el terme equivalent segons la versió) per localitzar tots els documents que comparteixen aquesta etiqueta, encara que estiguin en carpetes diferents.

OCR: convertir un escanejat en text cercable

Un document escanejat com a imatge no és cercable: si s'ha digitalitzat un contracte en paper i s'ha guardat com a PDF d'imatge, el text que hi apareix no es pot seleccionar ni buscar, per molt que a simple vista sembli un document normal. L'OCR (reconeixement òptic de caràcters) resol això analitzant la imatge i convertint-la en text reconeixible per l'ordinador, de manera que el document escanejat passa a ser cercable com qualsevol altre fitxer de text; és el pas imprescindible quan es digitalitza un arxiu en paper amb voluntat de conservar-lo de debò, no només d'emmagatzemar-lo.

Un cas pràctic molt habitual: es rep la factura de la llum escanejada com a PDF d'imatge, sense text seleccionable. Per poder-la cercar després per l'import o la data sense obrir-la una a una, cal passar-la per un procés d'OCR abans de desar-la definitivament.

Procediment pas a pas: aplicar OCR a un document escanejat

1. Obre el PDF escanejat amb un lector que inclogui OCR (per exemple, Adobe Acrobat, o l'opció de Google Drive descrita a continuació).
2. Amb Google Drive: puja el PDF o la imatge al Drive, fes-hi clic amb el botó dret, tria "Obre amb" > "Google Docs". Google Docs converteix automàticament el text reconegut en un document editable i cercable, conservant també una còpia de la imatge original a sota.
3. Revisa el text resultant: l'OCR no és perfecte, especialment amb lletra manuscrita o escanejats de baixa qualitat, així que cal repassar els números importants (imports, dates, DNI) abans de donar el document per bo.
4. Desa el resultat, ja sigui com a document de text o tornant-lo a exportar com a PDF cercable.

Cicle de vida del document

Tot document té un cicle de vida que va més enllà de crear-lo i desar-lo: es crea, es tramita o es revisa, s'arxiva quan deixa de ser d'ús actiu però encara pot caldre consultar-lo, i finalment es conserva de manera permanent o es destrueix segons el calendari de conservació aplicable (en l'àmbit públic, marcat per normativa d'arxius). Gestionar bé aquest cicle vol dir no barrejar en una mateixa carpeta els documents en tràmit actiu amb els ja tancats, i tenir clar quan un document deixa de ser útil dia a dia però encara té valor legal que obliga a conservar-lo -per exemple, les factures d'una activitat professional, que cal conservar diversos anys encara que ja no es consultin mai més en el dia a dia.

Errors habituals: confondre "arxivar" amb "esborrar" (un document arxivat encara pot caldre consultar-lo o té obligació legal de conservació); i oblidar que l'OCR converteix la imatge en text cercable, però no substitueix la imatge original com a prova, sobretot quan cal conservar l'aspecte exacte d'un document signat.

Núvol i sincronització a fons

Treballar amb serveis al núvol (Google Drive, OneDrive, Dropbox) sembla senzill fins que dos dispositius editen el mateix fitxer alhora sense connexió i el servei ha de decidir què fer.

Conflictes de sincronització

Quan això passa, apareix un conflicte de versions, que la majoria de serveis resolen creant una còpia paral·lela amb el nom original i un sufix (com "nom (conflicte de còpia d'algú)"), deixant a la persona usuària la feina de comparar-les i triar-ne una. Saber que això passarà tard o d'hora, i què fer quan passi, evita perdre feina per pànic o sobreescriptura accidental.

Procediment pas a pas: resoldre un conflicte de sincronització a Google Drive

1. Quan aparegui un fitxer duplicat amb un sufix del tipus "(conflicte de còpia d'algú)", obre totes dues versions.
2. Compara els canvis: si un dels dos fitxers només afegeix contingut al final, sovint la solució més ràpida és copiar aquest fragment nou dins de la versió que es vol conservar.
3. Un cop decidit quina versió és la bona, desa-la amb el nom original i elimina la còpia sobrant, però no ho facis fins haver comprovat que no es perd cap canvi important de l'altra versió.
4. Per evitar-ho en el futur, activa la comprovació de connexió abans d'editar documents sensibles en mode sense connexió, o treballa directament sobre documents natius del núvol (Google Docs, per exemple), que gestionen l'edició simultània en temps real en lloc de crear conflictes.

Còpia local o fitxers en flux

Aquests serveis ofereixen dues maneres de tenir els fitxers al dispositiu:

- La **còpia local**, que descarrega i manté sempre una rèplica completa a l'ordinador: ocupa espai en disc, però funciona sense connexió a internet.
- El **mode de fitxers en flux o streaming** (Files On-Demand, a OneDrive; Smart Sync, a Dropbox), que mostra tots els fitxers com si hi fossin però només els descarrega de debò quan s'obren, estalviant espai a canvi de necessitar connexió per accedir-hi de debò.

Triar una opció o l'altra depèn de l'espai disponible al disc i de si es preveu treballar sense internet (per exemple, en un desplaçament llarg o en una zona sense cobertura).

Procediment pas a pas: activar Files On-Demand a OneDrive (Windows)

1. Fes clic a la icona d'OneDrive a la safata del sistema (a prop del rellotge).
2. Ves a "Ajuda i configuració" > "Configuració".
3. A la pestanya "Configuració", marca la casella "Estalvia espai i baixa els fitxers a mesura que els utilitzis".
4. A partir d'ara, els fitxers apareixeran a l'Explorador amb una icona de núvol (encara no descarregats), de disc (ja descarregats localment) o de check verd (marcats perquè estiguin sempre disponibles sense connexió).

Xifratge en trànsit, en repòs i d'extrem a extrem

La seguretat d'aquestes dades es descriu amb dos conceptes que convé no confondre:

- El **xifratge en trànsit** protegeix la informació mentre viatja entre el dispositiu i els servidors del proveïdor, típicament amb el protocol HTTPS/TLS.
- El **xifratge en repòs** protegeix la informació mentre està emmagatzemada als servidors del proveïdor, evitant que algú amb accés físic o lògic als discos la pugui llegir directament.

Que un servei ofereixi tots dos no vol dir que el proveïdor no hi pugui accedir: només el **xifratge d'extrem a extrem**, on la clau només la té l'usuari, impedeix que el mateix proveïdor pugui llegir el contingut si li ho demanen. Aquest matís -que xifratge en trànsit i en repòs no equivalen a privacitat total davant del propi proveïdor- és una pregunta trampa habitual a l'examen.

Vendor lock-in i portabilitat de dades

Dipositar tota la informació en un únic servei crea dependència del proveïdor (vendor lock-in): com més integrat queda el flux de treball amb les eines d'una empresa concreta, més costa marxar-ne, encara que després pugi el preu o canviï les condicions. La portabilitat de dades és la capacitat de fer el contrari: exportar la informació en un format obert i reutilitzable per traslladar-la a un altre servei sense perdre'n l'estructura.

El Reglament general de protecció de dades (RGPD) recull explícitament el dret a la portabilitat, precisament per contrarestar aquesta dependència: qualsevol servei seriós ha d'oferir una manera d'exportar les dades pròpies en un format estàndard, com el CSV o el JSON ja explicats abans. Aquest dret és un dels pocs punts de l'RGPD que apareix de manera recurrent dins del temari d'alfabetització informacional, precisament perquè connecta la protecció de dades amb la gestió pràctica de fitxers.

Errors habituals: pensar que un servei xifrat "en trànsit i en repòs" garanteix privacitat total (no és així si el proveïdor té la clau); i confondre la còpia local amb una còpia de seguretat real -sincronitzar no és el mateix que fer backup, perquè si s'esborra un fitxer al núvol, també desapareix de la còpia local sincronitzada.

Curació de continguts

Seguir moltes fonts d'informació sense ofegar-se en el soroll és, en si mateix, una habilitat que es pot sistematitzar amb les eines adequades.

RSS i lectors de feeds

Els canals RSS, ja esmentats a l'apartat de cerca, són la peça central d'aquesta curació: en lloc de visitar cada dia deu pàgines web diferents per veure si hi ha novetats, un lector de feeds (com Feedly) reuneix totes les actualitzacions en un sol lloc, organitzades per carpetes temàtiques, i permet marcar com a llegit allò que ja s'ha revisat.

Procediment pas a pas: subscriure's a un canal RSS amb Feedly

1. Crea un compte a Feedly (feedly.com) o inicia sessió.
2. Fes clic a "Add Content" (o l'equivalent en català, "Afegeix contingut").
3. Escriu el nom del lloc web que vols seguir, o directament la seva adreça RSS si la coneixes.
4. Tria la font correcta d'entre els resultats suggerits i fes clic a "Follow" (Segueix).
5. Assigna-la a una carpeta temàtica (per exemple, "Oposicions" o "Administració") perquè quedi organitzada des del primer moment i no barrejada amb la resta.

Marcadors organitzats amb etiquetes

Els marcadors (favorits) del navegador, quan es deixen créixer sense estructura, es tornen inservibles al cap de poc temps: una llista de dos-cents enllaços sense ordre no serveix de res. Organitzats en carpetes temàtiques i, més encara, amb etiquetes (tags) que permeten que un mateix recurs aparegui sota més d'un criteri de cerca, es converteixen en una eina real.

Procediment pas a pas: organitzar els marcadors a Chrome

1. Fes clic a la icona de l'estrella a la barra d'adreces per desar la pàgina actual, o obre el gestor complet amb el menú de tres punts > "Marcadors i llistes" > "Gestor de marcadors".
2. Dins del gestor, crea carpetes temàtiques amb el botó dret > "Afegeix carpeta nova".
3. Arrossega els marcadors existents cap a la carpeta corresponent.

4. Revisa periòdicament la llista (per exemple, un cop al trimestre) i elimina els enllaços trencats o que ja no siguin útils; un gestor de marcadors que no es depura mai acaba sent tan inservible com no tenir-ne cap.

Alguns serveis externs de curació (Pocket, Raindrop) afegeixen la cerca de text complet dins del contingut guardat, no només pel títol: és a dir, permeten trobar un article desat encara que no recordis com es titulava, només perquè conté una paraula concreta dins del text.

Gestors de referències bibliogràfiques

Quan la informació que cal gestionar són referències bibliogràfiques -articles, llibres, informes- els gestors de referències com Zotero, Mendeley o EndNote permeten desar la fitxa completa d'una font (autor, any, títol, DOI) amb un sol clic des del navegador, organitzar-la en col·leccions temàtiques i generar automàticament la citació i la bibliografia final en el format que calgui (APA, Vancouver, ISO 690) sense teclejar-la a mà.

Procediment pas a pas: desar una referència amb el connector de Zotero al navegador

1. Instal·la l'extensió "Zotero Connector" al navegador (disponible per a Chrome i Firefox).
2. Navega fins a la pàgina de l'article o del llibre que vols desar.
3. Fes clic a la icona de Zotero que apareix a la barra d'adreces: canvia de forma segons el tipus de contingut detectat (un full per a un article, un llibre per a un llibre).
4. La referència es desa automàticament amb totes les dades bibliogràfiques a la teva biblioteca de Zotero, organitzada per col·leccions.
5. Quan calgui redactar la bibliografia, selecciona les referències desades i tria "Crea una bibliografia des dels elements", indicant l'estil de citació (APA, Vancouver...) que exigeixi el treball.

No cal dominar-los a fons per a l'ACTIC, però sí saber què resolen: eviten l'error de citar malament una font i estalvien hores quan un treball ha de justificar cadascuna de les seves afirmacions.

Errors habituals: deixar créixer els marcadors sense mai organitzar-los; i no distingir entre un lector RSS (que agrupa fonts senceres ja triades) i una alerta de cerca (que vigila una paraula clau a tot internet).

Còpia de seguretat i preservació digital

La regla 3-2-1

La referència bàsica en aquest bloc és la regla 3-2-1: mantenir com a mínim tres còpies de la informació, en dos suports diferents, amb una còpia fora de la ubicació física original (per exemple, al núvol o en un disc a un altre edifici). No és un caprici tècnic: si es guarden totes les còpies al mateix disc dur i aquest falla, les tres còpies desapareixen alhora, perquè en realitat només hi havia una còpia física, encara que estigués duplicada tres vegades dins del mateix suport.

Procediment pas a pas: aplicar la regla 3-2-1 a l'entorn domèstic

1. Còpia número u: els fitxers originals a l'ordinador de casa.
2. Còpia número dos: una còpia en un disc dur extern connectat només durant la còpia (per evitar que un virus o un error afecti alhora l'original i la còpia).
3. Còpia número tres: una còpia al núvol (Google Drive, OneDrive o similar), que compleix alhora el requisit de "fora de la ubicació original".
4. Amb això ja es tenen tres còpies (original + disc extern + núvol), en dos suports diferents (disc local i núvol) i una còpia fora de casa (el núvol).

Tipus de còpia: completa, incremental i diferencial

Cal distingir els tipus de còpia:

- Una **còpia completa** duplica tota la informació cada vegada: ocupa més espai i triga més, però és la més senzilla de restaurar perquè tot és en un sol lloc.
- Una **còpia incremental** només guarda els canvis des de l'última còpia, sigui completa o incremental: ocupa poc espai, però restaurar-la exigeix recórrer tota la cadena de còpies en ordre, una darrere l'altra.
- Una **còpia diferencial** guarda els canvis des de l'última còpia completa: ocupa més que la incremental, però es restaura més ràpid perquè només calen dos fitxers, la completa i l'última diferencial.

Truc per a l'examen: pensa en la incremental com una cadena (cal tots els esglaons per arribar dalt) i en la diferencial com un salt directe (només cal el punt de partida i el punt final). Si l'examen pregunta quina és més ràpida de restaurar entre incremental i diferencial, la resposta gairebé sempre és la diferencial, precisament perquè no depèn d'una cadena sencera de fitxers intermedis.

Procediment pas a pas: activar còpies de seguretat automàtiques a Windows

1. Ves a "Configuració" > "Actualització i seguretat" > "Còpia de seguretat" (a versions més noves, "Configuració" > "Sistema" > "Emmagatzematge" > "Opcions de còpia de seguretat avançades").
2. Connecta un disc dur extern i activa "Historial de fitxers" o "Fes una còpia de seguretat mitjançant l'historial de fitxers".
3. Configura la freqüència (per defecte, cada hora) i quant de temps es conserven les versions antigues.
4. Revisa periòdicament que el disc extern segueixi connectat i amb espai suficient; una còpia de seguretat que fa mesos que no s'executa perquè el disc ha estat desconnectat no serveix de res quan realment es necessita.

RAID: què és i què no substitueix

El RAID (Redundant Array of Independent Disks) és una tècnica a nivell de maquinari que distribueix o duplica dades entre diversos discos per tolerar la fallada d'un d'ells sense perdre informació; és una mesura de disponibilitat, no substitueix mai una còpia de seguretat real, perquè si algú esborra un fitxer per error, el RAID replica l'esborrat als altres discos igual de ràpid. Aquest és, probablement, el parany més repetit de tot aquest bloc a l'examen: RAID protegeix contra la fallada física d'un disc, no contra un error humà, un virus o un atac de xifratge maliciós, que es propaguen a tots els discos del conjunt exactament igual.

Verificació amb funcions hash

Per comprovar que una còpia no s'ha corromput en el trasllat, s'utilitzen funcions resum o hash (com SHA-256): es calcula el resum de l'arxiu original i, després de copiar-lo, es torna a calcular; si els dos valors coincideixen, el fitxer és idèntic bit a bit. És el mateix principi que permet verificar que un programa descarregat no ha estat manipulat pel camí, comparant el hash que publica l'autor original amb el que resulta del fitxer que realment s'ha descarregat.

Procediment pas a pas: calcular el hash SHA-256 d'un fitxer a Windows

1. Obre l'aplicació "Símbol del sistema" (o "PowerShell").
2. Escriu `certutil -hashfile "ruta\completa\del\fitxer" SHA256` i prem Retorn.
3. El sistema mostra una llarga cadena de lletres i xifres: aquest és el hash del fitxer.
4. Compara aquesta cadena amb la que hagi publicat la font original (per exemple, a la pàgina de descàrrega); si coincideixen exactament, el fitxer no s'ha alterat ni corromput pel camí.

Historial de versions

Per comprovar que una còpia no s'ha corromput en el trasllat, cal també saber que un sistema de còpies de seguretat que manté un historial de versions -i no només l'últim estat dels fitxers- aporta un valor afegit important: permet recuperar un fitxer tal com estava en un moment anterior, imprescindible si un atac de xifratge maliciós (per exemple, un ransomware que xifra tots els documents i en demana un rescat) ha corromput l'última còpia. Si el sistema de còpia només conservés l'última versió, i aquesta darrera versió ja estigués xifrada per l'atac, la còpia de seguretat també quedaria inservible; amb un historial de versions, sempre es pot tornar a un punt anterior a la infecció.

Preservació digital a llarg termini

Finalment, la preservació digital a llarg termini és un problema diferent del de la còpia de seguretat setmanal: consisteix a garantir que un document encara es pugui obrir d'aquí a trenta anys, quan potser ja no existeixi el programa que el va crear ni, fins i tot, el sistema operatiu sobre el qual funcionava.

Les estratègies passen per:

- Triar formats oberts i ben documentats (els mateixos ODT, ODS, CSV i PDF/A ja explicats en aquest capítol).
- Migrar periòdicament els fitxers a formats vigents abans que els antics quedin obsolets, en lloc d'esperar que un format desaparegui del tot i s'hagi de fer una recuperació d'emergència.
- En el cas d'institucions, fer servir sistemes distribuïts com LOCKSS ("Lots of Copies Keep Stuff Safe"), que mantenen còpies redundants entre diverses biblioteques perquè cap fallada puntual faci perdre el fons documental.

L'acrònim LOCKSS és, per si sol, una pregunta habitual d'examen: "moltes còpies mantenen les coses segures" resumeix tota la filosofia de la preservació digital institucional, que no confia mai en una única còpia ni en un únic responsable.

Errors habituals: confondre RAID amb còpia de seguretat (el RAID no protegeix contra l'esborrat accidental ni contra un virus); pensar que la còpia incremental sempre és millor perquè ocupa menys espai (a canvi, la restauració és més lenta i més fràgil, perquè depèn de tota la cadena); i oblidar que una còpia de seguretat setmanal no equival a una estratègia de preservació digital a llarg termini, que exigeix a més triar formats oberts i migrar-los periòdicament.

TEMA 2

Àrea 2. Comunicació i col·laboració

Comunicació professional: correu, canals i reunions

Triar el canal segons urgència i traçabilitat

Un professional que coordina un equip no fa servir sempre el mateix canal: tria segons la urgència real de la resposta i la necessitat que la conversa quedi registrada. La comunicació síncrona (trucada, videotrucada, xat en directe) exigeix que les dues parts hi siguin al mateix moment i té sentit per decidir alguna cosa de seguida o resoldre un dubte que amb text es faria etern. L'asíncrona (correu, un comentari en un document, una tasca anotada en un tauler) no obliga la persona destinatària a respondre a l'instant i deixa un rastre escrit consultable més endavant, cosa que una trucada o un missatge de veu no ofereixen igual.

La regla pràctica: si cal resposta immediata sobre un tema puntual, canal síncron; si el que importa és que la decisió quedi documentada, canal asíncron amb traçabilitat. Pensa en un cap d'equip que ha de canviar l'horari d'una reunió de demà a primera hora i necessita confirmació ja: aquí no té sentit obrir un fil de correu que potser ningú llegirà fins l'endemà, el que toca és trucar o obrir un xat en directe, perquè la urgència real exigeix resposta ràpida i el contingut és puntual, no una decisió que calgui consultar d'aquí a sis mesos.

Eines com Slack o Microsoft Teams organitzen la comunicació en canals, agrupats per projecte o equip i no per persona. Dins d'un canal es poden obrir fils per respondre a un missatge concret sense trencar la conversa principal (a Slack, «Reply in thread»; a Teams, «Respon»), de manera que qui entra hores després pot seguir el debat sense haver de rellegir cinquanta missatges intercalats. Les mencions (arrova més el nom d'una persona, per exemple @maria, o d'un canal sencer amb @canal o @equip) serveixen per cridar l'atenció puntual d'algú sense obligar-lo a llegir-ho tot: si mencionar algú es fa servir per a qualsevol cosa, l'usuari acaba silenciant les notificacions i el sistema deixa de funcionar.

Un error habitual, i que es paga car, és prendre per missatge directe privat decisions que afecten tot l'equip. Un membre de l'equip que comunica per xat privat a un company que a partir d'ara es canvia un procediment de treball genera un problema concret: es perd la traçabilitat de la decisió quan algú canvia de rol o s'incorpora nou al projecte, perquè ningú més la pot consultar ni entendre per què es va prendre. La bona pràctica és documentar la decisió al canal de l'equip, encara que la conversa prèvia de matisar-la s'hagi fet en privat: primer es parla en privat si cal, però la conclusió es publica on tothom hi té accés.

Truc per a l'examen: quan una pregunta et planteja «urgència i necessitat de resposta immediata», la resposta correcta sol ser el canal síncron (trucada o xat en directe); quan parla de «que quedi constància» o «documentar per a més endavant», la resposta correcta és l'asíncron amb traçabilitat.

Un altre exemple del dia a dia que ajuda a fixar el criteri: si vols demanar hora al CAP, no cal cap canal síncron amb una persona, n'hi ha prou amb el portal de cita prèvia, perquè no hi ha cap decisió que negociar, només reservar un forat en una agenda. En canvi, si el que necessites és que la infermera et confirmi si has d'anar en dejú per a una analítica programada per demà, aquí sí que convé un canal síncron (una trucada al centre), perquè el dubte és urgent i la resposta condiciona què fas en les properes hores. El mateix raonament s'aplica a l'entorn laboral: no tota pregunta necessita una trucada, i no tota

decisió es pot tancar bé amb un missatge de xat que ningú tornarà a trobar d'aquí a un mes.

El correu a nivell expert: filtres i regles que treballen soles

A nivell avançat el correu no es gestiona missatge a missatge, es gestiona amb regles. Un filtre defineix una condició (remitent, assumpte, paraules del cos, mida de l'adjunt) i una acció que es dispara sola: etiquetar, arxivar, reenviar, esborrar o respondre amb un model. Aquí hi ha un matís que sovint es passa per alt a l'examen: a Gmail els filtres s'executen al servidor de Google, per tant funcionen encara que no tinguis cap dispositiu obert; a Outlook, en canvi, hi ha regles de servidor i regles «només d'aquest ordinador», i aquestes últimes no s'apliquen si el client no està en marxa.

Per crear un filtre a Gmail des de l'ordinador:

1. Obre Gmail i fes clic a la fletxa cap avall que hi ha dins la barra de cerca, a la dreta.
2. Omple els camps que defineixen la condició (De, Assumpte, Conté les paraules...) i fes clic a «Crea un filtre».
3. Marca l'acció que vols que es dispari (Aplica l'etiqueta, Arxiva, Reenvia a, Suprimeix, Marca com a llegit) i fes clic a «Crea el filtre».
4. Opcionalment, marca «Aplica-ho també als N missatges de conversa que coincideixen» perquè el filtre actuï també amb retroactivitat sobre correus ja rebuts.

A Outlook (aplicació d'escriptori), el camí és Fitxer > Gestiona les regles i alertes > Regla nova, on tries la condició de partida (per exemple «missatges d'algú») i encadenes les accions. La casella clau és si la regla es marca com a regla de servidor (s'executa a Microsoft 365 encara que Outlook estigui tancat) o com a regla client (necessita el programa obert i en execució). Un exemple real: un funcionari que rep còpia de totes les entrades d'un registre pot crear una regla que busqui el domini del registre al remitent i etiqueti el missatge com «Tramitació» sense arxivar-lo, per seguir-lo veient a la safata mentre resol l'expedient.

Les regles s'encadenen: primer les de bloqueig o spam, després les d'organització. Si dues regles es contradiuen (una arxiva el missatge, l'altra el manté a la safata), sol guanyar l'ordre en què estan definides dins la llista de regles del client o servidor, no la lògica que un esperaria, i això genera errors freqüents en entorns amb moltes regles heretades d'anys anteriors. Truc per a l'examen: si et pregunten per què un filtre «no funciona» quan l'ordinador és apagat a Outlook, pensa primer si és una regla de client; a Gmail, en canvi, aquest problema no existeix perquè tot corre al núvol.

Un cas pràctic senzill: si cada mes reps la factura de la llum per correu i vols que s'etiqueti sola i s'arxivi sense passar per la safata d'entrada (perquè no cal que la llegeixis, només guardar-la), pots crear un filtre amb la condició «De: la-teva-companyia-electrica.com» i «Assumpte conté: factura», i com a acció «Aplica l'etiqueta Subministraments» més «Omet la safata d'entrada (arxiva-la)». D'aquesta manera la factura queda ordenada i localitzable sense que hagis de fer res cada vegada que arriba. Aquest tipus d'automatització (regla de baix risc, condició clara, acció reversible) és exactament el que es pregunta quan un examen parla de «gestionar el correu de manera eficient a nivell avançat».

