Aquest examen consta de 40 qüestions d'opció múltiple. En totes les qüestions hi ha una única opció correcta. Les respostes han de proporcionar-se en la fulla de respostes que s'ha proporcionat separada d'aquest enunciat.

Totes les qüestions tenen el mateix valor. Les que estiguen correctament contestades aportaran 0.25 punts a la nota d'aquest parcial. Les incorrectes descomptaran 0.05 punts. En cas de dubte, es recomana deixar-les en blanc.

Disposa de dues hores per a completar l'examen.

1. L'acoblament en una aplicació distribuïda:

A	Ha de ser alt ja que així es redueix la necessitat de comunicació i les aplicacions ofereixen millor rendiment. FALS. L'acoblament mesura les necessitats de comunicació entre mòduls, examinant el nombre d'arguments necessaris en cada interacció així com els tipus i àmbit d'aquests arguments. Es recomana que l'acoblament siga el més baix possible.
B	No existeix. En una aplicació distribuïda només hi ha cohesió, mai hi haurà acoblament. FALS. En poder distingir múltiples components en qualsevol aplicació distribuïda, l'acoblament estarà referit a les necessitats de comunicació entre els mòduls o components. Si que té sentit parlar d'acoblament en aquests entorns.
C	Ha de ser el més baix possible. Així només es transmetrà la informació estrictament necessària en cada interacció. CERT. Ja s'ha explicat per què en els dos apartats anteriors.
D	Està sempre lligat a la cohesió. Com més baix siga l'acoblament més baixa serà la cohesió. FALS. Generalment es necessita una cohesió alta per a obtenir un acoblament feble.
E	Totes les anteriors. L'única opció correcta és la C.
F	Cap de les anteriors. L'única opció correcta és la C.

2. La cohesió en qualsevol aplicació distribuïda:

A	Està lligada a l'acoblament. Com més baixa siga la cohesió, més baix serà l'acoblament. FALS. Generalment es necessita una cohesió alta per a obtenir un acoblament feble.
B	Convé que siga el més alta possible. Així serà fàcil reutilitzar els mòduls desenvolupats. CERT. Quan la cohesió és alta, cada mòdul d'una aplicació realitza una única funció i està destinat en exclusiva a això. Si posteriorment es necessitara la mateixa funcionalitat en altres aplicacions i el disseny del mòdul va ser acurat, resultarà fàcil reutilitzar-lo.
C	Convé que siga el més baixa possible. Així es redueix la necessitat de comunicació entre nodes. FALS. Amb una cohesió baixa s'hauran desenvolupat múltiples mòduls en una aplicació que faran múltiples funcions cadascun. Això reflecteix un mal disseny. Si el disseny va ser de baixa qualitat res garantirà que s'haja cercat reduir les necessitats de comunicació entre mòduls. A més, allò que podrà reduir les necessitats de comunicació és l'acoblament baix. La cohesió guarda relació amb la funcionalitat de cada mòdul, no amb les seues necessitats de comunicació.
D	Convé que siga el més alta possible. Així millora la robustesa de l'aplicació. FALS. La robustesa (fiabilitat, disponibilitat, mantenibilitat i seguretat) és una col·lecció d'atributs no funcionals de les aplicacions i no guarda relació directa amb el grau de cohesió d'una aplicació, que sí depèn de la funcionalitat de cada mòdul.
E	Totes les anteriors.
F	Cap de les anteriors.

3. La persistència en una aplicació distribuïda…:

A	No és recomanable ja que redueix el rendiment i impedeix que les aplicacions siguen escalables. FALS. En qualsevol aplicació distribuïda es pot necessitar que algunes dades es mantinguen de manera persistent. Si es modifiquen amb baixa freqüència o es fa un repartiment adequat d'elles a l'hora de gestionar-les no es limitarà fortament el rendiment de les aplicacions. Per exemple, MongoDB és un exemple de magatzem escalable de dades persistents.
B	Permet superar algunes situacions de fallada sense que es perda per complet l'estat. CERT. Les dades emmagatzemades de manera persistent superen diversos tipus de fallades en els ordinadors que les gestionen (de fet, totes aquelles fallades que no impliquen una destrucció del mitjà físic on residisquen). Aquestes dades poden utilitzar-se localment tan aviat com el node es recupere. En molts casos això permetrà reprendre el servei sense requerir la col·laboració d'altres nodes o minimitzant la quantitat d'informació a transferir per a completar la reconfiguració, agilitant la seua recuperació.
C	Condueix a una alta cohesió. FALS. La persistència no guarda relació amb la cohesió.
D	Redueix l'acoblament. FALS. La persistència no guarda relació amb l'acoblament.
E	Totes les anteriors.
F	Cap de les anteriors.

