CRITERIS D'AVALUACIÓ

NIVELL	**ESO4**
MATÈRIA	**Digitalització**
CURS	**26-27**

S.A.	Criteris d'avaluació
SA 1 Operació PC Rescat	1. Identificar els components interns i externs d'un ordinador i explicar la funció de cadascun dins el conjunt del sistema. [1.3] 2. Diagnosticar l'estat d'un equip aplicant un protocol de comprovació ordenat i registrar-ne els resultats a l'expedient tècnic. [1.3] 3. Configurar les opcions del sistema operatiu (comptes d'usuari, emmagatzematge, actualitzacions i aplicacions d'inici) en funció d'unes necessitats d'ús concretes. [1.2] 4. Resoldre una incidència tècnica senzilla, documentar el procediment seguit i verificar que la solució aplicada funciona. [1.3] 5. Reformular el procediment quan la primera actuació no resol la incidència, justificant el canvi de plantejament. [1.3] 6. Proposar una actuació de reutilització o d'actualització d'un equip valorant-ne el cost, la vida útil i l'impacte ambiental. [1.4] 7. Aplicar mesures d'estalvi i d'eficiència energètica en la configuració d'un equip i estimar-ne l'efecte. [1.4] 8. Organitzar l'entorn de treball de la matèria —estructura de carpetes, espai al núvol, permisos de compartició i portafolis— i mantenir-lo actualitzat de manera autònoma durant tot el curs. [2.5]
SA 2 Xarxa sota control	1. Distingir els elements d'una xarxa local (encaminador, commutador, punt d'accés, cablatge i dispositius finals) i explicar la funció de cadascun. [1.1] 2. Representar l'esquema d'una xarxa local indicant-ne la topologia, l'adreçament i els dispositius connectats. [1.1] 3. Connectar dispositius amb fil i sense fil i comprovar la connectivitat amb les eines de diagnosi del sistema operatiu. [1.1] 4. Configurar l'adreçament IP d'una xarxa local i justificar el rang i la màscara escollits. [1.1] 5. Diagnosticar una fallada de connectivitat seguint un procés ordenat de descart i documentar-ne la resolució. [1.3] 6. Aplicar mesures de seguretat a la xarxa: xifratge, canvi de les credencials per defecte, xarxa de convidats i actualització del microprogramari. [3.2] 7. Justificar amb arguments tècnics per què una configuració de xarxa concreta és més segura que una altra. [3.2]
SA 4 Dades amb superpoders	1. Localitzar un conjunt de dades obertes pertinent per a una pregunta plantejada i valorar-ne l'origen, la data i les limitacions. [2.1] 2. Netejar i preparar un conjunt de dades en un full de càlcul: tipus de dada, valors buits, duplicats i format. [2.3] 3. Calcular els indicadors necessaris amb les fórmules i funcions adequades del full de càlcul. [2.3] 4. Representar les dades amb el tipus de gràfic adequat a la informació que es vol comunicar i justificar-ne la tria. [2.3] 5. Identificar una representació gràfica enganyosa i explicar quin recurs concret la fa enganyosa. [2.3] 6. Produir una peça multimèdia que integri imatge, so i vídeo per comunicar la conclusió obtinguda de les dades. [2.3]