Reunions que no fan perdre temps

Una reunió convocada sense ordre del dia previ tendeix a allargar-se i acaba sense cap conclusió operativa. L'ordre del dia s'envia amb antelació, amb els punts concrets a tractar i, si cal, els documents de referència, perquè cada assistent hi arribi ja llegit i la reunió es dediqui a decidir. Abans de convocar-la, val la pena preguntar-se si de debò cal síncrona: moltes qüestions es resolen igual de bé amb un document compartit i un termini de comentaris.

Passos habituals per convocar una reunió eficaç amb una eina com Google Calendar o Outlook:

1. Crea l'esdeveniment amb data, hora i durada realista (no per defecte una hora si en calen quinze minuts).
2. Adjunta el document amb l'ordre del dia a la invitació, no el descrigueis només al cos del missatge.
3. Convida només les persones que han de decidir alguna cosa; a la resta se'ls pot enviar l'acta després.
4. Activa el recordatori i, si l'eina ho permet, demana confirmació d'assistència perquè es pugui reorganitzar si algú clau no hi pot ser.

Durant la reunió, algú pren nota en un document compartit en temps real, no en privat per repartir-lo després, de manera que qui no hi assisteix pot seguir-la igualment. L'acta final no ha de recollir la conversa sencera: transcriure-la paraula per paraula és un error habitual a nivell avançat perquè es converteix en un document il·legible que ningú torna a consultar. L'acta ha de recollir les decisions preses, la persona responsable de cada acció i el termini, res més. Aquesta acta, arxivada amb data i participants, és la prova a la qual es recorre setmanes després quan algú pregunta per què es va decidir una cosa concreta, per exemple si un ajuntament ha de justificar per què va triar un proveïdor determinat per a un servei.

Treball col·laboratiu al núvol: documents compartits

Permisos, jerarquia i compartició segura

Els núvols documentals (Google Drive, OneDrive, Nextcloud institucional) distingeixen diversos nivells de permís sobre un mateix fitxer: lector, comentarista i editor, i per sobre de tots, el propietari, que és l'única persona que pot canviar permisos d'altri o eliminar el fitxer definitivament. Un usuari amb permís de comentarista sobre un full de càlcul pot afegir comentaris i suggeriments, però no pot modificar directament el contingut ni els permisos: aquesta distinció es pregunta sovint perquè es confon amb «editor», que sí que pot canviar el contingut però tampoc pot tocar els permisos ni esborrar el fitxer.

Per compartir un document a Google Drive:

1. Amb el document obert, fes clic a «Comparteix» a la cantonada superior dreta.
2. Escriu el correu de la persona (o persones) amb qui vols compartir-lo i tria el seu rol al desplegable: Lector, Comentarista o Editor.
3. Si en comptes de persones concretes fas clic a «Canvia a qualsevol persona amb l'enllaç», tria també el rol i copia l'enllaç per enviar-lo.
4. Per afegir caducitat o contrasenya a un enllaç (funcionalitat disponible en comptes d'organització), obre la configuració avançada de l'enllaç compartit.

Compartir amb «qualsevol persona amb l'enllaç» no és el mateix que compartir amb persones concretes: amb l'enllaç obert, qualsevol que el rebi (fins i tot per reenviament no autoritzat) hi pot accedir, mentre que amb usuaris concrets identificats l'accés queda restringit als comptes triats. Per això les administracions solen exigir enllaços amb caducitat o amb contrasenya per a documents sensibles: si una administració ha de compartir externament un document amb dades personals, la pràctica adequada a nivell avançat és generar un enllaç amb data de caducitat o protegit amb contrasenya, en lloc d'un enllaç obert permanent que ningú controla un cop surt de la safata d'entrada original. Aquesta jerarquia és granular a propòsit: un col·laborador extern pot rebre permís de comentarista sobre un únic document sense que això li obri cap altra carpeta de l'espai de treball.

A OneDrive el procediment és molt semblant, amb noms lleugerament diferents: amb el fitxer seleccionat, fas clic a «Comparteix», tries entre «Persones que hi treballen» (usuaris concrets, amb accés a Edició o

Visualització) o «Qualsevol persona amb l'enllaç», i des de «La configuració del vincle pot canviar-se» pots fixar-hi una data de caducitat o exigir una contrasenya, especialment recomanable si es tracta d'un pressupost, un contracte o qualsevol document amb dades personals de tercers. Un error habitual, tant a Drive com a OneDrive, és compartir «amb tothom que tingui l'enllaç» per comoditat quan en realitat només calia compartir-ho amb dues persones concretes: sembla més ràpid en el moment, però deixa el document exposat a qualsevol reenviament posterior que ja no es pot controlar ni desfer.

Coedició en temps real i control de versions

La coedició en temps real permet que diverses persones treballin sobre el mateix full o document alhora; el sistema resol els conflictes caràcter a caràcter i mostra el cursor de cada usuari amb un color diferent, de manera que es veu qui escriu on en cada moment. Això és útil, per exemple, quan diversos tècnics d'un ajuntament omplen alhora un mateix formulari de seguiment d'un expedient sense haver-se de repartir còpies del fitxer per correu.

La coedició no substitueix el control de versions, que és un mecanisme diferent i complementari. A Google Docs, Fulls o Presentacions, l'historial es consulta a Fitxer > Historial de versions > Veure historial de versions; a Word i Excel amb OneDrive, des de Fitxer > Informació > Historial de versions. Aquest historial guarda instantànies senceres del document i permet:

1. Navegar cronològicament per les versions anteriors, agrupades sovint per data i persona.
2. Obrir una versió antiga sense perdre la versió actual.
3. Restaurar aquella versió com a versió vigent amb un sol clic, recuperant tot el document tal com era, no només l'última acció desfeta.

La diferència essencial entre les dues coses és aquesta: la coedició permet treballar diverses persones alhora sobre el document; el control de versions permet recuperar estats anteriors complets del fitxer. En un entorn de treball d'oposicions o de tramitació administrativa aquesta diferència és clau: la coedició evita duplicar fitxers (ningú necessita enviar «versió_final_definitiva_2.docx» per correu), i l'historial de versions evita perdre feina quan algú esborra per error un bloc sencer del document, ja que es pot tornar a un punt anterior a l'error sense haver de refer-ho de memòria.

Espais d'equip, plantilles corporatives i fluxos d'aprovació

Més enllà dels fitxers compartits un per un, les organitzacions creen espais compartits d'equip: un Drive compartit a Google Workspace, un Team a Microsoft Teams o una biblioteca a SharePoint. La propietat dels documents en aquests espais és de l'equip i no d'una persona concreta: si algú marxa de l'organització, els documents no desapareixen amb el seu compte personal, cosa que sí que passaria en una carpeta particular compartida des d'un compte individual (si aquella persona esborra el seu compte, la carpeta compartida des del seu Drive personal es perd per a tothom). Aquest és, precisament, l'avantatge principal d'un espai d'equip enfront d'una carpeta personal compartida: la continuïtat documental independent de qui hi treballa en cada moment.

Per crear un Drive compartit a Google Workspace:

1. Des de Google Drive, fes clic a «Unitats compartides» al menú de l'esquerra i després a «Nova».
2. Posa-hi un nom clar (per exemple, «Comunicació Ajuntament 2026») i defineix els membres inicials.
3. Assigna a cada membre el rol corresponent (gestor de contingut, colaborador, comentarista o visualitzador), separat dels rols de fitxers individuals.

Dins d'aquests espais s'hi treballa sovint amb plantilles corporatives, és a dir, documents base amb capçalera, peu de pàgina i tipografia ja definits. La seva finalitat principal és garantir que tots els

documents de l'organització surtin amb la mateixa imatge, sense que cada persona hagi de reinventar el format cada vegada que redacta un informe o una carta.

Quan un document ha de rebre el vistiplau d'algú abans de publicar-se, s'estableix un flux d'aprovació: qui l'ha redactat el proposa, un o diversos revisors poden aprovar-lo o rebutjar-lo amb comentaris, i el document només passa a l'estat «aprovat» quan totes les aprovacions requerides s'han produït, no n'hi ha prou amb una sola signatura si el flux en demana tres. Eines com Google Workspace, Microsoft Approvals o els gestors documentals municipals permeten configurar aquest circuit amb notificacions automàtiques a cada revisor. Aquest flux es pot aplicar fins i tot a nivell d'idea, abans d'escriure res: una proposta breu que es valida abans d'invertir temps a redactar el contingut sencer evita feina perduda si la idea es descarta d'entrada, per exemple si es proposa un nou tríptic informatiu i es valida el concepte abans de maquetar-lo sencer.

Gestió de projectes col·laboratius: taulers Kanban

Eines com Trello, Asana o el Planner de Microsoft organitzen el treball en targetes que representen tasques, agrupades en columnes que reprodueixen l'estat del flux de treball: pendent, en curs, en revisió, fet. Aquest model es coneix com a tauler Kanban i el seu principi és visual: d'un cop d'ull es veu on s'acumula feina i on hi ha un coll d'ampolla, sense haver de llegir cap informe escrit.

Per crear i moure una targeta a Trello:

1. Dins un tauler, fes clic a «Afegeix una targeta» a la columna corresponent (per exemple, «Pendent») i escriu-hi el nom de la tasca.
2. Obre la targeta i assigna-hi una persona responsable, una data límit i, si cal, etiquetes de color per categoritzar-la.
3. Si la tasca és gran, afegeix una llista de verificació amb subtasques dins la mateixa targeta.
4. Quan avanci la feina, arrossega la targeta d'una columna a la següent (per exemple, de «En curs» a «En revisió»).

Cada targeta s'assigna a una persona responsable, porta una data límit i sovint es desglossa en subtasques, i quan es mou d'una columna a una altra tothom que segueix el tauler ho veu reflectit de seguida, sense necessitat de preguntar-ho per correu.

La diferència amb una llista de correus o un document compartit és que el tauler no és una fotografia estàtica sinó un flux viu: registra automàticament qui ha mogut cada targeta i quan, cosa que ni un correu ni un document ordinari fan de manera nativa. Això serveix per detectar un retard abans que es converteixi en un problema real, per exemple si una columna «En revisió» acumula deu targetes i cap avança, és senyal que el coll d'ampolla és en la fase de revisió i no en la de redacció.

Asana i el Planner de Microsoft funcionen amb la mateixa lògica de fons, encara que la interfície canviï de nom: a Asana les tasques es poden veure en format tauler (per columnes), en format llista o en format calendari, i és la mateixa dada la que canvia de representació segons el que et convingui consultar en cada moment; al Planner, les «bústies» (buckets) fan la funció de columnes i cada tasca és una targeta amb responsable, data límit i etiquetes de progrés, integrada de manera nativa amb Teams perquè l'equip la vegi sense sortir del canal de xat. Un error habitual quan un equip comença a fer servir un d'aquests taulers és crear targetes massa grans («Fer la memòria del projecte») que no es mouen mai de la columna «En curs» perquè en realitat amaguen deu tasques diferents a dins; la pràctica correcta és desglossar-les en subtasques concretes i mesurables, perquè el tauler reflecteixi de debò l'avenç real i no doni una falsa sensació d'estancament.

Identitat digital professional i reputació

Marca personal i LinkedIn

La marca personal digital és la impressió coherent que algú projecta professionalment a través del que publica, del que comenta i de com respon en xarxes professionals. LinkedIn n'és l'eina de referència. Un perfil complet inclou:

1. Un extracte (secció «Informació») redactat en primera persona, que expliqui qui ets i què aportes, no una simple llista de tasques.
2. Recomanacions d'altres professionals, que aporten credibilitat externa perquè no les escrius tu mateix.
3. Una activitat regular (comentar publicacions d'altri, compartir-ne, escriure textos curts propis) que manté el perfil viu.

Per editar i completar un perfil de LinkedIn: entra al teu perfil, fes clic al llapis d'edició de cada secció (Informació, Experiència, Formació), i afegeix o actualitza el contingut. A la secció «Destacats» pots enllaçar treballs concrets (un article, una presentació, un projecte) perquè no quedin amagats dins l'experiència laboral.

Un error habitual a nivell avançat és tractar LinkedIn com un currículum passiu, penjat una vegada i oblidat. La plataforma prioritza als seus algorismes els perfils que generen interacció, per tant qui vol que la trobin per a col·laboracions professionals ha de participar activament (comentant, compartint, publicant), no només esperar que algú el trobi.

Portfolis en línia

Un portfoli en línia (una web personal senzilla, un espai a Behance, un repositori a GitHub segons la professió) mostra la feina feta, no només la descriu: és la diferència essencial respecte a un currículum textual convencional, que només explica amb paraules què s'ha fet. Un portfoli es pot enllaçar des de qualsevol altre perfil professional, inclòs el de LinkedIn, per crear un ecosistema coherent d'identitat digital.

Tenir una línia editorial personal, és a dir, decidir amb criteri quins temes es publiquen i amb quin to, és el que dona coherència al llarg termini i evita que un perfil acabi sent un calaix de sastre on es barreja de tot sense cap fil conductor reconeixible.

A la pràctica, muntar un portfoli senzill no exigeix coneixements de programació: serveis com Behance (orientat a disseny i creativitat), un GitHub Pages (orientat a codi i projectes tècnics) o fins i tot una pàgina feta amb un creador de webs sense codi permeten publicar-lo en poca estona. El mínim recomanable és: una presentació breu de qui ets, tres o quatre treballs representatius ben explicats (què es va fer, quin problema resolia, quin va ser el resultat) i una manera clara de contactar-hi. Un error habitual és penjar-hi absolutament tota la feina feta, sense triar: un portfoli amb quaranta treballs mediocres transmet menys criteri professional que un amb sis de ben seleccionats i ben explicats.

Gestió de crítiques públiques

Gestionar una crítica pública és una de les competències més delicades del nivell avançat. Una professional que rep una crítica negativa en un fòrum sobre la seva feina ha d'evitar dues reaccions concretes: esborrar el comentari incòmode o respondre-hi amb ràbia. Totes dues coses solen empitjorar la percepció, perquè en queda constància (algú fa una captura de pantalla abans que s'esborri) i genera l'efecte contrari al desitjat, el que es coneix com efecte Streisand: intentar amagar una cosa la fa més visible que si s'hagués deixat estar.

La pràctica recomanada és reconèixer el problema públicament de manera breu i professional (per exemple, «Gràcies pel comentari, ens posem en contacte per resoldre-ho») i traslladar la conversa detallada a un canal privat per resoldre-la sense esborrar el rastre de la resposta pública inicial. Qui llegeixi després la crítica veurà que hi va haver una resposta professional, no un silenci ni un esborrat sospitós.

Autenticació, signatura i reputació digital avançades

A nivell avançat cal distingir autenticació (provar qui ets, per exemple amb un certificat o una contrasenya més un segon factor) de signatura (provar que has consentit un contingut concret i que no s'ha alterat). eIDAS defineix tres nivells de seguretat d'identificació electrònica: baix, substancial i alt, segons la robustesa de les garanties tècniques i el risc que cobreixen. Una gestió com sol·licitar un certificat de residència pot demanar nivell substancial, mentre que una simple consulta d'informació pública pot no exigir cap identificació.

La reputació digital és el conjunt d'informació, opinions i rastres que una persona deixa a internet i que altres (una empresa, un tribunal d'oposicions, un futur ocupador) poden consultar. Gestionar-la de manera avançada implica tres accions concretes:

1. Auditar periòdicament què apareix en cercar el propi nom en un cercador.
2. Configurar alertes de menció (per exemple amb Google Alertes) perquè avisin quan apareix el teu nom en contingut nou.
3. Conèixer el dret a l'oblit, que no és un dret absolut a esborrar-ho tot d'internet, sinó el dret a sol·licitar que un cercador desindexi enllaços concrets quan la informació és inexacta, desactualitzada o desproporcionada, ponderant-lo sempre amb l'interès públic i la llibertat d'informació.

La petjada digital inclou també metadades que sovint es passen per alt. Un exemple molt concret: les dades EXIF incrustades en una fotografia (la ubicació geogràfica exacta on es va fer) es publiquen sense voler quan algú penja una foto feta amb el mòbil des de casa seva. Per revisar-les o eliminar-les abans de compartir una foto, la majoria de mòbils permeten desactivar l'etiquetatge de localització a la càmera (Configuració > Aplicacions > Càmera > Permisos > Ubicació) o eliminar les dades de la imatge abans de pujar-la amb l'opció «Elimina les dades EXIF» d'alguns editors.

Altres rastres oblidats són l'historial de dispositius vinculats a un compte i els permisos concedits fa anys a aplicacions de tercers que continuen tenint accés al correu o al calendari encara que ja no s'utilitzin. Per revisar-los a un compte de Google: entra a myaccount.google.com > Seguretat > «Les teves connexions amb tercers» (o «Aplicacions de tercers amb accés al compte»), i revoca l'accés de qualsevol aplicació que ja no facis servir. A Microsoft el camí equivalent és account.microsoft.com > Privadesa > Aplicacions i serveis que poden accedir a les teves dades. Revisar-los periòdicament i revocar el que ja no calgui és una de les tasques de manteniment de la identitat digital que més sovint s'obliden, i és exactament el tipus de pregunta d'examen que demana reconèixer un risc «invisible» que ningú comprova d'entrada.

Signatura electrònica, certificats digitals i representació

Els tres nivells de signatura electrònica

El Reglament eIDAS distingeix tres tipus de signatura electrònica i no són intercanviables:

- **Simple**: qualsevol dada electrònica associada a un signant que l'identifica mínimament (un PIN rebut per SMS, un clic acceptant condicions). Té valor probatori feble.
- **Avançada**: està vinculada de manera única al signant, permet identificar-lo, s'ha creat amb mitjans que el signant pot mantenir sota el seu control exclusiu, i qualsevol modificació posterior del document és

detectable. No cal dispositiu físic, però sí garanties tècniques fortes.

- **Qualificada**: és una signatura avançada creada amb un dispositiu qualificat de creació de signatura i basada en un certificat qualificat, emès per un prestador acreditat (per exemple, l'FNMT o idCAT). És l'única equiparada per llei a la signatura manuscrita en tots els estats membres.

A la pràctica, tramitar una sol·licitud a una seu electrònica amb el DNIe o amb idCAT Mòbil és fer servir signatura qualificada o avançada segons el cas; signar un correu amb la imatge escanejada de la rúbrica és, com a molt, signatura simple, i no acredita res per si sola: no incorpora cap mecanisme criptogràfic que vinculi la identitat del signant amb el document ni que detecti alteracions posteriors. Aquest matís, per què una imatge escanejada no val com a signatura plena, és de les preguntes clàssiques d'aquest bloc.

Per signar un document PDF digitalment amb un certificat instal·lat al navegador (per exemple amb Adobe Acrobat Reader):

1. Obre el PDF a Adobe Acrobat Reader i selecciona l'eina «Emplena i signa» o «Certificats».
2. Fes clic a «Signa digitalment» i dibuixa el rectangle on vols que aparegui la signatura visible.
3. Tria el certificat digital instal·lat (per exemple el de l'FNMT) de la llista que mostra el programa.
4. Introdueix el PIN del certificat i confirma; el programa incrusta la signatura criptogràfica i qualsevol canvi posterior al document quedarà detectat.

Cal distingir també la signatura (d'una persona física, que actua en nom propi o en representació) del segell electrònic (d'una persona jurídica, que identifica l'entitat). Un ajuntament pot segellar automàticament milers de notificacions generades per un aplicatiu, sense que cap funcionari les signi una a una: aquest és exactament el mecanisme que s'aplica quan una administració envia notificacions massives generades per un sistema informàtic. I convé no confondre signatura amb segell de temps (timestamp), que acredita de manera fefaent el moment exacte en què es va produir una signatura o un enviament, amb valor probatori propi, independent de qui va signar.

Certificats digitals: FNMT, idCAT i DNIe

Un certificat digital és un document electrònic emès per una autoritat de certificació que vincula una clau pública amb la identitat del titular. Els més habituals a Catalunya i Espanya són el certificat de l'FNMT (Fàbrica Nacional de Moneda i Timbre), l'idCAT (emès pel Consorci d'Administració Oberta de Catalunya) i el DNI electrònic. El certificat es distribueix en dos formats habituals: com a fitxer instal·lat al navegador o al sistema operatiu, o incrustat en una targeta criptogràfica (el DNIe) que necessita un lector de targetes connectat a l'ordinador.

La seva característica tècnica essencial és el parell de claus: la clau privada mai surt del dispositiu del titular i és la que signa; la clau pública es distribueix i és la que qualsevol pot fer servir per verificar la signatura. Aquest funcionament asimètric és el que fa que la signatura sigui fiable: encara que tothom pugui accedir a la clau pública per comprovar-la, ningú excepte el titular té la clau privada necessària per generar-la.

Per obtenir el certificat idCAT (emès pel Consorci AOC), el camí habitual és: entra a la web de l'idCAT, tria «Sol·licitar certificat», omple les dades i valida la identitat presencialment en un punt d'acreditació (o telemàticament amb un altre mètode admès), i descarrega el certificat al navegador un cop acreditat. Per fer servir el DNIe cal, a més del propi DNI electrònic, un lector de targetes connectat per USB i el programari oficial del Ministeri de l'Interior instal·lat.

Apoderaments i representació electrònica: el registre REA

Quan una persona actua no en nom propi sinó representant algú altre (un gestor que tramita per un client,

un càrrec que actua en nom d'una empresa), necessita un certificat de representant, diferent del personal: acredita alhora la identitat de qui signa i la relació de representació amb l'entitat representada. A l'Administració General de l'Estat aquesta relació es formalitza i es pot consultar mitjançant el registre electrònic d'apoderaments Representa (REA), on un ciutadà o una empresa pot apoderar una altra persona per a tràmits concrets o per a totes les gestions davant una administració.

El funcionament és senzill de resumir: el representant no necessita un certificat de la persona representada, actua amb el seu propi certificat, i el sistema comprova l'apoderament vigent al registre en el moment de la tramitació. L'apoderament es pot revocar en qualsevol moment, amb efecte immediat sobre els tràmits encara no iniciats: si un ciutadà havia apoderat una gestoria i revoca aquest apoderament, els expedients que encara no s'havien començat a tramitar queden bloquejats per a la gestoria a partir d'aquell mateix instant, mentre que els ja iniciats poden seguir un règim diferent segons la normativa aplicable.

Per apoderar algú al registre REA, els passos habituals des de la seu electrònica corresponent són: accedir a l'apartat d'apoderaments amb el propi certificat digital o Cl@ve, triar «Inscriure apoderament», indicar la persona o entitat apoderada (amb el seu NIF), seleccionar si l'apoderament és general (per a totes les gestions) o per a tràmits concrets (per exemple, només presentar recursos), i signar electrònicament la inscripció. La gestoria apoderada, a partir d'aquell moment, podrà tramitar en representació del ciutadà sense que aquest hagi de signar cada expedient un a un, cosa que estalvia temps sobretot quan es tracta d'una empresa amb desenes de gestions recurrents davant la mateixa administració.

L'Administració electrònica: seu, registre, notificacions i interoperabilitat

La seu electrònica i el registre electrònic general

La seu electrònica és l'adreça a internet on una administració exerceix la seva activitat administrativa amb plenes garanties jurídiques: publica la seva identitat, l'horari de funcionament del registre, el tauler d'edictes electrònic, i és on el ciutadà presenta instàncies, consulta l'estat dels seus expedients i rep notificacions. No és una web informativa qualsevol: té requisits d'autenticitat, integritat i disponibilitat regulats per llei. Per això és incorrecte pensar que ha d'oferir servei només dins l'horari laboral de l'administració: precisament el que NO se li exigeix és limitar-se a un horari d'oficina, ja que el registre electrònic funciona les 24 hores.

Per presentar una instància a una seu electrònica (per exemple per demanar una subvenció municipal o al·legar en un expedient):

1. Accedeix a la seu electrònica de l'organisme i localitza el tràmit concret al catàleg de tràmits.
2. Identifica't amb certificat digital, DNIe o Cl@ve, segons el que admeti el tràmit.
3. Omple el formulari, adjunta la documentació requerida en els formats admesos i revisa-ho abans d'enviar.
4. Signa electrònicament i envia; el sistema genera automàticament un justificant de recepció amb data, hora i número d'entrada, amb valor de prova de la presentació.

El registre electrònic general permet presentar sol·licituds les 24 hores, tots els dies de l'any. Un matís sobre el còmput dels terminis és clau i es pregunta sovint: el justificant recull la data i l'hora reals de presentació, però si es presenta en un dia inhàbil, es considera presentat el primer dia hàbil següent a efectes de còmput de terminis. Els terminis assenyalats en dies es compten, per defecte, en dies hàbils,

llevat que la norma digui expressament «dies naturals», com és el cas del termini per accedir a una notificació electrònica, que es compta en dies naturals precisament perquè no depengui del calendari laboral de cap administració.

e-NOTUM: comunicacions davant notificacions

e-NOTUM és el servei de notificacions electròniques del Consorci d'Administració Oberta de Catalunya, utilitzat per la Generalitat i molts ajuntaments catalans. La distinció més important d'aquest bloc és entre comunicació i notificació:

- Una **comunicació** és un avís informatiu que no necessita ser «acceptat» i no té efectes jurídics propis: per exemple, un recordatori que una cita ja s'ha confirmat.
- Una **notificació** té efectes jurídics i el termini associat comença a comptar des que el ciutadà hi accedeix, o des que passen deu dies naturals sense accedir-hi, moment en què es considera rebutjada i els efectes es produeixen igualment.