4. Les bases de dades relacionals:

A	Suporten transaccions amb garanties ACID. CERT. Les garanties d'atomicitat, consistència, aïllament i durabilitat són proporcionades per les transaccions utilitzades en els sistemes gestors de bases de dades relacionals.
B	Proporcionen persistència. CERT. La persistència resulta necessària per a garantir la durabilitat de les escriptures efectuades en cada transacció.
C	Limiten l'escalabilitat, ja que condueixen a bloquejos freqüents si hi ha un elevat grau de concurrència. CERT. El control de concurrència automatitzat que s'utilitza en els sistemes gestors de bases de dades relacionals pot provocar bloquejos apreciables quan el grau de concurrència siga alt. És el preu a pagar per a obtenir un aïllament fort ("serialitzable") entre les transaccions.
D	Minimitzen la duplicació de dades en les seues taules. Per a fer això utilitzen tècniques de normalització. CERT. L'objectiu de la normalització és reduir la quantitat de vegades que es manté un camp d'una entitat determinada en les relacions (taules) d'una base de dades.
E	Totes les anteriors.
F	Cap de les anteriors.

5. Les garanties ACID de les transaccions són ...

A	Aïllament, concurrència, internacionalització i durabilitat.
B	Aïllament, concurrència, indexació i disponibilitat.
C	Atomicitat, concurrència, aïllament i disponibilitat.
D	Fiabilitat, seguretat, mantenibilitat i disponibilitat.
E	Totes les anteriors.
F	Cap de les anteriors. Les garanties ACID de les transaccions són: atomicitat, consistència semàntica, aïllament i durabilitat. Cap dels apartats anteriors citava les quatre garanties correctes.

6. Per a millorar l'escalabilitat d'un magatzem de dades persistent mitjançant una base NoSQL:

A	S'utilitza una base de dades relacional. FALS. Les bases de dades relacionals utilitzen SQL com el seu llenguatge d'interrogació. Per tant, no formarien part de la família de "bases NoSQL".
B	Es renuncia a l'ús de transaccions amb garanties ACID. CERT. Com ja hem vist en qüestions anteriors la persistència no sempre limitarà l'escalabilitat. Per tant, què la limita en una base de dades tradicional? Principalment els seus mecanismes de control de concurrència. Aquests mecanismes resulten necessaris per a garantir l'aïllament entre transaccions concurrents. Per tant, si eliminem les transaccions tradicionals el sistema resultant podrà ser més escalable que un sistema gestor relacional.
C	No s'utilitza "*sharding*". FALS. El "sharding" és un dels mecanismes clau per a millorar l'escalabilitat d'un magatzem de dades persistent.
D	S'utilitzen llenguatges d'interrogació complexos, permetent múltiples "joins". FALS. L'ús de "joins" en el llenguatge d'interrogació complicaria excessivament el repartiment de les dades entre múltiples nodes (és a dir, el "sharding"). Sense repartiment de dades, l'escalabilitat estarà limitada. A més, la gestió d'un "join" implicarà que s'accedisca a múltiples taules o col·leccions i que es creuen les dades de diverses d'elles. Això ralentiria excessivament el servei d'aquest tipus de sentències, limitant també així l'escalabilitat.
E	Totes les anteriors.
F	Cap de les anteriors.

7. MongoDB:

A	És una base de dades relacional que utilitza "*sharding*" per a millorar la seua escalabilitat. FALS. MongoDB utilitza "sharding" per a millorar la seua escalabilitat però no és una base de dades relacional sinó un magatzem de documents escalable.
B	És un magatzem de dades clau-valor. FALS. MongoDB no pertany a aquesta classe de magatzems de dades escalables.
C	És un magatzem de documents. CERT. Aquesta és la classe de magatzem a la qual pertany.
D	És un magatzem de registres extensibles. FALS. MongoDB no pertany a aquesta classe de magatzems de dades escalables.
E	Totes les anteriors.
F	Cap de les anteriors.

8. El teorema CAP estableix...:

A	Que cap sistema distribuït pot ser robust.
B	Que un sistema no pot ser alhora fiable, segur i altament disponible.
C	Que tots els sistemes distribuïts són escalables.
D	Que cap sistema distribuït robust admet situacions de particionat de la xarxa.
E	Totes les anteriors.
F	Cap de les anteriors. El teorema CAP estableix que en qualsevol sistema distribuït no es podran garantir simultàniament tres propietats: consistència forta, disponibilitat de servei i tolerància a les situacions de particionat de la xarxa. Cap dels apartats anteriors deia això. Potser l'apartat que haja pogut provocar més dubtes siga el D. Un sistema distribuït robust serà simultàniament fiable, disponible, mantenible (invertirà poc temps en la seua recuperació) i segur. La robustesa no exigeix res quant a la consistència mínima que hauran de respectar les rèpliques d'un determinat servei. Per definició, un sistema robust és altament disponible. Podrà tolerar les situacions de particionat de la xarxa relaxant temporalment la consistència entre les diferents rèpliques de cada component. Amb això l'afirmació de l'apartat D seria falsa.