	7. Citar l'origen de les dades i del material reutilitzat i aplicar-hi les llicències d'ús corresponents. [4.1] Adaptar el missatge a l'audiència prevista i publicar-lo de manera responsable a l'espai compartit de la matèria. [4.4]
SA 5 Detectius digitals	1. Aplicar tècniques de cerca avançada per localitzar l'origen d'una informació. [4.3] 2. Verificar una informació dubtosa contrastant-la amb un mínim de dues fonts independents i documentar el procés seguit. [4.3] 3. Analitzar un missatge digital identificant-ne l'autoria, la intencionalitat, els biaixos, l'objectivitat i la caducitat. [4.3] 4. Distingir entre informació, opinió i publicitat en continguts digitals, i argumentar la distinció. [4.3] 5. Identificar els indicadors d'un frau en línia i descriure com cal actuar-hi davant. [4.2] 6. Descriure el procediment d'una gestió administrativa digital i els requisits d'identificació que demana. [4.2] 7. Reconèixer pràctiques segures en el comerç electrònic i justificar per què ho són. [4.2] 8. Argumentar com la bretxa digital afecta col·lectius concrets i proposar una mesura per reduir-la. [4.2]
SA 6 Mode Ciberescut	1. Auditar la configuració de privadesa dels comptes i espais virtuals d'ús habitual i corregir-ne els punts febles detectats. [3.1] 2. Explicar què és la petjada digital i quines accions la generen, i aplicar mesures per gestionar-la. [3.1] 3. Avaluar la robustesa de les contrasenyes i aplicar una estratègia segura de gestió de credencials, inclosa la verificació en dos passos. [3.2] 4. Configurar les mesures de protecció d'un dispositiu: bloqueig de pantalla, actualitzacions, antivirus, còpies de seguretat i permisos de les aplicacions. [3.2] 5. Identificar els indicadors d'un intent de suplantació d'identitat, d'una infecció o d'un accés no autoritzat. [3.3] 6. Redactar un pla de resposta davant d'un incident de seguretat amb els passos ordenats i els contactes de referència. [3.3] 7. Identificar situacions de risc per a la salut física i mental associades a l'ús de les tecnologies digitals i proposar mesures de prevenció. [3.4] 8. Reconèixer una situació de ciberassetjament i descriure les vies d'ajuda i de denúncia disponibles. [3.4]
SA 7 Codi en acció	1. Analitzar un problema real i redactar-ne les especificacions funcionals abans de començar a programar. [2.2] 2. Descompondre el problema en parts i representar la solució amb un algorisme abans d'escriure el codi. [2.2] 3. Programar l'aplicació o la pàgina web utilitzant variables, estructures condicionals i estructures repetitives. [2.4] 4. Identificar, localitzar i corregir els errors del codi amb les eines de depuració, i explicar la causa de cada error. [2.4] 5. Dissenyar una interfície comprensible i aplicar-hi els criteris bàsics d'accessibilitat. [2.4] 6. Dissenyar i executar un pla de proves amb casos concrets, registrant el resultat esperat i el resultat obtingut. [2.4] 7. Documentar l'aplicació de manera que una altra persona la pugui entendre, utilitzar i modificar. [2.4]

	8. Reutilitzar codi o recursos de tercers respectant-ne l'autoria i la llicència, i declarar-ho a la documentació. **[4.1]** 9. Integrar el producte i la seva documentació al portafolis personal, amb control de versions i permisos de compartició adequats. **[2.5]** 10. Millorar el producte a partir del retorn rebut i justificar els canvis introduïts. **[2.2]**
SA 8 Futur en beta	1. Descriure el funcionament bàsic d'una tecnologia emergent (intel·ligència artificial, IoT, realitat virtual o augmentada) amb vocabulari tècnic precís. **[5.3]** 2. Identificar canvis econòmics i socials concrets derivats de la digitalització en un àmbit determinat. **[5.1]** 3. Analitzar l'impacte d'una tecnologia digital sobre la societat relacionant-lo amb els ODS 10, 11 i 12. **[5.2]** 4. Valorar els efectes d'una tecnologia sobre el món laboral, el medi ambient i l'equitat, amb dades contrastades. **[5.2]** 5. Reconèixer biaixos algorítmics en un cas concret i explicar-ne l'origen i les conseqüències. **[5.2]** 6. Explicar per a què serveixen les eines de simulació i la supercomputació en el tractament de dades i quin impacte tenen. **[5.4]** 7. Dissenyar una proposta de solució a un problema real aplicant una tecnologia emergent i justificar-ne la tria. **[5.3]** 8. Avaluar la viabilitat, els riscos ètics i la sostenibilitat de la proposta dissenyada. **[5.3]** 9. Aplicar el pensament de disseny al llarg del procés i documentar les iteracions fetes. **[2.2]**