No obrir una notificació, doncs, no els evita, al contrari, els precipita: si algú deixa passar els deu dies naturals sense entrar-hi, la notificació es dona per rebutjada i el termini que comportava (per exemple, per recórrer una sanció) comença a córrer igualment. Aquesta xifra de deu dies és una de les dades que més es pregunta en un examen d'aquest nivell, així que val la pena memoritzar-la literalment: deu dies naturals, no hàbils.

Per accedir a una notificació d'e-NOTUM: entra a l'espai personal de notificacions (des de la seu electrònica corresponent o des de l'enllaç de l'avís rebut per correu o SMS), identifica't amb certificat digital, DNIe, idCAT Mòbil o Cl@ve, i confirma l'accés per «obrir» formalment la notificació, moment en què comença a córrer el termini associat.

Un cas pràctic ajuda a fixar-ho: imagina una persona a qui un ajuntament li notifica una sanció de trànsit per e-NOTUM. Rep un avís per correu dient que té una notificació pendent, però com que està de vacances no hi entra. Passats els deu dies naturals sense accedir-hi, la notificació es considera rebutjada igualment, i el termini per presentar-hi al·legacions comença a córrer des d'aquell moment com si l'hagués llegit, no des que finalment hi entri. Ignorar l'avís no li ha estalviat res, només li ha fet perdre uns dies del termini de resposta. És per això que, a la pràctica, es recomana activar avisos per correu i SMS quan arriba una notificació nova, precisament per no deixar passar aquest termini sense adonar-se'n.

Els ciutadans i empreses obligats a relacionar-se electrònicament amb l'Administració han de disposar d'una adreça electrònica habilitada, sovint gestionada mitjançant DEHú a nivell estatal. Aquesta obligació no és per a tothom: afecta persones jurídiques, entitats sense personalitat jurídica, professionals col·legiats en exercici de la seva activitat professional i representants d'un interessat que estigui alhora obligat a relacionar-se electrònicament. Una persona física particular, en canvi, pot triar si es vol relacionar amb l'Administració en paper o electrònicament, tret d'excepcions puntuals.

Interoperabilitat: no aportar el que ja tenen

El principi que regeix la interoperabilitat entre administracions és que un ciutadà no ha d'aportar un document que una altra administració ja té en el seu poder. Si algú sol·licita una ajuda i cal acreditar l'empadronament o estar al corrent amb la Seguretat Social, l'administració que tramita ho ha de consultar per via telemàtica, mitjançant plataformes com Via Oberta, en comptes de demanar el certificat en paper a la persona interessada. Aquest dret s'exerceix per defecte de manera implícita: si el ciutadà no diu res, l'administració consulta les dades directament. Si un ciutadà vol aportar ell mateix un document en lloc que es consulti telemàticament, cal que s'hi oposi explícitament, marcant-ho al formulari o comunicant-ho,

perquè el comportament per defecte del sistema és el contrari.

Gràcies a aquesta interoperabilitat, sostinguda a Catalunya per Via Oberta i EACAT entre administracions catalanes, un document registrat en un ajuntament es pot fer arribar a un altre ens (un consell comarcal, la Generalitat) sense que el ciutadà l'hagi de tornar a presentar en cap altre lloc, evitant que faci de missatger entre administracions que ja es poden parlar directament.

Factura electrònica i licitació electrònica

La factura electrònica és un document amb validesa legal que substitueix el paper, generat en un format estructurat (habitualment Facturae a l'Estat espanyol) que permet el seu processament automàtic pels sistemes comptables de qui la rep. Aquest és el punt que sol confondre a l'examen: un PDF escanejat d'una factura en paper NO es considera una factura electrònica vàlida en sentit tècnic i legal, precisament perquè no està generat en un format estructurat com Facturae que permeti aquest processament automàtic, encara que visualment sembli idèntica a una factura.

eFACT és la plataforma que utilitzen la Generalitat de Catalunya i molts ens locals catalans per rebre aquestes factures electròniques dels seus proveïdors, integrada amb la plataforma estatal FACe. Un proveïdor que factura a un ajuntament català típicament genera el fitxer Facturae amb el seu programa de facturació i el puja a través d'eFACT (o directament a FACe si l'ens no té eFACT integrat), en lloc d'enviar un PDF per correu.

Val la pena distingir-ho de l'experiència quotidiana d'un particular: quan a casa reps la factura de la llum en PDF adjunt a un correu de la companyia elèctrica, això no és tècnicament una factura electrònica en el sentit de Facturae, és un document pensat perquè el llegeixi una persona, no perquè el processi automàticament un sistema comptable. El format Facturae estructurat es fa servir sobretot en relacions entre empreses (B2B) i en la facturació a l'Administració, on qui rep la factura necessita que les dades (import, IVA, conceptes) es puguin llegir i comptabilitzar automàticament sense que ningú les hagi de teclejar a mà.

Quan una empresa vol optar a un contracte públic, la licitació es tramita a través d'una plataforma de contractació, com la Plataforma de Serveis de Contractació Pública de Catalunya. Allà es publiquen els plecs, es presenten les ofertes xifrades electrònicament fins a la data límit, i no es poden obrir ni consultar per part de l'òrgan de contractació fins que el termini de presentació ha finalitzat del tot. Aquesta garantia és exactament el que aporta el xifratge de les ofertes: que cap licitador conegui les ofertes de la resta abans que el termini hagi finalitzat, mantenint la competència en igualtat de condicions.

Participació ciutadana i comunitats de coneixement obert

Participació ciutadana digital

Més enllà de tramitar, les seus electròniques i portals de transparència incorporen mòduls de participació: consultes públiques prèvies a l'elaboració de normativa, pressupostos participatius on la ciutadania vota partides concretes, i bústies de queixes i suggeriments amb seguiment de l'expedient.

Cal distingir bé el paper de cadascuna d'aquestes eines. La consulta prèvia recull opinions per orientar com s'ha de redactar una norma, és a dir, la seva opinió serveix d'input però no vincula directament el resultat final; la votació vinculant, en canvi, determina directament on s'inverteix un pressupost concret, i per això té conseqüències pràctiques diferents i requeriments d'identificació també diferents.

La identificació per participar-hi acostuma a exigir un nivell de seguretat inferior al de tramitar (a vegades

n'hi ha prou amb un registre amb correu i contrasenya), però quan hi ha votació vinculant sol requerir-se autenticació amb certificat digital o Cl@ve, precisament per evitar vots duplicats i garantir que cada persona identificada vota una sola vegada. Aquest matís, per què cal més seguretat en la votació que en una simple consulta d'opinió, és un dels raonaments que més es demana entendre, no només memoritzar.

El mateix principi es veu clarament en un exemple allunyat de la participació però molt il·lustratiu: per demanar hora al CAP a través del portal del teu centre de salut, sol n'hi ha prou amb identificar-te amb el codi CIP i la data de naixement, un nivell de seguretat baix perquè el risc si algú s'equivoca és mínim (com a molt, reserves una hora que no et pertoca). En canvi, per consultar el teu historial clínic complet a La Meva Salut cal identificar-te amb un mètode de nivell alt (certificat digital, DNIe o Cl@ve Permanent), perquè les dades a què s'accedeix són molt més sensibles i el risc d'un accés indegut és molt més gran. El nivell d'exigència d'identificació, en definitiva, és proporcional al risc de l'operació, no un capritx del disseny del sistema.

Fòrums, wikis i llicències obertes

Els fòrums tècnics (Stack Overflow n'és l'exemple més conegut, però cada comunitat professional en té un d'específic) funcionen amb un sistema de reputació basat en vots: les respostes ben valorades pugen de posició, i amb prou reputació acumulada un usuari pot moderar continguts d'altri (editar preguntes mal formulades, tancar duplicats o assenyalar respostes incorrectes) sense necessitat de ser un administrador contractat per la plataforma. Aquesta moderació distribuïda és el que permet que comunitats amb milions d'usuaris funcionin sense un equip central que ho revisi tot.

Les wikis (Wikipedia com a exemple més gran, però també les wikis internes d'una organització) permeten que qualsevol persona autoritzada editi un contingut compartit, i mantenen un historial complet de versions que permet identificar qui ha canviat què i revertir un error o un vandalisme amb un sol clic, igual que passava amb l'historial de versions dels documents al núvol que hem vist abans, però aquí aplicat a un contingut públic i col·lectiu.

Compartir coneixement de manera oberta implica triar una llicència que digui explícitament què es pot fer amb el contingut. Les llicències Creative Commons són l'estàndard més utilitzat, des de la més permissiva (CC BY, que només exigeix citar l'autor) fins a variants que prohibeixen l'ús comercial o exigeixen compartir les obres derivades amb la mateixa llicència. Contribuir amb bones pràctiques (documentar una solució trobada, respondre dubtes d'altri, actualitzar informació obsoleta) és el que sosté aquests espais, que depenen íntegrament de la col·laboració voluntària de qui hi participa.

Bretxa digital i accessibilitat de les comunicacions

La bretxa digital no és només qui té o no té accés a internet; té almenys tres capes: la d'accés (disposar de connexió i dispositiu), la de competències (saber-los fer servir amb solvència) i la d'ús (aprofitar-los per obtenir un avantatge real, no només fer-ne un consum passiu). Una persona pot tenir un mòbil amb dades mòbils i quedar-se igualment fora d'un tràmit digital si no en sap prou fer-lo servir, encara que tingui l'accés tècnic perfectament resolt: aquest cas concret, algú amb connexió però sense saber completar el tràmit, correspon precisament a la capa de competències, no a la d'accés.

Redactar comunicacions accessibles és una responsabilitat de qui gestiona la comunicació d'equip o institucional. Alguns criteris pràctics:

1. Fer servir frases curtes i clares, evitant la jerga innecessària que només entenen els tècnics del ram.
2. Oferir un text alternatiu a qualsevol imatge (el camp «text alternatiu» o «alt text» en editar la imatge en

un document o web) perquè un lector de pantalla el pugui llegir a persones amb discapacitat visual.

3. Afegir subtítols als vídeos, tant per a persones amb discapacitat auditiva com per a qui els mira sense so.

4. Mantenir un contrast de color suficient entre text i fons perquè una persona amb baixa visió pugui llegir-lo sense esforç.

Acompanyar persones amb menys competències digitals no és només fer-los el tràmit en el seu lloc: és mostrar-los el procés pas a pas, amb paciència i sense donar per fet cap coneixement previ, perquè la propera vegada puguin fer-ho soles. Aquest acompanyament és, en definitiva, la manera pràctica d'atacar la bretxa digital en la seva capa de competències, que és sovint la que més costa de resoldre perquè no n'hi ha prou amb repartir dispositius o connexió.

TEMA 3

Àrea 3. Creació de continguts digitals

Text avançat: estils que mantenen el document sol

A nivell bàsic n'hi ha prou amb saber posar negreta i triar una mida de lletra. A l'avançat, l'ACTIC espera que dominis el que fa que un document sigui mantenible de veritat: els **estils**. Imagina un informe de subvencions per a l'ajuntament, de 40 pàgines, amb vint títols d'apartat. Si els has posat en negreta manual i mida 16, i el tècnic municipal et demana canviar-ho tot a mida 14 perquè "queda massa gros", has de repassar el document sencer, títol per títol, sense oblidar-te'n cap. Si en canvi has aplicat l'estil "Titol 1" a tots ells, només cal modificar la definició de l'estil una vegada i el canvi es propaga automàticament a tots els títols que el fan servir, sense tocar-los un per un.

Com es crea i es modifica un estil (Writer)

1. Escriu i selecciona el paràgraf que vols convertir en estil (per exemple, un títol amb la mida i el color que t'agraden).
2. Obre l'Estilista amb la tecla F11 (o Estils - Gestiona estils).
3. Amb el paràgraf encara seleccionat, fes clic dret sobre l'estil "Titol 1" a la llista i tria "Actualitza l'estil des de la selecció": totes les característiques del paràgraf (mida, color, espaiat) queden gravades a l'estil.
4. A partir d'ara, aplicar "Titol 1" a qualsevol altre paràgraf del document li donarà exactament aquest aspecte, i si tornes a modificar l'estil, tots els títols que el fan servir canvien alhora.

A Word el mateix procés es fa des de la pestanya Inici, panell Estils: clic dret sobre l'estil - Modifica, o "Actualitza Títol 1 perquè coincideixi amb la selecció".

Els estils no són només comoditat visual: són la base de tot el que ve després en un document llarg (índex automàtic, referències creuades, documents mestres). Un truc que es pregunta sovint a l'examen: un índex de continguts generat automàticament NOMÉS recull paràgrafs que tenen aplicat un estil de títol (Titol 1, Titol 2...); si has escrit un títol amb negreta manual sense estil, l'índex se'l saltarà encara que visualment sembli un títol.

Estils de caràcter, de pàgina i de llista

A banda dels estils de paràgraf hi ha altres famílies que convé distingir per l'examen:

- Un **estil de caràcter** s'aplica a una part d'una frase (per exemple, ressaltar sempre igual els termes tècnics d'un manual) sense afectar la resta del paràgraf.
- Un **estil de pàgina** controla marges, orientació, capçalera i peu, i és el que permet, per exemple, que uns annexos s'imprimeixin en horitzontal mentre la resta del document és en vertical.
- Un **estil de llista** defineix com es numeren o s'ordenen amb pics els elements d'una llista de manera consistent a tot el document.

Plantilles: el format d'organització es defineix una sola vegada

Les **plantilles** (fitxers .ott a LibreOffice, .dotx a Word) guarden estils, capçaleres, peus de pàgina, marques d'aigua i fins i tot macros, de manera que tota una organització (una acadèmia, una associació de veïns, un ajuntament) pot compartir el mateix format corporatiu sense refer-lo cada cop. Per crear-ne una a Writer: dissenyes un document amb tots els estils, capçalera i peu ja definits, i el desis amb Fitxer - Desa

com a plantilla; a partir d'aquí, Fitxer - Nou - Plantilles t'ofereix aquest disseny com a punt de partida per a qualsevol document nou. Una plantilla ben dissenyada estalvia hores i garanteix que l'informe que fa una persona del departament de comunicació tingui exactament el mateix aspecte que el que fa algú d'administració, encara que no hagin parlat entre elles del format.

Estructura professional de documents llargs

Seccions i salts d'estil de pàgina

Un document llarg sovint necessita trams amb formats diferents: una portada sense numeració, un cos a una columna, uns annexos amb orientació horitzontal i numeració pròpia. Això s'aconsegueix amb salts de secció, no pas amb salts de línia repetits fins que la pàgina "sembli" nova, que és l'error típic de qui no en sap prou. A Writer: Insereix - Més salts - Salt de secció, o bé, més robust, canviar l'estil de pàgina just en el punt on vols que canviï el format (Format - Estils de pàgina, o inserir un salt de pàgina "amb canvi d'estil" des d'Insereix - Salt de pàgina, triant l'estil nou al desplegable "Estil"). A Word l'equivalent és Disposició - Salts - Salts de secció - Pàgina següent.

Pas a pas per aconseguir que la portada no tingui número de pàgina i el cos sí, des de la pàgina 2 marcada com a "1":

1. Situa el cursor al final de la portada.
2. Insereix un salt de pàgina amb canvi d'estil (per exemple, de l'estil "Primera pàgina" a "Per defecte").
3. Al peu de pàgina del cos, insereix el camp de número de pàgina (Insereix - Camp - Número de pàgina).
4. Ves a Format - Estils de pàgina de la pàgina 2 i marca "Reinicia la numeració" a l'1, perquè el compte torni a començar just allà on acaba la portada.

Numeració complexa: xifres romanes, capítols i figures

La numeració de pàgines segueix la mateixa lògica de canvi d'estil: la portada i l'índex es poden numerar amb xifres romanes (i, ii, iii) i que el cos reprengui la numeració aràbiga des de l'1, sempre que hi hagi un canvi d'estil de pàgina pel mig, amb l'opció "Reinicia la numeració" activada al punt de canvi. També és habitual numerar els capítols amb prefix, de manera que les figures de l'apartat 3 es diguin "Figura 3.1", "Figura 3.2": per aconseguir-ho, la numeració de la figura s'ha de vincular al nivell d'esquema del capítol (a Writer, dins la definició de la numeració de llegendes, opció "Nivell", triant el nivell d'esquema corresponent al títol de capítol), de manera que el prefix numèric coincideix sempre amb l'apartat vigent, encara que afegeixis o eliminis capítols abans.

Índexs: taula de continguts, índex alfabètic i bibliografia

Els índexs van més enllà de la taula de continguts. Writer la genera a Insereix - Índex i taules - Índex i taules, llegint quins paràgrafs tenen aplicats els estils de títol (Titol 1, Titol 2...), no pas mirant la mida de lletra a ull. També pots crear un índex alfabètic, a partir d'entrades marcades manualment al llarg del text (seleccionant una paraula i fent Insereix - Índex i taules - Entrada), o una bibliografia a partir d'una base de dades de referències (Eines - Bibliografia), de manera que si canvies l'ordre de les cites al text, la llista final es reordena sola en actualitzar els camps (clic dret sobre l'índex - Actualitza índex).

Referències creuades

Lligat a l'estructura hi ha les referències creuades (Insereix - Referència): en lloc d'escriure "vegeu la figura 3 a la pàgina 12" a mà, insereixes una referència al número de figura i una altra al número de pàgina, i si

més endavant afegeixes una figura abans i tot es desplaça, el text s'actualitza sol en recalcular els camps (F9, o clic dret - Actualitza camps). Escriure aquests números a mà és l'error típic que l'examen penalitza, perquè es desincronitzen a la primera revisió del document: n'hi ha prou que s'afegeixi un paràgraf abans perquè "la figura 3" passi a ser en realitat la 4, i el text escrit a mà no ho sàpiga mai.

Documents mestres

Per a projectes molt grans (un llibre de dotze capítols, cadascun en un fitxer independent, escrits potser per autors diferents), Writer ofereix el document mestre (Fitxer - Nou - Document mestre): un fitxer especial que no conté text propi sinó enllaços als subdocuments (Insereix - Fitxer), de manera que es pot generar un índex general, una numeració contínua i una bibliografia unificada sense fusionar manualment tots els fitxers en un de sol. La idea clau per a l'examen és que el document mestre coordina, no substitueix, els subdocuments originals: si algú edita un capítol des del seu propi fitxer, el canvi es reflecteix en obrir o actualitzar el document mestre, sense que calgui tocar-lo des d'allà.

Formularis, combinació de correspondència i accessibilitat del document

Combinació de correspondència pas a pas

La combinació de correspondència enllaça un document model amb una font de dades (un full de càlcul o una base de dades amb noms i adreces) per generar cartes, etiquetes o correus personalitzats en massa: per exemple, la convocatòria d'una reunió de comunitat de veïns amb el nom de cada propietari. A Writer:

1. Prepara el full de càlcul amb una columna per camp (Nom, Adreça, Import...).
2. Obre el document model i ves a Eines - Assistent per combinar correspondència.
3. Selecciona el tipus de document (carta, missatge de correu, etiquetes) i tria la font de dades (el full de càlcul).
4. Insereix els camps de combinació al text amb Insereix - Camp - Més camps, o l'opció "Insereix camp de combinació" de la barra corresponent: apareixen com <<Nom>>, <<Adreça>>.
5. Previsualitza els registres (icona d'ullet) per comprovar que cada carta mostra les dades correctes.
6. Finalitza combinant en un document nou, imprimint directament, o enviant per correu electrònic si has triat missatge de correu.

Cal distingir bé els camps de combinació (com <<Nom>>), que se substitueixen pel valor de cada registre en generar els documents finals, dels camps de text normal que es repeteixen igual a totes les còpies: la salutació "Benvolgut/da," és igual per a tothom, mentre que <<Nom>> canvia registre a registre.

Formularis per emplenar a mà

Quan el document que has de repartir no és per emplenar amb dades massives sinó perquè algú el completi a mà (una sol·licitud de subvenció, una enquesta de satisfacció), el que interessa és un formulari amb camps de text, caselles de verificació o llistes desplegables. A Writer, la barra Controls de formulari (Visualitza - Barres d'eines - Controls de formulari) permet inserir aquests elements. Un cop dissenyat, cal protegir-lo (Eines - Protegeix el document - Formularis, o Format - Secció marcant "Protegit") perquè qui l'ompli només pugui escriure dins els camps habilitats i no pugui esborrar per error una pregunta o trencar el format de la resta del document.

Accessibilitat del document

L'accessibilitat d'un document ja no és un afegit opcional a nivell avançat: cal que qualsevol persona, faci servir o no un lector de pantalla, pugui accedir-hi. Això exigeix:

- Títols estructurats de veritat (estil "Titol 1", "Titol 2"...), no negreta feta a mà, que el lector de pantalla no reconeix com a títol i per tant no permet navegar-hi.
- Text alternatiu a cada imatge (clic dret sobre la imatge - Descripció, camp "Text alternatiu"): una descripció breu que el lector de pantalla llegeix en lloc de la imatge.
- Un ordre de lectura lògic quan hi ha elements superposats, quadres de text o columnes, perquè el lector de pantalla no salti d'una banda a l'altra sense sentit.
- Un contrast de color suficient entre text i fons.

En exportar a PDF (Fitxer - Exporta a PDF, pestanya General, marcant "Etiquetat PDF (accessibilitat)"), un PDF accessible ha de conservar aquestes etiquetes d'estructura. Un PDF fet a partir d'una imatge escanejada, en canvi, no és accessible perquè no té cap text real a sota: un lector de pantalla només hi veu una fotografia, per molt clar que es llegeixi a ull humà. Aquesta diferència, entre etiquetes d'estructura reals i imatge escanejada, és un dels punts que més es pregunta a l'examen avançat.

Edició d'imatge digital: capes, formats i resolució

Capes: l'edició no destructiva

Quan retoques una fotografia (per exemple, per afegir el logotip de l'acadèmia a una imatge promocional, o per retocar la foto d'un carnet), el pitjor que pots fer és dibuixar directament sobre la imatge original: si t'equivoques, ja no hi ha marxa enrere. Els editors d'imatge com GIMP (programari lliure) resolen això amb les capes: cada element (el fons, el text afegit, un requadre, una marca d'aigua) viu en la seva pròpia capa, apilades una sobre l'altra com làmines de vidre transparent. Pots editar, moure o esborrar el text d'una capa superior sense tocar ni un píxel del fons, que queda intacte a la capa de sota.

Pas a pas per afegir un text sobre una foto a GIMP sense fer-ho de manera destructiva:

1. Obre la fotografia (Fitxer - Obre).
2. Finestres - Finestres ancorables - Capes per veure el panell de capes.
3. Tria l'eina Text (icona "A") i escriu el text directament sobre la imatge: GIMP crea automàticament una capa nova només per a aquest text.
4. Pots moure, canviar de mida o de color aquesta capa de text sense afectar la fotografia de sota, i fins i tot esborrar-la del tot si canvies d'opinió.
5. Quan el resultat és definitiu, Imatge - Aplana la imatge fusiona totes les capes en una de sola (necessari abans d'exportar a JPEG, que no admet capes).

Aquest és el concepte que l'examen sol preguntar en forma de "quina funcionalitat permet editar text afegit a una fotografia sense alterar el fons original": la resposta és sempre les capes.

Formats d'imatge: quan triar JPEG, quan PNG

No tots els formats d'imatge serveixen per al mateix, i triar-ne un o altre té conseqüències pràctiques:

- **JPEG** (.jpg) comprimeix amb pèrdua: redueix molt el pes del fitxer descartant informació que l'ull gairebé no nota, la qual cosa el fa ideal per a fotografies que vulguis compartir o penjar a una web amb un pes de fitxer reduït, assumint una certa pèrdua de qualitat. No admet transparència.
- **PNG** admet transparència (el fons pot quedar "buit" en lloc de blanc) i comprimeix sense pèrdua, per això és el format que convé per a un logotip amb text nítid: les vores del text es mantenen perfectament definides, sense l'efecte de "boira" que la compressió JPEG produeix en vores nítides de color sòlid, i el fons transparent permet col·locar el logotip sobre qualsevol color de fons.
- **GIF** es fa servir sobretot per a animacions senzilles i imatges amb pocs colors.

- Formats com **.xcf** (natiu de GIMP) o **.psd** (natiu de Photoshop) conserven les capes intactes per poder seguir editant més endavant; s'han d'exportar a JPEG o PNG només quan la imatge ja és definitiva.

Un truc d'examen: si et pregunten per una fotografia per compartir amb pes reduït assumint una certa pèrdua, la resposta és JPEG; si et pregunten per un logotip amb text nítid i fons transparent, la resposta és PNG. Confondre els dos és l'error més freqüent en aquesta part del temari.

Resolució: ppp, pantalla i impressió

La resolució d'una imatge s'expressa en ppp (punts per polzada, o dpi en anglès) i indica quants punts de color hi ha en cada polzada de la imatge un cop impresa. Per a un contingut que només es veurà en pantalla (una foto de xarxes socials, una imatge dins d'una presentació que es projectarà des d'un ordinador), 72 ppp sol ser suficient, perquè les pantalles no necessiten més densitat de punts per mostrar-se nítides: pujar la resolució només fa el fitxer més pesant sense cap millora visible. En canvi, per imprimir una imatge en paper amb bona qualitat (un tríptic, un cartell), cal una resolució molt més alta, típicament 300 ppp, perquè a una densitat menor l'ull hi distingeix els punts individuals si t'hi acostes.

Cal no confondre la resolució (ppp) amb la mida en píxels (per exemple, 1920x1080): una mateixa imatge de 1920x1080 píxels pot mostrar-se amb qualitat suficient en una pantalla d'ordinador però quedar pixelada si s'imprimeix a mida gran, perquè els mateixos píxels s'han d'estirar sobre més superfície de paper.

Fulls de càlcul: referències, funcions i validació

Referències relatives, absolutes i mixtes

Aquí és on més es nota el salt de nivell respecte al certificat mitjà. Cal dominar la diferència entre referència relativa (A1), absoluta ($A$1) i mixta ($A1 o A$1). Si arrossegues la fórmula =A1B1 cap avall des de C1 fins a C20, A1 i B1 avancen fila a fila (A2B2, A3*B3...) perquè són referències relatives: el full de càlcul les interpreta com "la cel·la que hi ha dues posicions a l'esquerra", no com una adreça fixa. Però si vols multiplicar sempre pel mateix tipus d'IVA, situat a la cel·la B1, has de fixar-la com a $B$1: el símbol del dòlar davant de la lletra bloqueja la columna, i davant del número bloqueja la fila, de manera que en copiar la fórmula cap avall, la referència a B1 no es mou mai.

Exemple pràctic: una factura de la llum amb vint conceptes en columna A i preus unitaris en columna B, i vols aplicar el mateix percentatge d'IVA guardat a la cel·la E1 a totes les línies. La fórmula a C1 seria =B1*(1+$E$1), i en copiar-la cap avall fins C20, cada fila multiplica el seu propi preu (B2, B3...) pel mateix IVA fix (sempre E1). Un error clàssic d'examen: preguntar què passa si NO poses el dòlar. La resposta és que la referència a E1 es desplaçarà fila a fila (E2, E3, que probablement estan buides), i el resultat sortirà malament.

Funcions condicionals

Les funcions condicionals com SI (=SI(B2>=5;"Aprovat";"Suspès")) es combinen amb SUMAR.SI, COMPTAR.SI o la més potent SUMAR.SI.CONJUNT quan hi ha diversos criteris alhora: per exemple, =SUMAR.SI.CONJUNT(C:C;A:A;"Vendes";B:B;"Gener") suma només els imports de la columna C on la columna A digui "Vendes" i la columna B digui "Gener", una utilitat que un SUMAR.SI simple, que només admet un criteri, no pot oferir.

Quan una sola condició no basta, es fan servir funcions SI imbricades: =SI(B2>=9;"Excel·lent";SI(B2>=5;"Aprovat";"Suspès")) avalua primer la condició més exigent (nota igual o

superior a 9) i, si no es compleix, passa a la segona SI de dins, com una cadena de preguntes successives que només continua si l'anterior ha donat "fals". Un error habitual és desordenar les condicions posant primer la menys restrictiva: si escrius =SI(B2>=5;"Aprovat";SI(B2>=9;"Excel·lent";"Suspès")), qualsevol nota de 9 o més ja compleix "B2>=5" a la primera comprovació i es queda amb "Aprovat" per sempre, perquè mai s'arriba a comprovar la segona condició. Aquest és exactament el tipus d'error que l'examen posa a prova.

BUSCARV, BUSCARH i XLOOKUP

La funció estrella de nivell avançat és BUSCARV (VLOOKUP en anglès, o CONSULTAV): =BUSCARV(valor_cercat; matriu; núm_columna; ordenat). Imagina un full "Vendes" amb el codi de producte a la columna A, i un full "Productes" amb el codi a la columna A, el nom a la B i el preu a la C. Per recuperar automàticament el preu a "Vendes", escrius a la cel·la corresponent =BUSCARV(A2;Productes.A:C;3;FALS): busca el valor de A2 dins la primera columna de la matriu "Productes.A:C" i, quan el troba, retorna el valor de la columna 3 comptant des de la primera de la matriu (és a dir, el preu). El quart argument, FALS, és clau: obliga a una coincidència exacta del valor cercat; oblidar-lo (o posar VERTADER) és una de les errades més habituals i dona resultats incoherents quan les dades no estan ordenades, perquè la funció es conforma amb una coincidència aproximada.

La utilitat pràctica de BUSCARV és evitar teclejar a mà dades que ja existeixen en una altra taula: la fórmula va a buscar-les sola i, si el preu original canvia al full "Productes", es propaga automàticament arreu on s'ha fet servir la fórmula, sense haver de tocar res més. També cal conèixer BUSCARH (cerca horitzontal, quan les dades estan organitzades per files en lloc de columnes) i, en versions més modernes de full de càlcul, XLOOKUP o CONSULTAX, més flexible perquè no depèn de l'ordre de les columnes ni obliga que el valor cercat estigui a la primera.

Validació de dades

La validació de dades (Dades - Validesa a LibreOffice Calc, Dades - Validació de dades a Excel) evita errors d'entrada abans que es produeixin: pots obligar que una cel·la només accepti un nombre dins un rang (per exemple, una edat entre 0 i 120), una data vàlida, o restringir-la a una llista desplegable de valors permesos. Un exemple habitual: que un camp "Departament" només accepti "Vendes", "Producció" o "Administració" triats d'una llista, i no qualsevol text lliure escrit diferent cada vegada ("vendes", "Vendes ", "Comercial"...), que després faria fallar qualsevol recompte o filtre. Per crear-la:

1. Selecciona la cel·la o el rang de cel·les.
2. Dades - Validesa.
3. Tria el criteri: "Llista" per a un desplegable, "Nombre enter" amb un rang, "Data" amb límits.
4. A la pestanya "Missatge d'error" pots definir un avís que aparegui si algú intenta escriure un valor no permès.

És l'eina que garanteix que les dades d'entrada siguin consistents des del principi, cosa que després fa que BUSCARV i les taules dinàmiques funcionin sense sorpreses ni valors "orfes" que no coincideixen amb res.

Taules dinàmiques, format condicional, gràfics i protecció del full

Taules dinàmiques

Les taules dinàmiques (Dades - Taula dinàmica a Calc, Insereix - Taula dinàmica a Excel) permeten resumir milers de files, per exemple vendes per comercial i per mes, arrossegant camps a les àrees de

files, columnes i valors, sense escriure cap fórmula. Pas a pas:

1. Selecciona el rang de dades en brut (amb capçaleres de columna).
2. Dades - Taula dinàmica - Crea/Insereix.
3. Arrossega el camp "Comercial" a l'àrea de files, "Mes" a l'àrea de columnes, i "Import" a l'àrea de valors.
4. El programa agrupa i suma automàticament: cada cel·la de la taula resultant mostra el total de vendes d'un comercial en un mes concret.

Quan les dades en brut són tan voluminoses que cap ull humà les pot interpretar directament mirant-les fila per fila, la taula dinàmica les reagrupa i les resumeix (suma, mitjana, recompte, màxim) en segons, i permet canviar la perspectiva (per exemple, passar de "vendes per comercial" a "vendes per producte") simplement arrossegant els camps a àrees diferents. És l'eina d'anàlisi més potent d'un full de càlcul per a algú que no programa.

Format condicional

El format condicional (Format - Format condicional) canvia l'aparença d'una cel·la segons el seu contingut sense fer-ho a mà cel·la per cel·la: pot pintar de vermell tot allò per sota d'un llindar (per exemple, marcar en vermell les factures pendents de cobrament de més de 60 dies), aplicar una escala de color que passi de vermell a verd segons el valor (útil per veure d'un cop d'ull quins mesos han anat millor), o mostrar icones (fletxes, semàfors) que resumeixen visualment una columna sencera de xifres. També es pot basar en una fórmula pròpia quan la condició és més complexa que un simple llindar numèric, per exemple si depèn del valor d'una altra cel·la de la mateixa fila.

Gràfics: quin tipus per a quina dada

Els gràfics s'han de triar segons el tipus de dada, i aquest criteri és un dels que més es pregunta a l'examen:

- **Circular**: per a percentatges d'un total (per exemple, el repartiment del pressupost municipal per àrees).
- **De barres**: per comparar categories entre elles (vendes de cada botiga d'una cadena).
- **De línies**: per a l'evolució temporal (vendes mensuals al llarg d'un any).
- **De dispersió (XY)**: per veure la relació entre dues variables numèriques (per exemple, hores d'estudi i nota obtinguda), quan vols saber si una cosa influeix en l'altra.

Un error de disseny freqüent, i que l'examen sol assenyalar, és fer servir un gràfic circular amb dades que no sumen el 100%: el gràfic circular representa proporcions d'un tot, i si les parts no sumen el total (per exemple, perquè una mateixa persona pot triar més d'una opció en una enquesta), la lectura visual indueix a error, perquè l'ull interpreta automàticament que els trossos completen un cercle sencer.

Protecció del full i del llibre

Quan un full de càlcul es comparteix amb altres persones i conté fórmules delicades (com la taula "Productes" que alimenta un BUSCARV), convé protegir el full o les cel·les (Eines - Protegir full a Calc, Revisar - Protegir full a Excel): es poden bloquejar només les cel·les amb fórmules perquè ningú les esborri per error sense voler, i deixar lliures les cel·les d'entrada de dades perquè l'usuari les pugui omplir amb normalitat. Per fer-ho de manera selectiva: primer selecciones les cel·les que vols que quedin editables i, a Format - Cel·les - Protecció, desmarques "Protegit"; totes les altres queden protegides per defecte quan actives Eines - Protegir full. Protegir tot el llibre amb contrasenya (Eines - Protegir llibre), en canvi, n'impedeix qualsevol modificació estructural, com afegir o eliminar fulls sencers.

Errors habituals del full de càlcul i importació de dades

Importar un fitxer CSV

En importar un fitxer CSV a un full de càlcul cal fixar-se en dos paràmetres que sovint es passen per alt:

- El **caràcter delimitador**: coma o punt i coma, segons la configuració regional d'origen del fitxer (un CSV generat en un país que fa servir la coma com a separador decimal sol utilitzar el punt i coma per separar camps, per no confondre'ls).
- La **codificació de caràcters**: UTF-8 evita que els accents i la ñ surtin corromputs (símbols estranys en lloc de "informació" o "any"), un problema típic quan un fitxer s'ha generat amb una codificació antiga i s'obre assumint UTF-8, o a l'inrevés.

També cal indicar, durant l'assistent d'importació, quines columnes s'han d'importar com a text i no com a número: si un codi postal comença per zero (per exemple, 08001, de Barcelona), interpretar-lo com a número li esborrarà el zero inicial sense avisar, i quedarà com "8001", un codi postal que no existeix. El mateix passa amb números de telèfon que comencen per zero en alguns països, o amb codis d'articles que tenen zeros a l'esquerra amb significat.

Els errors que mostra el propi full de càlcul

Els errors que mostra el propi full de càlcul també formen part del temari avançat:

- **#N/A**: apareix quan una funció de cerca (com BUSCARV) no troba el valor cercat dins la matriu. Sol indicar que el codi que busques no existeix a l'altra taula, o que hi ha un espai en blanc o una diferència de format que impedeix la coincidència exacta.
- **#REF!**: surt quan una fórmula fa referència a una cel·la que s'ha esborrat (per exemple, has eliminat una fila o columna que una altra fórmula feia servir).
- **Referència circular**: es produeix quan una fórmula es refereix, directament o indirectament, a la seva pròpia cel·la, com escriure a A1 la fórmula =A1+B1. El programa la detecta i avisa perquè no té solució matemàtica única: per calcular A1 caldria ja conèixer A1, i és un bucle sense sortida. Un cas indirecte i més subtil és quan A1 depèn de B1, i B1 al seu torn depèn (a través d'altres cel·les) d'A1: el resultat és el mateix avís, encara que la circularitat no es vegi a simple vista en una sola fórmula.

Presentacions i comunicació visual

El patró de diapositives

A nivell avançat, el patró de diapositives (Visualitza - Patró de diapositives a Impress, o Visualització - Patró de diapositives a PowerPoint) és imprescindible: hi defineixes el logotip, els colors corporatius i la tipografia una sola vegada, i es repliquen a totes les diapositives que en depenen, de manera similar als estils de Writer. Pas a pas:

1. Visualitza - Patró de diapositives.
2. Insereix el logotip a la posició on vulguis que aparegui a totes les diapositives (per exemple, cantonada inferior dreta).
3. Defineix els colors i la tipografia dels títols i del text de cos des d'aquesta vista mestra.
4. Torna a la vista normal (Visualitza - Normal): totes les diapositives noves ja incorporen aquest disseny, i si canvies el logotip al patró, canvia a totes alhora.

Storytelling visual i jerarquia tipogràfica

Una bona presentació es construeix amb storytelling visual: cada diapositiva ha de transmetre una idea, no un bloc de text llegit en veu alta, de manera que la seqüència explica una història amb principi, desenvolupament i conclusió en lloc d'amuntegar dades soltes. Això es recolza en la jerarquia tipogràfica: un títol clarament més gran que el text de suport, un màxim de dues o tres mides per diapositiva, perquè l'ull sàpiga immediatament què llegir primer i en quin ordre.

El contrast entre text i fons (lletra fosca sobre fons clar, o a l'inrevés, mai gris clar sobre blanc, ni groc sobre blanc) és el que fa que una diapositiva es pugui llegir des del fons d'una sala, i és un dels criteris de llegibilitat que l'examen sol posar a prova amb exemples concrets de combinacions de color dolentes: si et donen a triar entre "text gris clar sobre fons blanc" i "text fosc sobre fons clar", la combinació assenyalada com a error és sempre la primera, perquè el contrast és insuficient per llegir-se còmodament, especialment des de lluny o en una sala amb llum ambiental.

Infografies

Les infografies resumeixen dades complexes en un format visual (icones, xifres destacades, un recorregut de lectura clar) pensat perquè es comprenguin d'un cop d'ull. Funcionen bé quan les dades són poques i clares (tres xifres clau sobre la participació d'una consulta ciutadana), i malament quan s'hi amunteguen massa xifres alhora, perquè llavors deixen de ser un resum visual i es converteixen en un altre bloc de text disfressat d'imatge.

Exportar una presentació segons l'ús

A l'hora d'exportar una presentació, el format tria l'ús:

- **PPTX o ODP**: per editar-la després en un altre ordinador.
- **PDF**: per llegir-la i imprimir-la sense sorpreses de compatibilitat, amb el format fixat.
- **Imatge** (una per diapositiva): per publicar-la a xarxes socials.
- **Vídeo**: quan la presentació s'ha d'executar sola, amb transicions i narració d'àudio incloses, sense que ningú l'hagi d'anar passant manualment, per exemple per deixar-la en un totem informatiu d'una fira.

Drets sobre les imatges d'una presentació

Quan una presentació incorpora imatges que no ha fet l'autor, cal vigilar-ne els drets: una imatge trobada a un cercador no és automàticament lliure d'usar, encara que aparegui als primers resultats. Cal recórrer a bancs d'imatges amb llicència oberta o pagar-ne els drets, citant l'autor quan la llicència ho exigeixi.

Multimèdia: vídeo, àudio, podcast i subtítols

Edició de vídeo bàsica-avançada

En edició de vídeo (per exemple amb Shotcut o Kdenlive, ambdós programari lliure), cal saber tallar clips, encadenar-los en una línia de temps amb diverses pistes de vídeo i àudio, aplicar transicions i barrejar una pista d'àudio de fons amb la veu original sense que una tapi l'altra. Quan es passa d'un clip a un altre, un tall sec pot resultar brusc; per evitar-ho s'aplica una transició, com una fosa encreuada, en què el primer clip es va esvaint mentre el segon apareix gradualment, de manera que el canvi es percep suau. Pas a pas per aplicar-ne una a la línia de temps:

1. Situa dos clips consecutius a la mateixa pista.
2. Arrossega'n un lleugerament sobre l'altre perquè se solapin uns instants.
3. El programa detecta el solapament i hi aplica automàticament una transició (o la selecciones manualment d'una biblioteca de transicions).

Còdecs i contenidors

El terme clau en aquest àmbit és el còdec: un contenidor com .mp4 pot dur a dins vídeo codificat en H.264 o H.265, i àudio en AAC o MP3. El contenidor no determina la qualitat, el còdec sí, i dos fitxers .mp4 poden tenir qualitats molt diferents perquè fan servir còdecs diferents amb nivells de compressió diferents. És a dir, el còdec és qui codifica i comprimeix el vídeo i l'àudio dins del contenidor, i determina en bona part la qualitat i el pes final del fitxer.

Resolucions de vídeo

Cal distingir les resolucions habituals de vídeo: HD (1280x720, o 1920x1080, aquesta darrera anomenada també Full HD) és l'estàndard per a contingut web i televisiu, mentre que 4K (uns 3840x2160) quadruplica el nombre de píxels respecte a l'HD, oferint més detall a canvi d'un fitxer més pesant i més exigent de processar, i s'utilitza per a projeccions grans o contingut on el detall importa especialment.

Streaming, descàrrega i podcasts

Cal diferenciar streaming de descàrrega: en streaming, el contingut es reprodueix mentre s'envia des del servidor sense quedar-se emmagatzemat sencer al dispositiu, per això cal connexió constant; en descarregar un fitxer, aquest passa sencer a l'equip i queda disponible sense connexió a partir d'aquell moment. Els podcasts funcionen com un vídeo només en àudio, distribuïts per episodis amb un feed que permet subscriure-s'hi perquè els capítols nous arribin sols a l'aplicació que fas servir, sense haver de buscar-los cada vegada.

Subtítols i transcripció

Finalment, els subtítols i la transcripció milloren l'accessibilitat d'un vídeo: la transcripció és el text complet del que es diu, mentre que els subtítols en són una versió sincronitzada amb el temps (sovint en un fitxer separat, com .srt, amb marques d'entrada i sortida per a cada línia), pensada perquè es pugui seguir el contingut sense so, per exemple mirant un vídeo al mòbil en un lloc públic, o en un idioma diferent de l'original.

Integrar vs. incrustar: la diferència que confon tothom

Quan poses una imatge o un full de càlcul dins un document, tens dues opcions. Vincular (link) manté el fitxer extern separat: el document només guarda la ruta al fitxer original, de manera que si algú edita l'original, el document es pot actualitzar automàticament la propera vegada que s'obri o s'actualitzin els enllaços, però si mous o esborres el fitxer font, o l'envies a algú sense l'arxiu vinculat, l'enllaç es trenca i deixa de mostrar les dades correctament.

Incrustar (embed) copia les dades dins el document mateix: el fitxer resultant és més gran, perquè inclou una còpia completa de l'objecte, però autosuficient i no depèn de res extern. A LibreOffice, en enganxar un objecte copiat d'un altre programa, Edita - Enganxament especial permet triar explícitament "Vincula" o no; si no ho marques, per defecte s'incrusta.

L'examen sol demanar quin dels dos convé en compartir un document amb algú altre: incrustar és més segur perquè evita enllaços trencats quan el destinatari no rep també el fitxer original, mentre que vincular té sentit quan el mateix document original és actualitzat sovint per diverses persones i vols que el document que el mostra reflecteixi sempre l'última versió sense haver de tornar a copiar-hi res.

Automatització: macros, algorismes i integracions

Què és una macro

Una macro és una seqüència d'accions gravada o programada que s'executa automàticament per estalviar feina repetitiva: per exemple, aplicar un format concret a totes les cel·les que compleixen una condició, o generar cada mes un informe amb el mateix disseny a partir de dades noves. A LibreOffice es graven amb Eines - Macros - Gravar macro:

1. Inicia la gravació.
2. Fes exactament les accions que vols que es repeteixin (per exemple, seleccionar una columna i aplicar-hi un format de moneda).
3. Atura la gravació i desa la macro amb un nom.
4. La propera vegada, Eines - Macros - Executa macros repeteix totes les accions en un instant.

Les macros queden escrites en llenguatge Basic, editable des d'Eines - Macros - Edita macros per afinar-les manualment si cal, per exemple per fer-les una mica més flexibles del que la gravació literal permet.

Pensament algorísmic

Entendre una macro senzilla exigeix pensament algorísmic: seqüència de passos (fes primer això, després allò), condicionals (si passa X, fes Y; si no, fes Z) i bucles (repeteix aquesta acció per a cada fila del full, fins que s'acabin les dades). Per exemple, un algorisme senzill que aplica un format especial només a les cel·les d'un full de càlcul que superin un cert valor fa servir precisament una estructura condicional: recorre les cel·les una a una (bucle) i, per a cadascuna, comprova si es compleix la condició (si supera el valor, aplica el format; si no, la deixa igual). L'ACTIC avançat no demana programar de zero, però sí reconèixer l'estructura lògica d'un algorisme senzill i saber quan té sentit automatitzar una tasca: quan és repetitiva, segueix sempre el mateix patró previsible i es duu a terme sovint, no pas per a una tasca que només faràs una vegada.

El risc de seguretat de les macros

Precisament perquè una macro executa codi, també comporta un risc de seguretat: un document descarregat d'origen desconegut, adjunt a un correu sospitós per exemple, pot dur incrustada una macro maliciosa que s'executi en obrir el fitxer si l'usuari l'activa sense pensar-hi, i que faci accions no desitjades. Per això els programes ofimàtics mostren un avís en obrir documents amb macros i, per defecte, les desactiven fins que l'usuari les autoritza explícitament amb un clic conscient. El criteri d'examen és clar: no activar mai macros d'un document que no ve d'una font de confiança, per molt legítim que sembli el remitent del correu.

Plantilles automatitzades

Més enllà de gravar accions puntuals, l'automatització també passa per plantilles amb camps que es recalculen sols: una data que sempre mostra el dia en què s'obre el document (camp "Data", actualitzat automàticament), un número de pàgina que s'actualitza en afegir o treure fulls, o un índex que es regenera en un sol clic. La idea de fons és la mateixa que amb els estils: definir una vegada un comportament perquè es repliqui sol, sense intervenció manual cada cop.

Integracions entre eines sense programar

A un nivell més ampli, moltes eines digitals es poden integrar entre elles sense escriure ni una línia de codi: un formulari en línia, com Google Forms, que aboca automàticament les respostes a un full de càlcul compartit, o un servei que envia un avís quan arriba un correu a la Gmail amb un adjunt concret, per

exemple mitjançant un filtre de Gmail combinat amb una regla d'automatització. L'avantatge d'aquestes integracions és estalviar la còpia manual de dades d'una eina a l'altra i el risc d'error humà que això comporta: cada vegada que algú copia i enganxa dades a mà, hi ha la possibilitat de saltar-se una fila o equivocar-se de columna.

Web i publicació digital

Publicar contingut al web implica entendre, a nivell conceptual, com funciona una pàgina web. Un domini (com opoademia.com) és el nom llegible associat a l'adreça numèrica real d'un servidor, una IP amb una sèrie de números que cap persona memoritzaria de bon grat; l'allotjament (hosting) és l'espai en un servidor on viuen els fitxers de la web perquè estiguin disponibles les 24 hores del dia; i l'HTML és el llenguatge de marcatge que estructura el contingut d'una pàgina (títols, paràgrafs, imatges, enllaços) perquè el navegador el pugui interpretar i mostrar-lo amb el format correcte, encara que avui la majoria de gent no l'escriu a mà.

Els gestors de continguts (CMS, de l'anglès Content Management System), com WordPress, permeten crear i mantenir una web sense escriure codi: a nivell d'usuari, es tracta d'omplir formularis i triar plantilles (temes) i mòduls (plugins, com un formulari de contacte o una botiga en línia) des d'un tauler d'administració, en lloc d'editar fitxers HTML directament. Això democratitza la publicació web, ja que qualsevol persona sense coneixements de programació pot tenir una web funcional, però també significa que cal mantenir el CMS i els seus complements actualitzats per motius de seguretat, ja que un plugin desactualitzat és una porta d'entrada habitual per a atacs.

Un cop la web existeix, cal que es pugui trobar: el SEO, o optimització per a motors de cerca, bàsic consisteix a triar bones paraules clau, les que la gent escriuria de veritat al cercador, escriure títols i descripcions clars a cada pàgina, i estructurar el contingut amb títols jeràrquics, un únic H1 per pàgina i subtítols H2 i H3 ben ordenats, de manera que els cercadors entenguin de què tracta la pàgina i la posicionin millor entre els resultats. I per saber si tot això funciona, l'analítica web, com Google Analytics, recull dades sobre qui visita la web, des d'on, per quin dispositiu i per quines pàgines passa, informació que permet decidir què millorar, per exemple si molta gent abandona una pàgina concreta, sense haver-ho d'endevinar a ulls clucs.

Drets d'autor i llicències Creative Commons, amb detall

Tota obra original (text, imatge, música, vídeo) neix protegida per drets d'autor des del moment mateix de la seva creació, sense necessitat de cap registre ni de posar-hi el símbol de copyright: n'hi ha prou que existeixi. Les llicències Creative Commons (CC) permeten a l'autor cedir alguns d'aquests drets de manera clara i predefinida, combinant quatre elements:

- **BY** (Reconeixement/Attribution): cal citar sempre l'autor. Apareix a totes les llicències CC, és l'única condició comuna a totes elles.
- **NC** (NoComercial): prohibeix l'ús amb finalitat comercial de l'obra o de les seves derivades.
- **ND** (SenseObraDerivada): prohibeix modificar l'obra; només es pot compartir tal qual.
- **SA** (CompartirIgual): les obres derivades s'han de distribuir amb la mateixa llicència que l'original.

Així, CC BY-SA és molt permissiva, permet fins i tot l'ús comercial i la modificació, i és la llicència que fa servir la Viquipèdia: qualsevol pot reutilitzar-ne el contingut, també amb finalitats comercials, sempre que citi la font i distribueixi el resultat amb la mateixa llicència. CC BY-NC-ND és la més restrictiva d'aquest

sistema: es pot compartir citant l'autor, però ni modificar-la ni usar-la comercialment, de manera que en la pràctica només permet redistribuir l'obra intacta. Cal saber també que domini públic, marcat sovint amb CC0, vol dir que l'autor renuncia a tots els drets, i l'obra es pot fer servir sense cap restricció, ni tan sols l'obligació de citar-ne l'autor.

Exemple pràctic: si trobes una fotografia amb llicència CC BY-NC per il·lustrar un article del blog de l'acadèmia, la pots fer servir citant qui l'ha feta, però no la podries fer servir en un anunci de pagament, perquè un anunci té finalitat comercial i la llicència ho prohibeix explícitament.

Propietat intel·lectual experta: més enllà de les llicències

Quan algú modifica, tradueix o adapta una obra original crea una obra derivada, i el permís per fer-ho no és automàtic: depèn per complet de la llicència de l'obra de partida. Aquí és on la compatibilitat entre llicències CC es torna delicada: si mescles una imatge CC BY-SA amb una altra CC BY-NC en un mateix treball, el resultat ha de respectar les condicions més restrictives de totes dues alhora, SA obliga a compartir el resultat amb la mateixa llicència, i NC prohibeix comercialitzar-lo, i cal comprovar clàusula a clàusula si la barreja és viable en cada cas concret. Barrejar dues obres amb ND (sense obra derivada) directament no es pot fer mai, perquè cap de les dues permet ser modificada ni tan sols per combinar-la amb una altra.

Un altre concepte clau és la cessió de drets: un autor pot mantenir la titularitat de la seva obra i, tot i així, cedir per contracte drets d'explotació concrets a una altra persona o empresa, per exemple publicar-la en un mitjà determinat durant un temps limitat, o per a un ús geogràfic concret, sense que això equivalgui a "vendre" l'obra sencera ni a renunciar-hi per sempre; l'autor conserva altres drets que no ha cedit explícitament.

Els drets d'imatge de les persones són independents dels drets d'autor de la fotografia: encara que tinguis tots els drets sobre una foto feta per tu mateix, si hi surt una persona reconeixible, en general necessites el seu consentiment per publicar-la amb finalitats que van més enllà de l'ús personal, sobretot si és comercial o publicitari, per exemple per il·lustrar la web d'un negoci.

El contingut generat amb intel·ligència artificial planteja preguntes que la legislació encara està resolent: en molts sistemes legals actuals, una obra generada íntegrament per una IA sense intervenció creativa humana significativa no es considera protegible per drets d'autor com una obra humana, i qui utilitza eines d'IA ha de vigilar si el resultat pot infringir drets de tercers, per exemple si el sistema ha après reproduint massa fidelment obres protegides existents. El criteri per a l'examen és entendre que és un terreny legal encara en desenvolupament, no una qüestió tancada amb una resposta única i definitiva.

Finalment, quan ets tu qui crea una obra, pots llicenciar-la tu mateix: triant explícitament una llicència Creative Commons, per exemple un avís "CC BY-SA 4.0" amb un enllaç a les condicions completes al peu del document o de la pàgina, comuniques amb claredat què poden fer els altres amb el teu treball, evitant l'ambigüitat per defecte de "tots els drets reservats" quan la teva intenció real és que es pugui compartir o reutilitzar sota unes condicions concretes.

Programari lliure i copyleft

El programari lliure es defineix per quatre llibertats, segons la Free Software Foundation: la llibertat d'executar-lo amb qualsevol finalitat, la d'estudiar-ne el codi font per entendre com funciona, la de redistribuir-lo a qui vulguis, i la de modificar-lo i redistribuir les modificacions perquè altres també se'n

puguin beneficiar. No s'ha de confondre amb "gratuït": programari lliure fa referència a la llibertat d'ús, no al preu, encara que sovint també ho és de gratuït. Un truc d'examen habitual: si et donen una llista d'opcions i una diu "garantir que el programa sigui sempre gratuït", aquesta NO és cap de les quatre llibertats, perquè el preu no forma part de la definició.

El copyleft és el mecanisme legal que garanteix que aquestes llibertats es mantinguin en les versions derivades: si algú modifica un programa amb llicència copyleft, com la GPL, i el redistribueix, ha de mantenir-lo amb la mateixa llicència lliure, sense poder "tancar-lo" ni convertir-lo en programari privatiu. Això el diferencia de llicències permissives com la MIT o la BSD, que permeten crear versions privatives a partir del codi lliure original: algú pot agafar codi amb llicència MIT, modificar-lo i vendre'l després com a programari tancat sense obligació de compartir-ne el codi font resultant, cosa que amb una llicència copyleft com la GPL no és possible.

TEMA 4

Àrea 4. Seguretat

Tallafocs: de la caixa negra al control real del trànsit

A nivell avançat cal entendre el tallafoc (firewall) no com una caixa negra sinó com un conjunt de regles que filtren trànsit segons origen, destinació, port i protocol. Un tallafoc personal (el de Windows o macOS) protegeix un sol equip; un tallafoc perimetral protegeix tota una xarxa, típicament integrat al router. La diferència pràctica és d'abast: si tens un portàtil de feina i el connectes a la wifi d'un aeroport, el tallafoc perimetral de l'aeroport no et protegeix (no és teu), i és el tallafoc personal de l'equip qui ha de fer la feina.

Regles d'entrada i de sortida

Els tallafocs moderns treballen amb el concepte de regles d'entrada i sortida: no n'hi ha prou de bloquejar qui vol entrar, cal vigilar què surt, perquè un malware ja instal·lat pot intentar "trucar a casa" (connectar-se a un servidor extern per rebre instruccions o per enviar-hi dades robades). Un exemple pràctic: si de sobte l'ordinador d'una oficina comença a enviar trànsit constant cap a una IP desconeguda a mitjanit, un tallafoc ben configurat amb inspecció de sortida ho detecta i ho talla, encara que l'antivirus no hagi identificat cap fitxer maliciós. Aquest matís es pregunta sovint a l'examen: la utilitat de la inspecció de sortida és precisament detectar el malware que ja ha entrat, no evitar-ne l'entrada.

Tallafocs de nova generació (NGFW)

Els tallafocs de nova generació (NGFW) afegeixen inspecció profunda de paquets (DPI, Deep Packet Inspection), és a dir, no miren només la capçalera del paquet (l'adreça i el port, com faria un tallafoc tradicional) sinó el contingut, cosa que permet detectar aplicacions concretes encara que facin servir un port "normal" per camuflar-se. Per exemple, un tallafoc tradicional que només mira ports no pot distingir entre navegació web normal i un client de BitTorrent configurat per fer servir el port 443 (el d'HTTPS); un NGFW amb DPI sí que ho pot identificar i bloquejar-ho selectivament. Aquesta capacitat també permet crear polítiques per aplicació: permetre l'accés a la videoconferència corporativa però bloquejar xarxes socials en horari laboral, per exemple.

Pas a pas: revisar el tallafoc de Windows

En un equip amb Windows, comprovar i ajustar el tallafoc és senzill:

1. Obre el menú Inici i escriu "Seguretat de Windows" (o "Firewall de Windows Defender").
2. Entra a l'apartat "Firewall i protecció de xarxa".
3. Comprova que estigui activat per als tres tipus de xarxa: de domini, privada i pública. La xarxa pública (com la wifi d'una cafeteria) hauria de tenir sempre el nivell de protecció més estricte.
4. Per revisar o afegir una regla concreta, clica "Configuració avançada", que obre l'eina "Firewall de Windows Defender amb seguretat avançada".
5. Allà pots consultar les "Regles d'entrada" i les "Regles de sortida" per separat, i crear-ne de noves si un programa necessita accedir a internet i el sistema el bloqueja per defecte.

Pas a pas: revisar el tallafoc a macOS

A un Mac el procediment és:

1. Obre "Preferències del Sistema" (o "Configuració del Sistema" a les versions més recents).
2. Ves a l'apartat "Xarxa" i clica "Tallafocs".
3. Activa'l si no ho està, i clica "Opcions del tallafocs" per revisar quines aplicacions tenen permís per rebre connexions entrants.

Errors habituals amb el tallafoc

Un error freqüent és desactivar el tallafoc perquè "una aplicació no funciona" sense entendre per què el bloqueja; el correcte és crear una excepció puntual per a aquella aplicació concreta, no desactivar tota la protecció. Un altre error és pensar que el tallafoc del router ja protegeix qualsevol dispositiu que hi ha connectat contra tot: protegeix el perímetre (l'entrada des de fora), però no filtra necessàriament el trànsit entre dispositius de la mateixa xarxa local, ni substitueix el tallafoc personal de cada equip quan es connecta a xarxes que no controles.

Xifratge: simètric, asimètric i el cadenat HTTPS

Xifratge simètric: una sola clau

El xifratge simètric fa servir una única clau per xifrar i desxifrar (ràpid, ideal per a grans volums de dades, com quan xifrem un disc dur sencer amb BitLocker o FileVault). El problema és compartir aquesta clau de forma segura: si l'emissor i el receptor no es coneixen prèviament, com es posen d'acord en una clau sense que algú que intercepti la comunicació també l'obtingui? Aquest és exactament el problema que resol el xifratge asimètric.

Xifratge asimètric: la parella de claus

Aquí entra el xifratge asimètric, amb parella de claus pública i privada: el que es xifra amb la pública només es desxifra amb la privada corresponent, i viceversa. La clau pública, com el seu nom indica, es pot compartir obertament (fins i tot publicar-la a internet) perquè qualsevol te'n pugui enviar un missatge xifrat que només tu, amb la teva clau privada, podràs llegir. El desavantatge és que el xifratge asimètric és molt més lent computacionalment que el simètric, per això no s'utilitza per xifrar grans volums de dades directament.

Com es combinen dins HTTPS

HTTPS combina totes dues coses: primer fa servir xifratge asimètric per acordar una clau de sessió (el famós "encaixada de mans" o handshake TLS) i després xifratge simètric, molt més eficient, per a la resta de la comunicació. En termes senzills: el navegador i el servidor es posen d'acord en una clau temporal fent servir criptografia asimètrica (lenta però segura per intercanviar un secret), i a partir d'aquell moment tota la conversa (la pàgina que veus, les dades que envies en un formulari) es xifra amb aquesta clau de sessió mitjançant xifratge simètric, molt més ràpid. Aquest procés passa en fraccions de segon cada cop que obres un lloc web amb "https://" a l'adreça.

El cadenat: què garanteix i què no

El cadenat és senzill de comprovar: quan veiem el cadenat tancat al navegador, el certificat digital del lloc web ha estat validat per una autoritat de certificació (CA) de confiança. Això garanteix que la comunicació és privada (ningú la pot llegir pel camí), però no garanteix que el lloc sigui legítim: un web de phishing també pot tenir HTTPS i cadenat, perquè avui dia els certificats gratuïts (com els de Let's Encrypt) són trivials d'obtenir en pocs minuts. És un error molt estès pensar que "si té cadenat, és segur"; només vol dir que ningú intercepta la connexió pel camí, no que qui hi ha a l'altre costat sigui de fiar. Aquest matís és un

dels punts que més es pregunta a l'examen en aquest bloc.

Pas a pas: comprovar el certificat d'un lloc web

Si dubtes de la legitimitat d'una pàgina (per exemple, una que et demana dades bancàries després de rebre un correu sospitós):

1. Clica la icona del cadenat, a l'esquerra de l'adreça del navegador.
2. Selecciona "La connexió és segura" i després "El certificat és vàlid" (o similar, segons el navegador).
3. Comprova a qui s'ha emès el certificat: hauria de coincidir exactament amb el nom del domini oficial (per exemple, "labancal.com" i no "labanc-al.com" o "labancal-seguretat.info").
4. Desconfia si el domini és molt semblant però no idèntic a l'oficial: aquest és un patró clàssic de phishing, amb domini vàlid i certificat vàlid, però suplantant el lloc real.

Xifratge de disc: BitLocker i FileVault

El xifratge de disc (BitLocker a Windows, FileVault a macOS) protegeix un altre escenari: si et roben el portàtil, treure el disc i connectar-lo a un altre equip no serveix de res sense la clau, perquè tot el contingut és il·legible, cosa que una simple contrasenya d'inici de sessió no garanteix davant un accés físic directe (un atacant amb accés físic al disc pot arrencar-lo des d'un altre sistema operatiu i saltar-se la contrasenya de Windows, però no pot desxifrar el contingut sense la clau de BitLocker).

Pas a pas: activar el xifratge de disc

A Windows (edicions Pro):

1. Obre l'Explorador d'arxius i fes clic amb el botó dret sobre la unitat C:.
2. Selecciona "Activa BitLocker".
3. Segueix l'assistent i desa la clau de recuperació en un lloc segur (el compte de Microsoft, un fitxer imprès o un llapis USB apart), mai al mateix equip que xifres.

A macOS:

1. Obre "Preferències del Sistema" i ves a "Seguretat i privadesa".
2. A la pestanya "FileVault", clica "Activa FileVault".
3. Igual que amb BitLocker, guarda la clau de recuperació en un lloc separat de l'equip.

Xifratge d'extrem a extrem

El xifratge d'extrem a extrem (WhatsApp, Signal) garanteix, en canvi, que només l'emissor i el receptor poden llegir el contingut d'un missatge, ni tan sols el proveïdor del servei. El matís habitual, i que sovint es pregunta, és que protegeix el contingut però no sempre les metadades: qui parla amb qui i quan pot seguir sent visible per al proveïdor del servei, encara que el text del missatge estigui completament il·legible per a tercers.

VPN i DNS: què amaguen i què no

Què fa realment una VPN

Una xarxa privada virtual (VPN) crea un túnel xifrat entre el dispositiu i un servidor intermedi. Serveix per protegir el trànsit en xarxes wifi públiques no fiables (un bar, un aeroport, la sala d'espera d'un aeroport) i per amagar la IP real davant del lloc web de destinació, que només veurà la IP del servidor VPN.

Què no fa una VPN: mites habituals

Cal tenir clar què no fa una VPN, perquè és on més confusió hi ha entre l'usuari mitjà i l'usuari expert: no converteix la navegació en anònima del tot (el proveïdor de la VPN pot veure el trànsit si no té una política real de "no logs", és a dir, si guarda registres de la teva activitat), no protegeix contra malware ni contra phishing (si obres un fitxer infectat o entres en un lloc fals, la VPN no t'ho impedeix), i no evita que un lloc et reconegui per galetes (cookies) o per l'empremta digital del navegador (fingerprinting), que combina dades com la resolució de pantalla, el tipus de lletra instal·lat o la versió del navegador per identificar-te encara que canviïs d'IP.

VPN a la feina

En un context laboral, una VPN corporativa també serveix per accedir a recursos interns de l'empresa (una carpeta compartida, una aplicació de gestió) com si l'equip estigués físicament a l'oficina, encara que la persona treballi des de casa o des d'un altre país.

Pas a pas: activar una VPN

A un mòbil (Android o iPhone), un cop instal·lada l'aplicació de VPN de confiança:

1. Obre l'aplicació i inicia sessió amb el compte del servei.
2. Selecciona un servidor (per país o per velocitat, segons el que necessitis).
3. Prem "Connecta". El sistema operatiu et demanarà autorització per crear una configuració de VPN la primera vegada: accepta-la.
4. Comprova que el trànsit passa per la VPN visitant un lloc que mostri la teva IP pública i confirmant que correspon a la ubicació del servidor triat, no a la teva ubicació real.

El DNS: la llibreta d'adreces d'internet

De manera semblant a com el cadenat no garanteix legitimitat, el DNS també amaga menys del que sembla. El DNS tradueix el nom d'un lloc web (per exemple, "seu.gencat.cat") a una adreça IP (una sèrie de números que identifica el servidor), i aquesta consulta sovint viatja sense xifrar, cosa que permet que algú a la mateixa xarxa vegi quins llocs visites encara que la navegació vagi per HTTPS: encara que el contingut de la pàgina estigui xifrat, el nom del lloc que consultes al DNS pot no estar-ho.

DNS segur

El DNS segur (xifrat sobre HTTPS o sobre TLS), ja present a la majoria de navegadors moderns, tapa aquesta escletxa: no substitueix la VPN (perquè segueix mostrant la teva IP real al lloc de destinació), però complementa la idea que cada capa de seguretat tapa un forat diferent, i totes juntes formen una protecció més completa que qualsevol d'elles per separat.

Pas a pas: activar DNS segur al navegador

A Chrome:

1. Obre el menú (les tres puntes verticals) i entra a "Configuració".
2. Ves a "Privadesa i seguretat" i després a "Seguretat".
3. Activa l'opció "Utilitza DNS segur" i tria un proveïdor de la llista (per exemple, Cloudflare o Google).

A Firefox el procés és equivalent: "Configuració" > "Privadesa i Seguretat" > apartat "DNS sobre HTTPS", on pots activar-ho i triar proveïdor.

Defensa en profunditat: capes, privilegis mínims i segmentació

El concepte de defensa en profunditat

La seguretat avançada no es basa en un sol producte "miraculós" sinó en la defensa en profunditat: diverses capes (tallafoc, antivirus, actualitzacions, còpies de seguretat, formació de les persones usuàries) de manera que si una falla, n'hi ha una altra al darrere que aguanta. Cap capa és perfecta per si sola; el que fa robust un sistema és que les debilitats d'una capa quedin cobertes per les altres.

Actualitzacions com a política

Les actualitzacions, en aquest sentit, no s'han d'entendre com una molèstia puntual que ajornem indefinidament sinó com una política contínua: gairebé tots els grans incidents de seguretat (WannaCry n'és l'exemple de manual) exploten vulnerabilitats ja conegudes i corregides pel fabricant que la víctima encara no havia instal·lat. Configurar les actualitzacions automàtiques del sistema operatiu, del navegador i de les aplicacions habituals redueix dràsticament aquesta finestra d'exposició.

El principi de mínim privilegi

El principi de mínim privilegi diu que cap compte ha de tenir més permisos dels necessaris: cal fer servir un compte estàndard per al dia a dia i reservar el d'administrador només per instal·lar programari o canviar la configuració, perquè un malware executat des d'un compte estàndard fa molt menys mal (no pot modificar arxius de sistema ni instal·lar-se de forma persistent amb els mateixos privilegis que tindria si l'usuari treballés sempre com a administrador).

Pas a pas: crear un compte estàndard a Windows

1. Obre "Configuració" (icona de l'engranatge al menú Inici).
2. Ves a "Comptes" i després a "Família i altres usuaris".
3. Clica "Afegeix un altre usuari" i segueix l'assistent.
4. Un cop creat, entra a "Comptes" de nou, selecciona l'usuari nou i comprova que el "Tipus de compte" sigui "Estàndard" i no "Administrador".
5. Reserva el compte d'administrador (idealment amb una contrasenya diferent i forta) només per a tasques d'instal·lació o configuració.

Segmentació de xarxa

Segmentar aplica la mateixa lògica del mínim privilegi a la xarxa: una wifi separada per a convidats i per a dispositius de l'internet de les coses (com una bombeta intel·ligent o un assistent de veu, sovint amb seguretat molt més fràgil que la d'un ordinador) evita que, si un d'ells queda compromès, l'atacant salti cap als equips importants de la xarxa principal, com l'ordinador amb els documents de la feina o el telèfon amb l'aplicació del banc.

Pas a pas: crear una xarxa wifi de convidats

La majoria de routers domèstics ho permeten:

1. Escriu a un navegador l'adreça de gestió del router (normalment 192.168.1.1 o 192.168.0.1; ve indicada a l'etiqueta del mateix router).
2. Inicia sessió amb les credencials d'administrador (si no les has canviat mai, revisa l'etiqueta del router; si les has canviat i no les recordes, caldrà restaurar-lo de fàbrica).
3. Busca l'apartat "Xarxa d'convidats" o "Guest network".
4. Activa-la, posa-li un nom (SSID) diferent del principal i una contrasenya diferent.
5. Si el router ho permet, activa l'opció "Aïllament de client" (client isolation) perquè els dispositius

connectats a la xarxa de convidats no puguin veure's entre si ni accedir als dispositius de la xarxa principal.

Còpies de seguretat: la regla 3-2-1 i la còpia desconnectada

La regla 3-2-1

La regla clàssica es resumeix amb els números 3-2-1: 3 còpies de la informació (l'original més dues), en 2 suports diferents (per no dependre d'un sol tipus de dispositiu que pugui fallar igual, per exemple no tenir totes les còpies en discs durs del mateix model i del mateix lot de fabricació), i 1 còpia fora de les instal·lacions (offsite, al núvol o en un disc guardat en un altre lloc), per sobreviure a un incendi, un robatori o una inundació que afecti l'edifici on hi ha l'original.

La còpia desconnectada davant el ransomware

Cal afegir un matís que la regla clàssica, pensada originalment per a incendis o robatoris, no preveia del tot: el ransomware modern rastreja també les unitats de xarxa i els discos externs connectats, i pot xifrar còpies que estan sempre connectades a l'equip infectat. Per això la defensa real és la còpia desconnectada (offline): un disc que només es connecta durant la còpia i després es desendolla, o un núvol amb versionat que permeti recuperar versions anteriors d'un fitxer encara que les versions actuals ja estiguin xifrades pel malware.

RPO i RTO

En l'àmbit professional s'hi afegeixen dos conceptes senzills però que sovint es confonen: el RPO (Recovery Point Objective, quanta informació et pots permetre perdre segons quant fa de l'última còpia; si fas còpia cada 24 hores, el RPO és de fins a 24 hores de feina perduda) i el RTO (Recovery Time Objective, quant de temps pots estar sense el sistema fins que el restaures del tot). Una empresa amb un RTO molt baix necessita procediments de restauració ràpids i provats; una amb un RPO molt baix necessita fer còpies amb molta freqüència.

Pas a pas: fer una còpia de seguretat al núvol

Amb Google Drive a l'ordinador:

1. Instal·la l'aplicació "Còpia de seguretat i sincronització" (o "Drive per a l'escriptori") des del lloc oficial de Google.
2. Inicia sessió amb el teu compte de Google.
3. Selecciona quines carpetes de l'ordinador (Documents, Escriptori, Imatges) vols que es sincronitzin automàticament.
4. Comprova que la sincronització estigui activa mirant la icona de núvol a la barra de tasques.

Amb OneDrive (integrat a Windows), el procés és equivalent: cerca "OneDrive" al menú Inici, inicia sessió i tria les carpetes a sincronitzar des de la configuració.

Pas a pas: programar una còpia desconnectada

1. Connecta un disc dur extern només quan vulguis fer la còpia.
2. Copia-hi manualment les carpetes importants, o fes servir una eina de còpia programada (com l'Historial de fitxers de Windows, apuntant al disc extern).
3. Un cop acabada la còpia, desconnecta físicament el disc i guarda'l en un lloc separat de l'ordinador.
4. Repeteix aquest procés amb una periodicitat regular (setmanal, per exemple), segons el RPO que et

puguis permetre.

Provar les restauracions

Una còpia mai provada de restaurar no és, a la pràctica, fiable: cal fer proves periòdiques recuperant algun fitxer real de la còpia per confirmar que el procés funciona i que els fitxers no estan corromputs. Un error molt habitual és configurar les còpies de seguretat una vegada i no tornar-les a comprovar mai més, fins que fan falta de veritat i es descobreix que no funcionaven.

Programari maliciós: un zoo amb noms propis

Cal distingir bé les famílies, perquè l'examen sovint demana identificar quina característica és específica de cada una:

- Ransomware: xifra els fitxers de la víctima i en demana un rescat (sovint en criptomoneda) per desxifrar-los. El cas WannaCry (2017) va paralitzar hospitals i empreses arreu del món explotant una vulnerabilitat de Windows no actualitzada. La millor defensa no és pagar (no hi ha garantia de recuperar res) sinó tenir còpies de seguretat desconnectades de la xarxa (offline), perquè el ransomware modern també xifra les còpies connectades.
- Troià (troia): es fa passar per programari legítim (una app útil, un document adjunt aparentment normal) per obtenir accés al sistema; a diferència del cuc, no es replica sol, necessita que l'usuari l'executi.
- Cuc (worm): es propaga automàticament d'un sistema a un altre explotant vulnerabilitats de xarxa, sense necessitat que l'usuari faci res, ni tan sols obrir un fitxer.
- Spyware: recopila informació de l'usuari (hàbits de navegació, tecles premudes amb un keylogger) sense el seu consentiment, sovint de manera silenciosa i durant molt de temps abans de ser detectat.
- Adware: mostra publicitat no desitjada; sovint no és perillós per si sol però pot ser la porta d'entrada a altres amenaces, o alentir molt l'equip.
- Rootkit: s'instal·la a un nivell molt profund del sistema per amagar-se ell mateix i altres malwares, dificultant-ne enormement la detecció fins i tot per a antivirus habituals.

La doble extorsió

El ransomware actual s'ha sofisticat amb la doble extorsió: abans de xifrar els fitxers, els atacants en fan una còpia i l'extreuen cap als seus servidors, de manera que encara que la víctima restauri les còpies sense pagar, amenacen amb publicar la informació robada si no es paga el rescat, cosa que converteix un incident tècnic també en una bretxa de dades amb obligacions legals de notificació que veurem més endavant.

Pas a pas: què fer si sospites que tens malware

1. Desconnecta l'equip de la xarxa (wifi o cable) per evitar que es propagui o segueixi enviant dades.
2. No obris ni executis res més fins a comprovar l'estat de l'equip.
3. Executa un anàlisi complet amb l'antivirus instal·lat, o amb una eina de rescat que s'executi des d'un llapis USB si l'antivirus habitual no arrenca correctament.
4. Si es confirma una infecció greu (ransomware, per exemple), no paguis el rescat; valora restaurar l'equip des d'una còpia de seguretat neta anterior a la infecció.
5. Un cop resolt, canvia les contrasenyes dels serveis més sensibles des d'un altre dispositiu net, per si l'atacant les havia capturat abans de la desconnexió.

Identitat digital: gestors de contrasenyes i passkeys

Contrasenyes fortes segons el NIST

Una contrasenya forta no és només "llarga i amb símbols": la recomanació actual (NIST, l'organisme nord-americà de referència en estàndards de seguretat) prioritza la longitud per sobre de la complexitat forçada, i defensa l'ús de frases de pas ("CafèAmbLletDimarts47!") més fàcils de recordar que una combinació críptica com "Xk9#mP2", i alhora molt més difícils d'endevinar per força bruta gràcies a la seva longitud.

El problema real: la reutilització

El problema real, a nivell avançat, no és tant inventar una bona contrasenya com no reutilitzar-la mai. Si reutilitzes la mateixa contrasenya al correu, a una botiga en línia i al banc, n'hi ha prou que un d'aquests tres serveis pateixi una filtració perquè un atacant provi la mateixa combinació als altres dos (una tècnica coneguda com credential stuffing). Aquí és on el gestor de contrasenyes és imprescindible.

Com ajuda un gestor de contrasenyes

Un gestor de contrasenyes genera i recorda una contrasenya única per a cada servei, avisa si alguna ha aparegut en una filtració coneguda, i n'autocompleta les credencials només al domini legítim, cosa que dificulta caure en un lloc de phishing semblant a l'original: si el gestor no reconeix el domini (perquè és una imitació amb una lletra canviada), no autocompletarà res, i aquest silenci ja és en si mateix un senyal d'alerta.

Pas a pas: configurar un gestor de contrasenyes

1. Tria un gestor de confiança (integrat al navegador, com el de Chrome o Firefox, o una aplicació dedicada) i crea'n el compte amb una contrasenya mestra llarga i única que no facis servir enlloc més.
2. Instal·la l'extensió del gestor al navegador i, si cal, l'aplicació al mòbil.
3. Importa les contrasenyes existents (moltes eines ho permeten des d'un fitxer exportat del navegador) o vés-les desant a mesura que inicies sessió a cada servei.
4. Revisa l'informe de seguretat que sol incloure el gestor: t'assenyala contrasenyes dèbils, repetides o compromeses en filtracions conegudes.
5. Ves canviant, servei per servei, les contrasenyes repetides o dèbils per unes de generades pel mateix gestor.

La contrasenya mestra i la recuperació d'emergència

Tot el sistema descansa en una contrasenya mestra, per això cal preveure la còpia de seguretat de la volta: si es perd l'accés al gestor, calen els codis de recuperació d'emergència, guardats en un lloc físic segur i separat (no al mateix ordinador, ni en un document sense protegir). Perdre la contrasenya mestra sense tenir aquests codis pot significar perdre l'accés a totes les credencials desades de cop.

Passkeys

Les passkeys són el pas següent, pensat per eliminar la contrasenya directament. Es basen en l'estàndard FIDO2/WebAuthn: el dispositiu genera una parella de claus, la privada mai no en surt i queda protegida pel desbloqueig biomètric o el PIN del mateix dispositiu. Per iniciar sessió no s'envia cap contrasenya per la xarxa, sinó que el dispositiu signa un repte criptogràfic que el servidor verifica. Per això una passkey no es pot "phishejar": no hi ha cap secret compartit que robar, i la clau només funciona amb el domini real per al qual es va crear, de manera que si algú et porta a un lloc fals, la passkey simplement no funcionarà.

Pas a pas: crear una passkey

Al compte de Google, per exemple:

1. Entra a la configuració del compte de Google i ves a "Seguretat".
2. Busca l'apartat "Com inicies sessió a Google" i selecciona "Clau d'accés i seguretat de la clau".
3. Clica "Crea una clau d'accés" i confirma amb el desbloqueig biomètric del dispositiu (empremta digital o reconeixement facial) o amb el PIN.
4. A partir d'aquell moment pots iniciar sessió en aquell dispositiu sense escriure la contrasenya, només confirmant amb la biometria.

La verificació en dos passos: jerarquia i matisos

La verificació en dos passos (2FA) no és sempre igual de segura. Hi ha una jerarquia real que conve tenir clara:

1. SMS: el mètode més feble, vulnerable al SIM swapping (algú convenç l'operadora de traspassar el teu número a una altra targeta SIM, tècnica que veurem en detall més endavant).
2. Aplicació d'autenticació (Google Authenticator, Authy): genera codis TOTP (basats en el temps, Time-based One-Time Password) localment al dispositiu, sense dependre de la xarxa mòbil, cosa que la fa immune al SIM swapping.
3. Clau física (com YubiKey, sota l'estàndard FIDO2/WebAuthn): la més robusta, perquè requereix possessió física i és resistent al phishing, ja que la clau verifica el domini real abans d'autenticar, igual que passa amb les passkeys.

Pas a pas: activar el 2FA amb una app d'autenticació

1. Instal·la una aplicació d'autenticació al mòbil (per exemple Google Authenticator).
2. Al servei que vulguis protegir (el correu, una xarxa social), entra a "Seguretat" o "Verificació en dos passos".
3. Selecciona l'opció "Aplicació d'autenticació" i escaneja el codi QR que et mostra el servei amb la càmera de l'app.
4. Introdueix el codi de sis xifres que genera l'app per confirmar la vinculació.
5. Desa els codis de recuperació que el servei et proporciona, en un lloc segur diferent del mateix mòbil, per si el perds i necessites entrar de nou.

Els límits del 2FA

Un matís important que conve recordar per a l'examen: el 2FA redueix dràsticament el risc, però no l'elimina del tot. Un atac de phishing en temps real (adversary-in-the-middle) pot interceptar fins i tot un codi TOTP si la víctima l'introdueix en un lloc fals que el retransmet immediatament al lloc real, abans que el codi caduqui (els codis TOTP solen ser vàlids només durant trenta segons, però un atac automatitzat pot fer aquest relleu en el mateix instant).

Comptes: recuperació, filtracions i comptes oblidats

La via de recuperació

Un compte ben protegit amb 2FA es pot ensorrar igualment si el mètode de recuperació és fràgil. Cal revisar de tant en tant quin correu i quin telèfon tens configurats com a via de recuperació i mantenir-los actualitzats: un correu de recuperació que ja no controles (per exemple, un compte de la universitat que vas deixar de fer servir fa anys) és una porta oberta de bat a bat si algú aconsegueix accedir-hi.

Pas a pas: revisar la recuperació d'un compte Google

1. Entra a myaccount.google.com i ves a "Dades personals".
2. Revisa l'apartat "Informació de contacte": comprova que el telèfon i el correu de recuperació siguin actuals i que encara hi tinguis accés.
3. Ves a "Seguretat" i clica "Verificació en dos passos" per comprovar quins mètodes tens activats i eliminar els que ja no facis servir.
4. Baixa i guarda els codis de recuperació si encara no ho has fet.

Preguntes de seguretat i comptes oblidats

Els codis de recuperació d'emergència s'han de descarregar i guardar en un lloc segur, no deixar-los per quan facin falta i descobrir llavors que no els vas guardar mai. Les preguntes de seguretat clàssiques ("el nom de la teva mascota", "la ciutat on vas néixer") sovint es poden esbrinar a les xarxes socials de la víctima; una pràctica avançada és respondre-hi amb informació falsa, guardada al gestor de contrasenyes com si fos una contrasenya més, de manera que ningú pugui endevinar la resposta encara que t'investigui a fons.

Comprovar filtracions

Comprovar si les teves adreces han aparegut en alguna filtració és una revisió que qualsevol usuari expert hauria de fer de tant en tant, per exemple amb serveis com Have I Been Pwned, que permeten saber si una adreça ha sortit en alguna fuita coneguda de dades.

Pas a pas: comprovar una filtració

1. Obre un navegador i ves al lloc de Have I Been Pwned (haveibeenpwned.com).
2. Escriu la teva adreça de correu al camp de cerca.
3. Si el lloc mostra alguna filtració coneguda associada a aquella adreça, revisa a quin servei corresponia i canvia'n la contrasenya immediatament.
4. Comprova també si aquella contrasenya (o una molt semblant) l'has reutilitzat en algun altre servei, i canvia-la-hi també.

Comptes que ja no fas servir

Finalment, els comptes que ja no fas servir (una xarxa social abandonada, un fòrum de fa deu anys, un servei de compres que vas provar una vegada) no desapareixen sols: continuen guardant dades personals amb contrasenyes antigues i febles, i són l'objectiu ideal per a un atacant que fa mineria de dades per construir un perfil complet amb què després accedir als comptes que sí que t'importen avui. Auditar quins comptes tens oberts (moltes vegades el propi gestor de contrasenyes ja et n'ofereix un llistat) i eliminar els que no facis servir forma part de la higiene digital d'un usuari avançat.

Amenaces dirigides i sofisticades

Spear phishing

A diferència del phishing massiu, algunes amenaces es construeixen a mida de la víctima. L'spear phishing (phishing dirigit) parteix d'informació real sobre la persona objectiu, obtinguda de xarxes socials o filtracions prèvies, per redactar un missatge molt versemblant, per exemple mencionant el nom real del cap de la víctima o un projecte concret en què treballa.

Suplantació del CEO / Business Email Compromise

La variant corporativa és la suplantació del CEO o Business Email Compromise: l'atacant es fa passar (per correu, o amb una veu o un vídeo clonats amb intel·ligència artificial) per un directiu i demana a algú de finances una transferència urgent i confidencial, jugant amb la jerarquia i la pressa perquè no es verifiqui la petició per un altre canal. El fet que la petició vingui "de dalt" i insisteixi en la confidencialitat és precisament el que dificulta que la víctima consulti amb un company abans d'actuar.

SIM swapping

El SIM swapping mereix més detall que la simple menció com a punt feble del 2FA per SMS: l'atacant recopila dades personals de la víctima (sovint de xarxes socials o de filtracions prèvies) per convèncer l'operadora de telefonia que és ella qui ha perdut la SIM i en necessita una de nova. Si l'operadora hi cau, el número passa a una SIM en mans de l'atacant, que rep a partir d'aquell moment totes les trucades i SMS, inclosos els codis bancaris; un senyal d'alarma clàssic és quedar-se sense cobertura de sobte, sense cap raó aparent. La defensa és demanar a l'operadora un PIN addicional per autoritzar canvis de SIM i no dependre del SMS com a únic segon factor en comptes crítics, com el del banc.

Estafes amb intel·ligència artificial

Les estafes amb intel·ligència artificial afegeixen credibilitat als atacs clàssics: amb pocs segons d'àudio real (per exemple, d'un vídeo penjat a les xarxes socials) és possible clonar la veu d'una persona per a una trucada ("he tingut un accident, ingressa'm diners ara mateix"), i s'han documentat videotrucades corporatives amb participants deepfake fent-se passar per directius per autoritzar transferències multimilionàries. La defensa segueix sent la mateixa que amb qualsevol pretext urgent: verificar per un canal independent abans d'actuar, per exemple trucant directament a la persona que suposadament demana l'ajuda o l'autorització, per un número que ja teníem guardat abans, no un que ens acaben de facilitar.

Codis QR maliciosos

Els codis QR maliciosos (quishing) aprofiten que molta gent els escaneja sense pensar-hi: un adhesiu fals enganxat sobre un QR legítim d'un pàrquing municipal o d'una carta de restaurant pot portar a un lloc de phishing, i com que el contingut és una imatge, molts filtres de correu que busquen enllaços de text no ho detecten. Abans d'escanejar un QR en un espai públic, val la pena fixar-se si l'adhesiu sembla enganxat sobre un altre codi original.

Xarxes wifi falses

Les xarxes wifi falses (evil twin) creen un punt d'accés amb el mateix nom que una xarxa de confiança (per exemple, "Wifi_Aeroport_Free") perquè els dispositius s'hi connectin automàticament i tot el trànsit passi per l'equip de l'atacant, que pot llavors interceptar dades sensibles; la defensa és desconfiar de xarxes obertes en llocs públics i fer servir una VPN en xarxes que no es controlen, precisament perquè xifra el trànsit encara que la xarxa wifi sigui insegura o falsa.

Phishing i enginyeria social: la família s'amplia

El phishing clàssic per correu electrònic ha evolucionat en variants específiques segons el canal utilitzat:

- Smishing: phishing per SMS, sovint suplantant missatgeria ("el teu paquet no s'ha pogut lliurar, clica aquí") o el banc, amb un enllaç que porta a una pàgina falsa.
- Vishing: phishing per veu (trucada telefònica), on l'atacant es fa passar per suport tècnic, l'operadora o el banc per obtenir dades o convèncer la víctima d'instal·lar programari de control remot amb l'excusa de

"solucionar un problema".

- Spoofing: suplantació de la identitat d'origen d'una comunicació, ja sigui d'una adreça de correu (mostrant un remitent fals), d'un número de telèfon (mostrant un número conegut, com el del propi banc) o d'una IP.
- Whaling: phishing dirigit a càrrecs directius d'una organització, molt personalitzat i preparat amb informació real sobre la víctima.
- Pretexting: l'atacant crea una situació inventada (un "pretext") per justificar per què necessita determinada informació, com fer-se passar per un tècnic informàtic que necessita la contrasenya "per solucionar una incidència urgent".

Com verificar un missatge sospitós

La defensa avançada no es basa només a "fixar-se en les faltes d'ortografia" (els atacs actuals sovint estan ben redactats, fins i tot generats amb intel·ligència artificial, sense els errors gramaticals que abans delataven un correu fraudulent). El procediment correcte davant un missatge urgent és:

1. No cliquis cap enllaç ni obris cap adjunt directament des del missatge sospitós.
2. Identifica per un altre canal el contacte oficial (per exemple, el número de telèfon que apareix al dors de la targeta del banc, no el que et faciliten al missatge).
3. Truca o contacta per aquell canal independent i pregunta directament si la comunicació és real.
4. Si es confirma que és fals, elimina'l i, si escau, denuncia'l a l'entitat suplantada.

Aquest exemple s'aplica igual a un correu que sembla venir de l'Agència Tributària demanant "regularitzar" una devolució, a un SMS de Correus sobre un paquet retingut, o a una trucada que diu ser de la companyia elèctrica avisant d'un "tall imminent" si no es facilita un número de compte.

RGPD i LOPDGDD: el marc legal de la privadesa

Principis bàsics

El Reglament General de Protecció de Dades (RGPD, d'aplicació a tota la Unió Europea des del 2018) i la seva llei de desenvolupament a Espanya, la LOPDGDD (Llei Orgànica de Protecció de Dades i Garantia dels Drets Digitals), estableixen els principis que regeixen com es tracten les dades personals: licitud, lleialtat i transparència; limitació de la finalitat (les dades només es fan servir per allò per què es van demanar, i no per a qualsevol altra cosa que se li acudeixi a l'organització més endavant); minimització (no recollir més dades de les necessàries per a la finalitat concreta); i limitació del termini de conservació (no guardar-les indefinidament un cop deixen de ser necessàries).

Les bases jurídiques

Per tractar dades personals cal comptar amb una base jurídica que ho legitimi; el RGPD en preveu sis: el consentiment, l'execució d'un contracte, el compliment d'una obligació legal, la protecció d'interessos vitals, l'exercici de poders públics i l'interès legítim del responsable. No totes valen igual per a tot: enviar publicitat exigeix normalment consentiment, mentre que gestionar la nòmina d'un treballador es basa en el contracte laboral, sense necessitat de demanar-li permís cada mes per pagar-lo.

Responsable i encarregat del tractament

Cal distingir també entre responsable del tractament (qui decideix per a què i com es tracten les dades, com una clínica que decideix quines dades mèdiques recull dels pacients) i encarregat del tractament (qui les tracta per compte seu, com l'empresa que gestiona el servidor on es guarden aquelles dades

mèdiques), relació que s'ha de formalitzar amb un contracte de tractament de dades que fixi què pot fer i què no pot fer l'encarregat amb la informació.

Avaluació d'impacte

Quan un tractament pot comportar un risc alt (videovigilància massiva en un espai públic, dades de salut a gran escala en un hospital), el RGPD obliga a fer prèviament una anàlisi de riscos, formalitzada en una avaluació d'impacte (AIPD o EIPD, Avaluació d'Impacte relativa a la Protecció de Dades) que identifica els riscos i les mesures per reduir-los abans de començar a tractar les dades, no un cop ja s'ha detectat un problema.

Consentiment vàlid i privacy by design

El consentiment, quan és la base jurídica escollida, ha de ser lliure, específic, informat i inequívoc. Les caselles premarcades no són vàlides com a consentiment; l'usuari ha de fer una acció afirmativa clara, com marcar activament una casella buida. El privacy by design (privadesa des del disseny) obliga les organitzacions a incorporar la protecció de dades des del primer moment en què dissenyen un servei o producte, no com un pedaç que s'afegeix més endavant quan algú es queixa o hi ha una inspecció.

Els drets ARSOPOL

Els drets de la ciutadania es coneixen amb l'acrònim ARSOPOL en l'àmbit espanyol: Accés (saber quines dades té una organització sobre tu i per a què les fa servir), Rectificació (corregir-les si són incorrectes), Supressió o "dret a l'oblit" (eliminar-les quan ja no calguin per a la finalitat original), Oposició (negar-se a un tractament concret, com la publicitat directa), Portabilitat (rebre-les en un format estructurat per traspassar-les a un altre proveïdor, per exemple canviar de companyia telefònica), i Limitació del tractament (congelar-lo temporalment sense eliminar les dades, per exemple mentre es resol una discrepància). La LOPDGDD hi afegeix els drets digitals, com el dret a la desconnexió digital en l'àmbit laboral (no haver de respondre missatges de feina fora d'horari), el dret a l'educació digital o el dret a l'actualització d'informacions en mitjans de comunicació.

Pas a pas: exercir un dret ARSOPOL

1. Identifica l'organització responsable del tractament (per exemple, una empresa amb qui vas contractar un servei).
2. Envia una sol·licitud per escrit (correu electrònic o formulari del seu lloc web) indicant clarament quin dret vols exercir i sobre quines dades.
3. Adjunta un document que acrediti la teva identitat, si t'ho demanen.
4. L'organització disposa, amb caràcter general, d'un mes per respondre.
5. Si no respon o la resposta no és satisfactòria, pots presentar una reclamació davant l'autoritat de control corresponent (a Catalunya, l'Autoritat Catalana de Protecció de Dades; a la resta de l'Estat, l'AEPD).

Transferències internacionals

Quan les dades viatgen fora de la Unió Europea, entra en joc el règim de transferències internacionals: només es poden fer amb garanties equivalents a les europees, per una decisió d'adequació de la Comissió Europea sobre el país de destinació, per clàusules contractuals tipus, o per mecanismes com el marc de privadesa de dades UE-EUA, que va substituir l'antic Privacy Shield després que el Tribunal de Justícia de la UE l'invalidés (sentència Schrems II).

Sancions

L'incompliment pot comportar sancions molt elevades: fins a 20 milions d'euros o el 4% de la facturació anual global, el que sigui més alt. No són xifres teòriques: Meta va ser sancionada amb 1.200 milions d'euros el 2023 per transferir dades a Estats Units sense garanties suficients, i Amazon amb 746 milions el 2021 per la seva publicitat basada en dades personals; també hi ha sancions per vigilància excessiva de treballadors, com la imposada a una coneguda cadena de roba per emmagatzemar dades personals innecessàries dels seus empleats.

El delegat de protecció de dades

Algunes organitzacions han de nomenar un delegat de protecció de dades (DPD): és el cas de les administracions públiques i de les empreses l'activitat principal de les quals impliqui observació sistemàtica a gran escala o tractament a gran escala de dades sensibles (salut, ideologia, orientació sexual). El DPD assessora l'organització, en supervisa el compliment i fa d'enllaç amb l'autoritat de control quan cal.

Bretxes de dades i com actuar davant un incident

Què és una bretxa i el termini de notificació

Una bretxa de seguretat (data breach) és qualsevol incident que comprometi la confidencialitat, integritat o disponibilitat de dades personals. El RGPD obliga les organitzacions a notificar-ho a l'autoritat de control (a Catalunya, l'Autoritat Catalana de Protecció de Dades; a la resta de l'Estat, l'AEPD) en un termini de 72 hores des que en tenen coneixement, i a informar les persones afectades quan el risc per als seus drets sigui alt. Aquest termini de 72 hores és un dels punts que més cau a l'examen.

Pas a pas: què fer si et pirategen un compte

A escala individual, reaccionar bé davant un incident és tan important com prevenir-lo:

1. Canvia la contrasenya des d'un altre dispositiu net (no des de l'equip que pot estar compromès).
2. Tanca totes les sessions actives del compte des de la configuració de seguretat (la majoria de serveis tenen una opció com "Tanca totes les sessions" o "Dispositius connectats").
3. Revisa si s'han afegit regles de reenviament automàtic de correu que no has creat tu, perquè l'atacant continuï rebent els teus missatges encara que hagis recuperat el control del compte.
4. Activa el 2FA si encara no el tenies.
5. Avisa els teus contactes si l'atacant hagués pogut enviar missatges en nom teu.

Pas a pas: què fer davant un ransomware

Si es tracta d'un ransomware, el primer pas és desconnectar l'equip de la xarxa (treure el cable o desactivar la wifi) per evitar que es propagui a altres dispositius o còpies connectades; el consell dels experts i dels cossos policials és clar: no pagar el rescat, perquè no hi ha garantia real de recuperar els fitxers i, a més, es finança l'activitat criminal que permetrà noves víctimes. Un cop aïllat l'equip, cal valorar la restauració des d'una còpia de seguretat neta, prèvia a la infecció, i denunciar l'incident.

On demanar ajuda a Catalunya

Davant qualsevol estafa cal actuar de seguida i preservar les proves (captures de pantalla, capçaleres de correu, registres de trucades), sense esborrar res encara que faci vergonya reconèixer que s'ha caigut en un parany. Els llocs on denunciar o demanar ajuda són els Mossos d'Esquadra, la línia 017 d'INCIBE (assessorament gratuït i confidencial en ciberseguretat, disponible per telèfon i per xat) i, quan afecta

dades personals, l'Autoritat Catalana de Protecció de Dades o l'AEPD.

Benestar, vigilància i sostenibilitat digital

Tecnoestrès i disseny persuasiu

El tecnoestrès és la fatiga que genera la hiperconnexió constant: notificacions sense parar i l'expectativa implícita de respondre missatges de feina a qualsevol hora, fins i tot al vespre o el cap de setmana. No és només força de voluntat individual: cal anar més enllà del tòpic de "menys pantalles" i entendre que el problema és sovint el disseny persuasiu de moltes aplicacions (notificacions constants, scroll infinit, recompenses variables imprevisibles, similars a les d'una màquina escurabutxaques) pensat deliberadament per maximitzar l'enganxament de la persona usuària, no el seu benestar.

Pas a pas: reduir el tecnoestrès

1. Revisa la configuració de notificacions de cada aplicació i desactiva les que no siguin essencials (deixa només trucades i missatges directes de persones properes, per exemple).
2. Estableix franges horàries sense mòbil, o activa el mode "No molestar" programat per a les nits.
3. Treu les aplicacions més enganxoses de la pantalla principal, perquè calgui un pas conscient per obrir-les.
4. Si la feina ho permet, acorda amb l'equip uns límits clars sobre quan s'espera resposta a missatges fora d'horari, exercint si cal el dret a la desconnexió digital que ja hem vist.

La privadesa com a valor

La privadesa mereix defensar-se com un valor en si mateix, no només com un requisit legal per por a una sanció. L'argument de "no tinc res a amagar" ignora que la privadesa protegeix tothom: la vigilància constant, a la feina o a l'espai públic, canvia el comportament de les persones encara que no facin res de dolent (el simple fet de saber-se observat modifica com actuem), i concentra poder en mans de qui controla aquella informació.

Sostenibilitat digital

Pel que fa a la sostenibilitat digital, la petjada de carboni no és menyspreable: els centres de dades consumeixen una part creixent de l'electricitat mundial, i l'emmagatzematge "al núvol" no és immaterial encara que ho sembli, perquè al final és energia i maquinari físic en algun lloc del món.

Pas a pas: practicar una sostenibilitat digital real

1. Revisa periòdicament la safata d'entrada del correu i esborra missatges i fitxers adjunts que ja no calguin, especialment els de mida gran.
2. Buida també la carpeta de baixades i les còpies duplicades d'arxius grans (vídeos, fotos) que ocupin espai al núvol sense necessitat.
3. Allarga la vida útil dels dispositius en lloc de renovar-los cada any: una bateria que es canvia pot allargar anys la vida d'un mòbil que encara funciona bé.
4. A l'hora de triar proveïdor de núvol o d'allotjament web, valora si publica informació sobre l'ús d'energies renovables als seus centres de dades.
5. Abans de descartar un aparell que ja no fas servir, valora reparar-lo o donar-li una segona vida (venent-lo, regalant-lo) en lloc de llençar-lo directament, seguint la lògica d'una economia circular en comptes de l'"usar i llençar".

TEMA 5

Àrea 5. Resolució de problemes

Diagnosticar amb mètode: el pas a pas d'un expert

Per què cal un mètode, i no anar tocant coses

El més habitual quan un ordinador falla és tocar coses fins que sembla que torna a funcionar. Al nivell avançat de l'ACTIC no serveix: cal seguir un mètode. El clàssic és aïllar variables: reproduir el problema de forma controlada, canviar només un element cada vegada i documentar què s'ha provat. Si canvies dues coses alhora, per exemple un controlador (driver) i un cable de xarxa, i el problema desapareix, no sabràs mai quina de les dues l'ha resolt de debò; potser encara hi és, latent, i tornarà a aparèixer la setmana següent quan menys t'ho esperis. Aquest és, de fet, un dels errors més habituals que cometen fins i tot persones amb força experiència: la pressa per "acabar ja" fa saltar-se el pas de comprovar un canvi a la vegada, i el resultat és un diagnòstic que sembla resolt però que no ho és de veritat.

Si un ordinador de l'oficina no es connecta a la impressora de xarxa, no té sentit reinstal·lar el sistema operatiu abans de comprovar si l'ordinador té IP, si fa ping a la impressora i si el servei d'impressió està actiu. Un diagnòstic seriós descarta primer les causes més probables i barates de comprovar (cable, Wi-Fi, DNS) abans d'anar a les complexes (controlador corromput, conflicte de firmware). Aquest ordre d'actuació, de la causa més senzilla i probable a la més complexa i improbable, és el fil conductor de tot bon diagnòstic, i és exactament el criteri que distingeix un tècnic metòdic d'algú que va provant coses a l'atzar.

Les tres capes on pot estar l'origen d'una incidència

És útil distingir tres capes on pot estar l'origen d'una incidència: maquinari (alimentació, memòria, disc, temperatura), programari (sistema operatiu, controladors, aplicacions, permisos) i xarxa (adreçament IP, DNS, encaminament, ample de banda). Separar mentalment aquestes tres capes evita perdre temps buscant al lloc equivocat: un ordinador que "va lent a Internet" pot tenir el problema al maquinari (un disc pràcticament ple que frena tot el sistema), al programari (un navegador amb massa extensions carregades) o a la xarxa (un router saturat perquè algú està fent una descàrrega pesada). Preguntar-se primer "en quina de les tres capes pot estar això?" abans de tocar res estalvia moltes proves inútils.

Consultar els registres del sistema abans d'actuar

Abans de tocar res, val la pena mirar què ja ha quedat enregistrat. El sistema operatiu guarda automàticament un historial d'errors, avisos i esdeveniments, i llegir-lo abans d'actuar és sempre més ràpid que actuar a cegues, perquè sovint el problema ja s'hi ha manifestat abans i queda descrit amb detall.

A Windows, el visualitzador d'esdeveniments (Event Viewer) es consulta així:

1. Prem la tecla Windows i escriu "Visor de eventos" (o "Event Viewer").
2. Obre l'aplicació i desplega, a l'esquerra, "Registres de Windows".
3. Entra a "Sistema" o "Aplicació" segons si sospites d'un problema del sistema operatiu o d'un programa concret.
4. Ordena la llista per data i fixa't en les entrades marcades com a "Error" (icona vermella) properes al moment en què va aparèixer el problema.

5. Fes doble clic sobre l'entrada per veure'n el detall: sol incloure el nom del component que ha fallat i un codi d'error que es pot cercar a Internet.

En sistemes Linux, l'equivalent és consultar `journalctl` (l'historial del sistema) o els fitxers de text de la carpeta `/var/log`. No cal memoritzar la sintaxi exacta de cada comanda per a l'examen: el que importa és entendre el concepte de fons, que un registre d'errors és la memòria del sistema, i que consultar-lo és sempre el primer pas abans de reproduir un problema des de zero.

El Monitor de recursos: llegir els senyals correctes

El Monitor de recursos (o Administrador de tasques al Windows, o Monitor d'activitat al Mac) mostra en temps real el consum de CPU, memòria RAM, disc i xarxa; ordenar la llista de processos per qualsevol d'aquestes columnes sol donar la resposta a "per què va lent" en trenta segons. El procediment és senzill:

1. A Windows, prem `Ctrl + Maj + Esc` (o botó dret sobre la barra de tasques i "Administrador de tasques").
2. Ves a la pestanya "Processos".
3. Fes clic a la capçalera de la columna "CPU", "Memòria" o "Disc" per ordenar de major a menor consum.
4. Identifica el procés que encapçala la llista: si és un programa que reconeixes i que no necessites en aquell moment, el pots tancar des d'allà mateix.

Al Mac, l'eina equivalent és el Monitor d'activitat (dins d'Aplicacions > Utilitats), amb el mateix funcionament d'ordenar per columna. Aquest pas tan senzill és, a la pràctica, el que resol la majoria de casos de "l'ordinador va lentíssim" sense necessitat d'anar més enllà.

Les eines bàsiques de diagnòstic de xarxa

A xarxa, comandes com `ping`, `tracert`/`traceroute`, `ipconfig`/`ifconfig` o `nslookup` permeten saber en quin punt del trajecte es trenca la comunicació. Per fer-les servir a Windows:

1. Prem la tecla Windows, escriu "cmd" i obre el símbol del sistema.
2. Escriu `ping` seguit d'una adreça (per exemple, `ping 8.8.8.8` o `ping www.gencat.cat`) i prem Retorn.
3. Si el `ping` a l'adreça IP funciona però el `ping` al nom de domini no, el problema és de resolució DNS, no de connectivitat: l'ordinador arriba a Internet, però no sap traduir el nom que li has demanat a una adreça numèrica.
4. Escriu `ipconfig` per veure la teva pròpia adreça IP, la porta d'enllaç (el router) i el servidor DNS configurat.
5. Escriu `tracert` seguit d'una adreça per veure cada salt (hop) del recorregut fins arribar-hi.

`tracert`/`traceroute` va un pas més enllà que el `ping` i mostra cada salt del recorregut, cosa que permet localitzar exactament on es perd la connexió quan el problema no és local: si els primers salts responen amb normalitat i, a partir d'un punt concret, deixen de respondre, el problema no és al teu ordinador ni al teu router, sinó més enllà, en algun punt intermedi de la xarxa de l'operador. `nslookup`, per la seva banda, permet consultar directament quina adreça IP correspon a un nom de domini, útil per confirmar de forma independent si el problema és realment de DNS.

Cas pràctic: la impressora de l'oficina no respon

Imagina't aquesta situació, molt habitual en qualsevol oficina: en Marc arriba un dilluns i la impressora de xarxa no li respon, tot i que dijous passat funcionava sense problemes. Un diagnòstic per capes, ben fet, seguiria aquest ordre:

1. Comprova primer el maquinari més bàsic: la impressora té llum verda? Té paper i tòner? Algú l'ha apagat sense voler durant el cap de setmana de neteja?
2. Si el maquinari sembla correcte, passa a la xarxa: obre el símbol del sistema i fes `ping` a l'adreça IP de la impressora. Si respon, la impressora té connexió; si no respon, comprova el cable de xarxa o si la impressora s'ha reconnectat a una IP diferent (algunes impressores canvien d'IP si es reinicia el router).
3. Si el `ping` funciona però el document no s'imprimeix, el problema és de programari: comprova la cua d'impressió de l'ordinador (pot haver-hi un document antic bloquejant-la) i que el servei d'impressió del sistema operatiu estigui actiu.
4. Només si res d'això funciona té sentit plantejar-se reinstal·lar el controlador de la impressora, i encara menys reinstal·lar el sistema operatiu sencer, que seria un error clàssic de saltar-se l'ordre lògic.

Errors habituals en diagnosticar, i el que cal recordar per l'examen

Els errors més freqüents en un diagnòstic mal fet solen ser sempre els mateixos: començar per la solució més dràstica sense haver descartat les causes senzilles, canviar diverses coses alhora i no saber després quina ha estat la solutiva real, i no consultar mai els registres del sistema tot i tenir-los disponibles i gratuïts. Val la pena fixar dues idees, perquè reapareixen sovint formulades amb casos diferents: l'ordre correcte de treball (de la causa senzilla a la complexa) i què indica que un `ping` per IP funcioni però per nom de domini no (sempre DNS).

Quan arrencar net, quan restaurar i quan reinstal·lar

Arrencada neta: pas a pas

Quan un problema apareix just després d'instal·lar un programa o un controlador, la temptació és desinstal·lar-ho tot i tornar a començar, però hi ha passos intermedis més eficients. L'arrencada neta (clean boot) engega el sistema amb el mínim de serveis i programes d'inici imprescindibles: si el problema desapareix, es tracta d'anar reactivant serveis d'un en un fins a trobar el culpable. A Windows, es fa així:

1. Prem la tecla Windows, escriu "msconfig" i obre "Configuració del sistema".
2. Ves a la pestanya "Serveis", marca la casella "Amaga tots els serveis de Microsoft" i fes clic a "Inhabilita-ho tot".
3. Ves a la pestanya "Inici" (o obre l'Administrador de tasques i la pestanya "Inici" si estàs en una versió recent de Windows) i desactiva els programes que s'obren en engegar l'ordinador.
4. Reinicia l'equip: ara arrenca només amb el mínim indispensable.
5. Si el problema ha desaparegut, torna a activar els serveis i programes d'un en un, reiniciant entre cada activació, fins que el problema torni a aparèixer: aquell serà el responsable.

Mode segur: pas a pas i quan fer-lo servir

El mode segur (safe mode) és semblant a l'arrencada neta però més restrictiu, perquè carrega només els controladors bàsics del sistema operatiu, sense els de tercers, i és l'eina de referència quan es sospita d'un controlador de vídeo, de xarxa o d'àudio recentment actualitzat. Per entrar-hi a Windows:

1. Des del menú Inici, mantén premuda la tecla Maj (Shift) mentre fas clic a "Reinicia".
2. A la pantalla blava que apareix, selecciona "Solucionar problemes" > "Opcions avançades" > "Configuració d'inici" > "Reinicia".
3. Quan l'ordinador torna a engegar, apareix una llista numerada d'opcions; prem la tecla corresponent a "Habilita el mode segur amb funcions de xarxa" si necessites Internet, o simplement "Mode segur" si no.
4. Un cop dins, comprova si el problema que et va portar allà (una pantalla que parpelleja, un so

distorsionat) ha desaparegut: si és així, el sospitós més probable és el controlador corresponent, i toca actualitzar-lo o revertir-lo des del Gestor de dispositius.

Després d'actualitzar un controlador i començar a tenir problemes de pantalla, aquesta és precisament l'estratègia més adequada: arrencar en mode segur per aïllar si el problema prové d'aquest controlador, abans de plantejar-se res més dràstic.

Restaurar el sistema a un punt anterior

Si el problema ve d'un canvi recent i concret (una actualització, una instal·lació), restaurar el sistema a un punt anterior desfà exactament aquell canvi sense afectar els documents. És l'opció intermèdia entre "no fer res" i "reinstal·lar-ho tot": ràpida, reversible i que no fa perdre feina. A Windows, l'eina es diu System Restore:

1. Prem la tecla Windows, escriu "Crea un punt de restauració" i obre l'opció corresponent.
2. Fes clic al botó "Restauració del sistema".
3. Selecciona un punt de restauració anterior al moment en què va començar el problema (Windows en crea automàticament abans de moltes actualitzacions i instal·lacions).
4. Confirma i deixa que l'equip es reinicïi: en acabar, els programes i configuracions tornaran a l'estat d'aquell punt, però els teus documents personals no es veuran afectats.

Al Mac, l'equivalent és una còpia de Time Machine, que permet recuperar l'estat complet del sistema en una data anterior. En un servidor virtualitzat, el mecanisme habitual és un punt de restauració (snapshot), una fotografia completa de l'estat de la màquina virtual en un instant concret, a la qual es pot tornar en qualsevol moment. En tots tres casos, la idea de fons és la mateixa: capturar un estat conegut i bo, i poder-hi tornar sense haver de refer res des de zero.

Reinstal·lar de zero: quan és realment la millor opció

Reinstal·lar el sistema operatiu de zero és, malgrat tot, de vegades la millor opció, i saber-ho triar és part de la competència avançada. Té sentit quan el temps que costaria diagnosticar i netejar un sistema molt deteriorat (programari brut acumulat, un malware persistent que es reactiva després de cada neteja, anys de configuracions incompatibles entre si) supera clarament el temps que costa configurar-lo de nou, o quan es prepara un equip per a un altre usuari i cal garantir que no queda cap rastre de dades anteriors. La clau és no fer-ho servir com a primer recurs per estalviar-se pensar, sinó com a decisió raonada quan les alternatives ja no compensen: si arrencada neta, mode segur i restauració del sistema no han resolt res, o si el diagnòstic ja apunta a un problema massa profund i acumulat, aleshores sí que reinstal·lar surt a compte.

Cas pràctic: un ordinador va lent i erràtic després d'instal·lar un programa nou

La Laura instal·la un programa de disseny nou i, des d'aleshores, l'ordinador va lent i de tant en tant es queda penjat. Seguint l'ordre lògic d'aquest apartat:

1. Primer prova una arrencada neta: si l'ordinador torna a anar fluid, el problema és algun servei o programa d'inici, potser el mateix programa nou o algun component que instal·la de manera automàtica.
2. Si l'arrencada neta no ho resol, i sospita concretament d'un controlador (per exemple, el de la targeta gràfica, si el programa de disseny n'ha instal·lat un de nou), prova el mode segur.
3. Si tampoc això funciona però sap exactament quin dia va començar el problema, la restauració del sistema a un punt anterior a la instal·lació és la següent opció, ja que desfà el canvi sense tocar els seus documents ni els dissenys ja fets.

4. Només si res d'això funciona, i l'equip ja arrossegava altres problemes previs, té sentit valorar una reinstal·lació completa.

Truc per a l'examen: no confondre les tres opcions

Aquestes tres eines es confonen sovint perquè totes tres "arreglen" coses, però actuen de manera diferent: l'arrencada neta i el mode segur no canvien res de manera permanent, només limiten què s'executa en aquella sessió, per poder aïllar el culpable; la restauració del sistema sí que desfà canvis reals, però només els dels programes i configuracions, mai els documents; i la reinstal·lació és l'única que esborra tot i comença de zero.

Maquinari, programari i xarxa: casos habituals

Un ordinador que no arrenca: els pips de la BIOS

Un ordinador que no arrenca i fa un so de pips repetits està donant un codi POST: cada patró de pips (segons el fabricant de la BIOS) indica un component concret que falla, sovint la memòria RAM mal encaixada. Davant d'aquesta situació, el primer pas pràctic, abans de buscar el significat exacte del codi (que varia segons el fabricant de la placa base), és obrir la caixa i comprovar que els mòduls de memòria estan ben encaixats als seus sòcols; és una causa sorprenentment freqüent, sobretot després de transportar l'equip o de fer-hi neteja interior.

Un ordinador extremadament lent amb el disc gairebé ple

Un sistema que arrenca però va extremadament lent pot tenir el disc gairebé ple, massa programes a l'inici o un procés en segon pla consumint recursos; el Task Manager ordenat per ús de CPU o disc sol donar la resposta, tal com s'ha vist a l'apartat anterior. Un truc pràctic per alliberar espai ràpidament és revisar la carpeta de descàrregues (sol acumular fitxers oblidats de mesos), buidar la paperera i desinstal·lar programes que no s'utilitzen; si el disc arriba pràcticament al 100% de la seva capacitat, el mateix sistema operatiu comença a anar més lent perquè li falta espai de maniobra per als seus propis fitxers temporals.

Quan un programa deixa de funcionar després d'una actualització

La incompatibilitat entre versions de programari (una macro d'Excel que deixa de funcionar en actualitzar Office, o una aplicació que no arrenca després d'una pujada de versió del sistema operatiu) es resol comprovant els registres de canvis (cha ngelog) i, si cal, fent un rollback controlat en lloc de reinstal·lar-ho tot de zero. El procediment recomanat, davant d'aquest tipus de cas, és:

1. Consulta el registre de canvis (changelog) de l'actualització: sol explicar quines funcions s'han modificat o retirat, i sovint hi trobaràs directament la causa.
2. Si l'actualització ha desactivat macros per motius de seguretat (un canvi habitual en versions recents d'Office), revisa la configuració de seguretat de macros a l'aplicació abans de donar per fet que la macro "s'ha trencat".
3. Si el problema persisteix i és urgent, valora fer un rollback (tornar a la versió anterior) mentre s'investiga amb calma la solució definitiva, en lloc de deixar sense eina de treball a qui la necessita.
4. Documenta la incidència perquè, si torna a passar amb la propera actualització, ja hi hagi un procediment conegut.

IP privada, IP pública i NAT

A xarxa, cal distingir IP privada (dins la xarxa local, per exemple 192.168.1.25) d'IP pública (la que el router

mostra cap a Internet), i entendre el paper del NAT (traducció d'adreces de xarxa): totes les IP privades d'una casa surten a Internet amb una única IP pública compartida. És a dir, quan des de casa fas un tràmit a la seu electrònica de l'ajuntament, el servidor de l'ajuntament no veu la IP privada del teu portàtil (192.168.1.25), sinó la IP pública del teu router, que és la mateixa per a tots els dispositius de casa teva: el mòbil, la tauleta i l'ordinador de sobretaula surten tots amb la mateixa "cara" cap a l'exterior, tot i tenir adreces diferents internament. El NAT és precisament el mecanisme que fa aquesta traducció d'anada i tornada, perquè les respostes sàpiguen a quin dispositiu concret de dins de casa han de tornar.

Quan una única aplicació "no es connecta a Internet"

Un firewall mal configurat que bloqueja un port és una causa freqüent que una aplicació "no es connecti a Internet" mentre la resta funciona amb normalitat. Aquest és un patró que cal reconèixer bé: si el navegador funciona, el correu funciona, però una aplicació concreta (per exemple, un programa de videotrucades o un joc en línia) no aconsegueix connectar, el més probable no és un problema de xarxa general, sinó que el tallafocs (firewall) del sistema o del router està bloquejant específicament el port que fa servir aquell programa. La comprovació passa per revisar la configuració del firewall de Windows (Configuració > Privadesa i seguretat > Seguretat de Windows > Tallafocs i protecció de xarxa) i comprovar si l'aplicació hi apareix permesa.

Xarxes domèstiques i d'oficina, a fons

Les dues bandes de Wi-Fi: 2,4 GHz i 5 GHz

El router és el centre de qualsevol xarxa local, i entendre'l a fons és cada vegada més part de la competència digital quotidiana. El Wi-Fi es transmet en dues bandes de freqüència habituals: 2,4 GHz, que arriba més lluny i travessa millor les parets però és més lenta i pateix més interferències (perquè la comparteixen molts altres aparells domèstics, com microones o telèfons inalàmbrics), i 5 GHz, que va més ràpid però té menys abast. A la pràctica, un mòbil o un portàtil connectats a la xarxa de 5 GHz a la mateixa habitació que el router aniran notablement més ràpid, però si et mous a l'altra punta de la casa amb parets de per mig, sovint és la xarxa de 2,4 GHz la que manté la connexió estable mentre la de 5 GHz es perd.

Ampliar la cobertura: repetidor, mesh o PLC?

Un pis gran amb el router en un extrem sol necessitar cobertura addicional, i hi ha tres solucions habituals amb comportaments força diferents:

Un repetidor Wi-Fi capta el senyal existent i el retransmet, però crea una xarxa nova (o duplica el nom) i afegeix un salt que pot introduir latència: el dispositiu es connecta al repetidor, que al seu torn parla amb el router, i cada salt suma un petit retard.

Un sistema mesh instal·la diversos punts coordinats entre si que formen una única xarxa intel·ligent, amb un sol nom i canvi automàtic de punt: mentre et mous per casa amb el mòbil, et vas connectant sense adonar-te'n al punt mesh més proper, sense haver de canviar mai de xarxa manualment. Sol donar millor resultat en habitatges grans precisament per això.

El PLC (Power Line Communication) és una tercera via: fa servir la instal·lació elèctrica de l'edifici per portar les dades mitjançant endolls, útil quan el Wi-Fi no hi arriba de cap manera (per exemple, un soterrani o un annex separat de la casa principal amb parets molt gruixudes), encara que el rendiment depèn molt de l'estat del cablejat i pot no funcionar bé entre circuits diferents del quadre elèctric.

DNS i el cas de "tinc Wi-Fi però no tinc Internet"

A nivell conceptual, cada dispositiu d'una xarxa necessita una adreça IP per identificar-se, i el DNS fa la feina de traduir noms fàcils de recordar (un domini web) a l'adreça IP numèrica que fa servir la xarxa per comunicar-se; és per això que, com s'ha vist abans, un `ping` que funciona per IP però no per nom assenyala sempre un problema de DNS.

Un cas molt habitual a la pràctica és "tinc Wi-Fi però no tinc Internet": el símbol de Wi-Fi ple només indica que el dispositiu s'ha connectat correctament al router, no que el router tingui sortida a Internet. Imagina't que un vespre vols pagar la factura de la llum a través de la web de la comercialitzadora, i el mòbil mostra totes les barres de Wi-Fi però la pàgina no carrega mai: si el mòdem ha perdut la connexió amb el proveïdor, o el servidor DNS no respon, es manté la xarxa local (es pot imprimir, compartir fitxers entre ordinadors de casa) però no arriba res de l'exterior. Distingir aquests dos nivells, la connexió al router i la connexió del router a Internet, és la clau per no confondre's diagnosticant: en aquest cas, no cal reiniciar el mòbil ni tocar la configuració Wi-Fi, sinó comprovar el mòdem o esperar que el proveïdor restableixi el servei.

QoS: prioritzar qui necessita la xarxa de veritat

Un router modern permet també prioritzar dispositius mitjançant QoS (Quality of Service): es pot indicar que una videotrucada de feina tingui preferència sobre una descàrrega en segon pla, cosa que evita talls quan diverses persones fan servir la xarxa alhora. Un cas típic: mentre fas una videotrucada important per feina, algú altre a casa comença a veure una sèrie en 4K o descarregar un fitxer pesat, i la trucada comença a tallar-se; configurar el QoS del router perquè prioritzi el trànsit de videotrucades sobre el de descàrrega evita aquest problema sense haver de demanar a ningú que deixi de fer servir Internet.

Xarxa de convidats i dispositius IoT

Igualment recomanable és crear una xarxa de convidats, separada de la principal: permet que les visites naveguin sense accedir als dispositius i carpetes compartides de casa, i limita el risc si l'equip d'un convidat porta programari maliciós. Aquesta lògica de separació és encara més important amb els dispositius IoT (Internet de les coses): bombetes, càmeres o altaveus intel·ligents solen portar credencials per defecte que molts usuaris no canvien mai, reben actualitzacions de seguretat amb poca freqüència i, un cop compromesos, poden fer servir la connexió per atacar altres equips de la xarxa. Posar-los en una xarxa de convidats separada, i canviar sempre l'usuari i la contrasenya de fàbrica, redueix molt aquest risc.

Cas pràctic: configurar la xarxa domèstica bàsica, pas a pas

Un exercici habitual per posar en pràctica tot aquest apartat és entrar a la configuració del propi router:

1. Obre el navegador i escriu l'adreça IP del router (normalment 192.168.1.1 o 192.168.0.1; si no la saps, executa `ipconfig` i mira la "porta d'enllaç predeterminada").
2. Introdueix l'usuari i la contrasenya d'administració (si mai no els has canviat, sol venir escrit a l'etiqueta del mateix router; canviar-los és el primer que caldria fer).
3. Busca l'apartat de xarxes sense fils (Wi-Fi) i comprova si hi ha una xarxa de 2,4 GHz i una de 5 GHz diferenciades.
4. Localitza l'opció de "xarxa de convidats" (guest network) i activa-la si vols oferir Internet a visitants sense donar-los accés a la resta de dispositius de casa.
5. Si el router ho permet, entra a l'apartat de QoS i marca com a prioritaris els dispositius que facis servir per a videotrucades de feina.

Maquinari amb criteri

Els tres components que cal conèixer

Un equip es pot descriure per uns quants components clau: el processador (CPU) fa els càlculs, la memòria RAM és l'espai de treball on el sistema manté obert tot allò que s'està fent servir, i l'emmagatzematge (disc) guarda la informació de manera permanent. Una manera senzilla d'imaginar-ho és pensar en una taula de treball: el disc és l'armari on es guarda tot de forma permanent, la RAM és la superfície de la taula on es col·loquen els documents que s'estan fent servir en aquell moment, i el processador és la persona que hi treballa. Una taula petita (poca RAM) obliga a desar i tornar a treure documents constantment, cosa que alenteix tota la feina encara que la persona (el processador) sigui molt ràpida.

SSD contra HDD

El SSD (unitat d'estat sòlid) llegeix i escriu dades moltíssim més ràpid que un HDD (disc dur mecànic) perquè no té peces mòbils, i per això un ordinador amb SSD s'engega i obre programes molt més de pressa; el HDD continua tenint sentit quan cal molt d'espai a baix cost, per exemple per emmagatzemar còpies de seguretat o arxius grans que no es consulten cada dia. La diferència de velocitat no és subtil: un ordinador que triga un minut a arrencar amb un HDD pot arrencar en pocs segons amb un SSD, i és, amb diferència, la millora individual que més es nota en un equip antic.

El coll d'ampolla: on val la pena invertir

Un concepte clau per decidir on invertir és el coll d'ampolla: el component que limita el rendiment de tot el conjunt, encara que la resta siguin excel·lents. Ampliar la memòria RAM d'un equip amb un disc dur mecànic molt ple i fragmentat no soluciona gaire cosa si el problema real és la velocitat del disc; en canvi, canviar aquell mateix disc per un SSD sol notar-se molt més que qualsevol altra millora aïllada. Saber identificar quin és el coll d'ampolla abans de gastar diners és exactament el criteri que distingeix un usuari avançat: la manera pràctica de fer-ho és tornar al Monitor de recursos vist al primer apartat i observar, mentre l'ordinador va lent, quin dels quatre indicadors (CPU, RAM, disc, xarxa) es manté sistemàticament al límit.

Ampliar o renovar l'equip

D'aquí ve també la decisió d'ampliar versus renovar: quan un equip és relativament recent i només li falta memòria o un SSD, ampliar-lo surt molt a compte; quan la placa base o el processador ja no admeten més memòria, o el maquinari és tan antic que no aguanta les versions actuals de programari, val més renovar l'equip sencer. El criteri de fons és sempre el mateix: si el maquinari base (placa i processador) encara admet la millora, val la pena ampliar; si ja ha arribat al seu límit físic, cap ampliació parcial no compensarà, i és millor invertir en un equip nou sencer.

Compatibilitat de components abans de comprar

Cal tenir en compte, a més, la compatibilitat de components a nivell d'idea: no qualsevol peça encaixa amb qualsevol altra (el sòcol del processador ha de coincidir amb el de la placa base, el tipus de memòria RAM, per exemple DDR4 o DDR5, ha de ser el que admet la placa), i comprovar les especificacions abans de comprar una peça estalvia disgustos. Abans de comprar un mòdul de memòria RAM per ampliar un ordinador, la comprovació imprescindible és sempre la mateixa: mirar quin tipus de memòria admet exactament la placa base (no només la quantitat màxima, sinó la generació concreta, perquè un mòdul DDR5 no funciona en una placa que només admet DDR4).

Perifèrics professionals segons la necessitat

Més enllà de l'ordinador en si, els perifèrics professionals responen a necessitats concretes: un monitor amb calibratge de color per a qui treballa amb imatge, un teclat mecànic o un ratolí ergonòmic per a qui hi passa moltes hores, un escàner de qualitat per a qui digitalitza documents amb regularitat. Triar el perifèric adequat no és un caprici: una persona que edita fotografies professionalment amb un monitor mal calibrat pot lliurar feina amb colors que es veuran diferents en qualsevol altra pantalla.

Vigilar la salut del maquinari abans que falli

I val la pena vigilar la salut del maquinari abans que falli del tot: els discos incorporen un sistema anomenat SMART que en monitoritza l'estat intern i pot avisar amb temps d'una fallada imminent, i les bateries dels portàtils es degraden amb els cicles de càrrega, motiu pel qual els sistemes actuals solen mostrar un percentatge de "salut de la bateria" que baixa amb els anys encara que continuï carregant-se amb normalitat.

Escollir l'eina adequada, no la que ja coneixem

Full de càlcul o base de dades?

Una competència avançada real és saber triar l'eina segons la necessitat, no per costum. El dubte més típic a la feina és full de càlcul o base de dades. Un full de càlcul (Excel, Google Sheets) és ràpid per a anàlisis puntuals, càlculs visuals i informes petits amb poques desenes de files relacionades. Una base de dades (Access, PostgreSQL, MySQL) és la resposta quan hi ha múltiples usuaris escrivint alhora, quan cal garantir que no s'hi dupliquen registres (integritat referencial), quan el volum creix per sobre de desenes de milers de files o quan diverses taules s'han de relacionar sense repetir informació.

Portar un registre de socis d'una entitat en un full de càlcul funciona fins que dues persones l'editen a la vegada i es trepitgen els canvis; aleshores cal migrar a una base de dades amb control d'accés real. Imagina't una associació de veïns amb dues-centes persones sòcies: mentre és la mateixa persona qui gestiona el full de càlcul en solitari, funciona; el dia que dues persones voluntàries diferents necessiten actualitzar dades alhora (una dona d'alta a un nou soci mentre l'altra registra un pagament), el full de càlcul comença a donar problemes de sobreescriptura que una base de dades relacional resol de sèrie.

Els criteris que haurien de pesar en triar una eina digital

Els criteris de selecció d'eines digitals, en general, haurien d'incloure: cost total (llicència més manteniment), interoperabilitat (exporta a formats oberts com CSV o ODS?), escalabilitat (aguanta si el volum de dades es multiplica per deu?), accessibilitat (la poden fer servir persones amb diversitat funcional?) i el que se sol oblidar: qui es queda amb les dades si es deixa d'utilitzar el servei. Aquest darrer punt és, sovint, el que decideix la tria a llarg termini, i és precisament el criteri que amb més facilitat es passa per alt quan es tria una eina només mirant el preu o la interfície del primer dia.

Programari lliure o propietari: una qüestió de control

Triar programari lliure enfront de propietari no és una qüestió ideològica sinó de control: què passa si l'empresa que el fabrica tanca o canvia el model de negoci. Amb programari lliure, el codi font és accessible i, si el projecte s'abandona, sempre hi ha la possibilitat que algú altre el continuï o que es pugui migrar les dades sense dependre d'una única empresa. Amb programari propietari, si l'empresa desapareix o decideix pujar molt el preu de cop, l'usuari queda en una posició més feble.

Programari expert: versions, entorns i comptes

Actualitzar amb criteri

Gestionar versions i compatibilitat és una feina contínua: mantenir el programari actualitzat corregeix vulnerabilitats de seguretat, però en un entorn crític (una empresa, un servei que no es pot aturar) cal comprovar abans que l'actualització no trenqui res, llegint el registre de canvis i, si és possible, provant-la primer en un equip que no sigui de producció. El procediment prudent, en aquests casos, seria:

1. Llegir el registre de canvis (changelog) de la nova versió per identificar si afecta funcions crítiques.
2. Instal·lar l'actualització primer en un equip de prova, mai directament al sistema que dona servei real.
3. Comprovar que les funcions essencials continuen funcionant correctament en aquest entorn de prova.
4. Només llavors, desplegar l'actualització a la resta d'equips, idealment en un moment de baix ús.

Treballar al núvol

Cada vegada més, la feina no viu en un sol ordinador sinó al núvol: treballar amb documents i eines emmagatzemats en serveis com Google Workspace o Microsoft 365 permet continuar exactament on ho havies deixat des de qualsevol dispositiu amb connexió, amb l'avantatge de la continuïtat però també la contrapartida de dependre d'Internet i de confiar les dades a un proveïdor extern. Si vols demanar cita al CAP des del mòbil pel matí i completar un tràmit relacionat des de l'ordinador de la feina a la tarda, el treball al núvol fa possible aquesta continuïtat.

Màquines virtuals

Una màquina virtual, a nivell conceptual, és un ordinador simulat per programari dins d'un ordinador real: eines com VirtualBox, VMware o Hyper-V permeten fer córrer un sistema operatiu sencer dins d'una finestra del sistema principal. Serveix per provar programari dubtós sense arriscar l'equip real, per fer servir un sistema operatiu diferent del propi (per exemple, Linux dins d'un Windows), o per mantenir entorns de prova aïllats de l'entorn de producció. No cal saber-la configurar per a l'ACTIC avançat, sinó entendre per a què serveix i quan té sentit enfront d'instal·lar el programari directament: si dubtes de si un programa descarregat d'una font poc habitual pot ser maliciós, provar-lo primer dins d'una màquina virtual evita que, si ho és, faci mal a l'equip real.

Comptes d'usuari i permisos

La gestió de permisos i comptes d'usuari també és part del criteri expert: treballar sempre amb un compte administrador, en lloc d'un compte estàndard per al dia a dia, amplia molt la superfície de risc si s'executa per error un programa maliciós, perquè aquest hereta els mateixos permisos que l'usuari que l'ha llançat. En entorns compartits (una oficina, una família), assignar comptes diferenciats amb els permisos justos que necessita cada persona evita tant errors accidentals com accessos indeguts.

Instal·lar i desinstal·lar amb criteri

Finalment, instal·lar i desinstal·lar programari amb criteri vol dir mantenir-ho simple: descarregar sempre de la font oficial, sense complicar-se la vida amb instal·lacions automatitzades o silencioses que no aporten res a un usuari normal, i en desinstal·lar, fer-ho de manera neta, perquè moltes aplicacions deixen enrere fitxers de configuració o entrades residuals que un desinstal·lador ben fet hauria de retirar. Un sistema ple d'aquestes restes acaba anant més lent i és més difícil de diagnosticar.

Automatització i productivitat

Dreceres de teclat que fan guanyar temps cada dia

El nivell avançat pressuposa un ús creatiu de la tecnologia, no només d'usuari passiu. La productivitat comença per coses senzilles: dominar dreceres de teclat avançades (no només copiar i enganxar, sinó moure's entre finestres, cercar dins d'un document llarg, desar amb un sol gest) estalvia temps acumulat cada dia i redueix la dependència del ratolí. Algunes de les més rendibles a la pràctica: `Alt + Tab` per canviar entre finestres obertes, `Ctrl + F` per cercar una paraula dins d'un document o d'una pàgina web, `Ctrl + S` per desar sense passar pel menú, `Ctrl + Z` per desfer un error abans que sigui massa tard, i `Ctrl + Maj + T` al navegador (Chrome, Edge, Firefox) per recuperar la darrera pestanya tancada per error. Cap d'elles és espectacular per separat, però la suma de segons estalviats cada dia, multiplicada per un any de feina, és considerable.

Plantilles i respostes automàtiques de correu

Les plantilles i les respostes automàtiques de correu eviten redactar des de zero un missatge que es repeteix sovint. A Gmail, es configuren així:

1. Fes clic a la roda dentada de configuració, a dalt a la dreta, i entra a "Veure tots els ajustos".
2. Ves a la pestanya "Avançat" i activa l'opció "Plantilles".
3. Torna a redactar un correu nou; escriu el text que vulguis reutilitzar.
4. Fes clic als tres punts de la finestra de redacció, entra a "Plantilles" i tria "Desa el redactat com a plantilla".
5. La propera vegada, obre un correu nou, torna a "Plantilles" i selecciona la que has desat per inserir-la de cop.

Regles i filtres per no ofegar-se a la safata d'entrada

Les regles i filtres classifiquen automàticament els missatges entrants (per remitent, per assumpte, per paraules clau) perquè la safata d'entrada no es converteixi en un caos. A Gmail:

1. Fes clic a la fletxa desplegable dins de la barra de cerca, a dalt.
2. Omple el criteri que vulguis filtrar (per exemple, tots els correus d'un remitent concret, o que continguin una paraula clau a l'assumpte).
3. Fes clic a "Crea un filtre".
4. Tria l'acció que s'ha d'aplicar automàticament: aplicar una etiqueta, arxivar-lo directament, marcar-lo com a llegit o destacar-lo com a important.

Automatitzar entre aplicacions diferents

Un pas més enllà hi ha l'automatització entre aplicacions diferents: una macro a Excel/Sheets que genera un informe mensual, o eines com Zapier, Make o IFTTT que connecten serveis diferents (per exemple, que cada resposta d'un formulari de Google es guardi automàticament en un full de càlcul i enviï un correu de confirmació). Aquestes plataformes funcionen totes amb la mateixa lògica: un disparador (trigger) i una acció, és a dir, quan passa X, fes Y. El disparador pot ser tan senzill com "algú envia un formulari" o "arriba un correu amb un adjunt", i l'acció, la resposta automàtica que se'n deriva sense que ningú hagi de fer res manualment.

RPA: automatització de tasques repetitives basades en regles

Un pas encara més avançat en aquest món és el RPA (Robotic Process Automation, automatització robòtica de processos): programari que imita, pas a pas, les accions que faria una persona sobre diverses aplicacions (obrir un programa, copiar una dada, enganxar-la a un altre sistema, prémer un botó) i les repeteix exactament igual cada vegada. El RPA és més adequat per a tasques repetitives i basades en

regles clares, com copiar dades entre sistemes seguint sempre els mateixos passos, per exemple traspassar cada matí les comandes rebudes per correu a un programa de facturació intern que no té cap connexió directa amb el correu. A diferència d'una integració via API, el RPA no necessita que els dos sistemes "es parlin" tècnicament entre si: simplement repeteix la seqüència exacta de clics i tecleig, cosa que el fa útil amb programes antics sense cap altra forma d'integració.

Scripts: quan paga la pena escriure'n un

Sense necessitat de saber programar gaire, un script és un conjunt de passos escrits que un ordinador executa sols; resol tasques repetitives (renombrar centenars de fitxers, extreure dades d'un munt de documents) que a mà costarien hores i que fetes així triguen segons, sempre que els passos siguin exactament iguals cada vegada. La condició clau és aquesta darrera: un script és perfecte quan la tasca és mecànica i repetitiva de manera idèntica; en canvi, si cada cas requereix una petita decisió humana diferent, un script mal dissenyat pot fer més mal que bé, perquè aplicarà la mateixa regla cega a situacions que en realitat eren diferents.

APIs i webhooks: la comunicació entre serveis

La integració d'eines sovint passa per APIs (interfícies que permeten que un programa demani dades a un altre de manera estructurada) i per webhooks (notificacions automàtiques que un servei envia a un altre quan passa un esdeveniment). Entendre que existeixen, encara que no calgui programar-les, permet detectar quan un problema "d'aplicació" és en realitat un problema d'integració: si un formulari web deixa d'enviar dades a un CRM, sovint no és culpa de cap dels dos serveis sinó que ha caducat la clau d'accés (token) de la connexió que els uneix. Aquest cas enganya sovint, perquè tant el formulari com el CRM, provats per separat, funcionen amb normalitat: el problema és exactament al mig, en la connexió que els uneix.

Intel·ligència artificial en profunditat

Com genera text un model d'IA generativa

Un model d'IA generativa com els que hi ha darrere de ChatGPT, Gemini o Copilot no "sap" coses: ha après, a partir d'enormes quantitats de text durant un procés d'entrenament, a ajustar milions de paràmetres interns fins a predir quina és la paraula (o fragment, anomenat token) més probable que vingui després d'una altra, donat el context. Entrenar el model vol dir precisament això: ajustar aquests paràmetres interns perquè aprengui els patrons estadístics del llenguatge a partir de milions de textos, no memoritzar fets concrets un per un com faria una base de dades.

Per què al·lucina, i per què no és un simple error

Aquest funcionament estadístic explica per què pot generar text convincent i alhora fals: quan no té prou informació fiable, igualment produeix la resposta més probable segons el patró après, encara que no sigui certa. Això es coneix com a al·lucinació, i és inherent al disseny actual d'aquests sistemes, no un simple error puntual que es corregeix amb una actualització: el model, quan no té informació fiable sobre alguna cosa, igualment genera la resposta estadísticament més probable en lloc de dir simplement "no ho sé". Per això cal contrastar sempre les dades, dates, cites o xifres concretes que dona una IA generativa amb una font fiable, sobretot quan la resposta sona molt segura de si mateixa: la seguretat aparent del to no té cap relació amb la veracitat real del contingut.

Escriure bons prompts

Escriure bons prompts (les instruccions que es donen al model) marca una diferència real en la qualitat de la resposta: donar context suficient, indicar quin rol o to s'espera, aportar un exemple del resultat desitjat i especificar el format de sortida (una llista, una taula, un text breu) redueix moltíssim les respostes genèriques. Un prompt del tipus "escriu sobre atenció al client" donarà una resposta vaga; un prompt que digui "actua com un responsable d'atenció ciutadana d'un ajuntament petit, redacta en to formal però proper una resposta a una queixa sobre el retard d'una llicència d'obres, en cent paraules" donarà un resultat molt més aprofitable.

Els límits del sistema: la data de tall

Cal tenir presents els límits del sistema més enllà de les al·lucinacions: tot model té una data de tall en el seu entrenament, a partir de la qual no sap res del que ha passat, tret que estigui connectat a una cerca en temps real, i cal comprovar sempre si aquest és el cas abans de confiar en una resposta sobre fets recents. Preguntar a un model d'IA generativa qui ha guanyat unes eleccions recents, sense assegurar-se abans que té accés a cerca en temps real, és una manera segura de rebre una resposta inventada amb tota la confiança del món.

Biaixos algorísmics

Els biaixos algorísmics són un altre punt clau: si les dades amb què s'ha entrenat un model reflecteixen desigualtats socials existents (per exemple, currículums històrics on predominen homes en càrrecs directius), el model tendirà a reproduir-les en les seves respostes, encara que ningú ho hagi programat expressament. Un sistema de selecció de personal automatitzat entrenat amb dades esbiaixades pot discriminar sense cap intenció explícita: ningú ha escrit una regla que digui "prioritza els homes", però si les dades històriques mostren majoritàriament homes en càrrecs directius, el model aprendrà aquest patró com si fos una correlació vàlida i el reproduirà.

Privadesa i RGPD en l'ús professional de la IA

La privadesa és una preocupació pràctica i no teòrica: escriure dades personals, mèdiques o d'una empresa en un xat d'IA generativa pot significar que aquesta informació s'utilitzi per entrenar futures versions del model, segons la política de cada servei. El RGPD exigeix minimitzar les dades que es comparteixen i comprovar si l'eina permet desactivar l'ús de les converses per a entrenament: no enganxar mai dades de salut d'un pacient, dades fiscals d'un client o informació confidencial d'una empresa en un xat d'IA gratuït sense haver comprovat abans la seva política de privadesa.

Deepfakes: com sospitar-ne

La mateixa lògica generativa que produeix text serveix per generar imatges, veus i vídeos sintètics: els deepfakes (imatges, vídeos o veus que suplanten una persona real) han passat de ser una curiositat tècnica a un risc real de frau i desinformació. Detectar-los del tot és cada vegada més difícil a ull nu, però hi ha senyals: il·luminació inconsistent, parpelleig poc natural, moviments de la boca no del tot sincronitzats amb l'àudio, o context sospitós (una notícia extraordinària sense cap altra font que la confirmi). Cap d'aquests senyals és definitiu per si sol, però la combinació de diversos, sumada al sentit crític davant d'un contingut dissenyat per provocar una reacció immediata (indignació, por, urgència de compartir), és el millor filtre disponible avui dia.

Ús ètic professional i el Reglament europeu d'IA

L'ús professional i ètic d'aquestes eines implica ser transparent quan es fa servir contingut generat (indicar-ho), verificar la font original i no delegar-hi decisions que requereixen criteri humà (una avaluació

mèdica, una selecció de personal, una sentència judicial). Ser transparent sobre l'ús de contingut generat per IA és rellevant, en termes ètics, perquè afecta la confiança de qui el rep: permet que la persona destinatària valori la fiabilitat del contingut sabent com s'ha produït, en lloc de donar per fet, sense saber-ho, que és obra íntegrament humana.

La Unió Europea ha respost a aquests riscos amb el Reglament d'IA (AI Act), que classifica els sistemes segons el nivell de risc: des de pràctiques d'un risc inacceptable i directament prohibides, fins a sistemes d'alt risc (com els que decideixen sobre crèdits, feina o justícia) sotmesos a obligacions estrictes de transparència, passant per sistemes de risc limitat o mínim amb requisits més lleugers. Com més capacitat té un sistema d'IA d'afectar drets fonamentals de les persones, més exigent és la regulació que se li aplica: un sistema que decideix si una persona rep un crèdit hipotecari, o si és contractada per a una feina, cau dins la categoria d'alt risc precisament perquè les conseqüències d'un error o d'un biaix hi són molt més greus.

Aprendre a aprendre, i ensenyar-ho

El marc DigComp: la competència digital no s'acaba mai

La tecnologia canvia més ràpid que qualsevol temari, i el marc DigComp en què es basa l'ACTIC ho assumeix explícitament: la competència digital no és un estat que s'assoleix i ja està, sinó un procés continu que requereix autoavaluació i actualització constant. Aquesta idea, aparentment abstracta, té una conseqüència molt concreta per a qui es prepara aquest certificat: aprovar l'examen no és el punt final d'aprendre, sinó una fotografia d'un moment concret d'un procés que continua després.

Triar bé les fonts per mantenir-se al dia

Mantenir-se al dia vol dir triar bé les fonts: documentació oficial dels fabricants, mitjans especialitzats amb criteri editorial, comunitats de pràctica, i desconfiar del soroll de xarxes socials que sovint amplifica rumors abans que fets contrastats. Quan un problema tècnic sembla nou o estrany, val més començar per la documentació oficial del fabricant o per un fòrum de comunitat de pràctica reconegut, que no pas per la primera resposta que apareix en una xarxa social sense cap contrast.

Aprendre fent projectes reals

La manera més sòlida d'aprendre segueix sent fent projectes reals, encara que siguin petits: muntar una xarxa domèstica des de zero, automatitzar una tasca repetitiva del propi dia a dia, provar una màquina virtual per curiositat. No cal esperar a tenir un problema real a la feina: crear un filtre de correu propi, accedir al router de casa, o muntar una petita automatització amb un formulari consolida molt més que llegir-ho.

Ensenyar per consolidar: la pregunta clau

I la manera més sòlida de consolidar el que s'ha après és ensenyar-ho a algú altre: explicar un problema tècnic i la seva solució obliga a ordenar les idees i deixa clar de seguida on hi ha llacunes que semblaven cobertes. Una manera senzilla de fer-ho és preguntar-se, davant de cada problema resolt: podria explicar a algú altre exactament què ha fallat i per què la solució ha funcionat? Si la resposta és no, encara no s'ha entès el problema, només s'ha "apedaçat". Aquesta pregunta és, de fet, una bona manera d'autoavaluar-se abans de l'examen mateix: per a cada tema d'aquest capítol, val la pena provar d'explicar-lo en veu alta a algú, sense mirar els apunts, i veure on es queda encallat el discurs.

Construir-se un pla personal de competències

Aquesta lògica també val per planificar la pròpia formació a mig termini. L'ACTIC és un bon punt de partida, però no un punt final: existeixen itineraris i certificacions més especialitzades (en ciberseguretat, en anàlisi de dades, en eines concretes) per a qui vulgui aprofundir. Autoavaluar-se vol dir revisar periòdicament quines eines fem servir i per què, identificar què hem après "per costum" i què entenem de veritat, i construir-se un pla personal de competències: quines llacunes concretes cal tapar aquest any, amb quins recursos, i com se sabrà que s'han tapat de debò.