9. Segons el teorema CAP...

A	Un servei altament disponible no podrà mantenir una consistència forta quan la xarxa es particione i diverses de les seues rèpliques queden desconnectades. CERT. Mantenim la disponibilitat (A) i la tolerància a situacions de particionat (P) sacrificant la consistència (C).
B	Quan la xarxa es particione els serveis del sistema seguiran estant disponibles i mantindran una consistència seqüencial. FALS. Com la consistència seqüencial és un model de consistència fort s'estarien mantenint les tres propietats (C, A i P). El teorema CAP implica que almenys una d'elles no hi haurà manera de garantir-la.
C	La xarxa no podrà particionar-se mai en un servei escalable. FALS. Per a garantir la disponibilitat associada a un servei escalable se sol preferir sacrificar la consistència i admetre les situacions de particionat.
D	La disponibilitat d'un servei es perdrà quan aquest haja d'actualitzar-se. FALS. Que es perda la disponibilitat d'un servei quan aquest s'actualitze no té res a veure amb el teorema CAP.
E	Totes les anteriors.
F	Cap de les anteriors.

10. En un magatzem de documents…

A	L'esquema de la base de dades és fix i està format per un conjunt determinat de taules. FALS. Això ocorre en un sistema relacional, però no en un magatzem de documents escalable.
B	L'esquema de la base de dades és dinàmic i està compost per una sèrie de col·leccions capaces d'albergar cadascuna qualsevol classe de document/objecte. CERT. Ho hem pogut comprovar en utilitzar MongoDB.
C	S'utilitza SQL com a llenguatge d'interrogació. FALS. Això ocorre en els sistemes relacionals.
D	Les transaccions engloben múltiples sentències i les sentències admeten "joins" entre taules o col·leccions. FALS. Això ocorre en els sistemes relacionals.
E	Totes les anteriors.
F	Cap de les anteriors.

11. La seguretat…

A	És un atribut dels sistemes distribuïts robusts. CERT. Al costat de la fiabilitat, disponibilitat i mantenibilitat.
B	És una propietat derivada del teorema CAP. FALS. El teorema CAP relaciona altres tres propietats (consistència, disponibilitat, tolerància a les situacions de particionat de la xarxa) però no diu res sobre la seguretat.
C	És una propietat que compleix tot servei distribuït altament disponible. FALS. La disponibilitat no implica seguretat. Si ho fera, no s'haurien citat ambdues explícitament en definir la robustesa.
D	És una de les garanties de les transaccions ACID. FALS. ACID acull atomicitat, consistència semàntica, aïllament i durabilitat, però no cita per a res la seguretat.
E	Totes les anteriors.
F	Cap de les anteriors.

12. Objectius principals de la seguretat:

A	Consistència, disponibilitat i tolerància a les particions de la xarxa. FALS. Aquestes són les tres propietats considerades en el teorema CAP però no guarden relació directa amb els objectius principals de la seguretat.
B	Disponibilitat, fiabilitat i mantenibilitat. FALS. Aquests són els tres altres atributs de la robustesa ("dependability"), però no poden considerar-se objectius de la seguretat.
C	Recuperació, alta cohesió i baix acoblament. FALS. Són característiques aconsellables en qualsevol sistema, però no objectius de la seguretat.
D	Confidencialitat, integritat, disponibilitat i comptabilitat. CERT. Així se citava en el tema 7.
E	Totes les anteriors.
F	Cap de les anteriors.

13. Els tres elements que intervenen en una política de seguretat són:

A	Estratègies, mecanismes i garanties. FALS. En qualsevol sistema de seguretat hi haurà estratègies, mecanismes, polítiques i garanties. Aquests tres últims elements es consideren "eines de seguretat". Per tant, els elements citats en aquest apartat no intervenen en una política sinó que són "elements" que estan al seu mateix "nivell".
B	Agents, objectes i accions. CERT. L'agent és l'element que podrà realitzar les accions d'una política. L'objecte és l'element sobre el qual podrà actuar l'agent. Finalment, l'acció és l'operació que podrà dur a terme l'agent sobre l'objecte. Com a resultat, una política és una especificació precisa que indica per a cada agent quines accions podrà fer sobre cada objecte. Per tant, aquests són els tres elements que intervenen en la política.
C	Vulnerabilitats, amenaces i atacs. FALS. Aquests són els tres tipus de riscos que s'han identificat en analitzar la seguretat. Són tipus de risc, no elements d'una política.
D	Disponibilitat, consistència i confidencialitat. FALS. Tant la disponibilitat d'accés com la confidencialitat són objectius generals de la seguretat. La consistència és una propietat que ha de cercar-se en els sistemes en els quals es repliquen serveis o informació. Cap dels tres és un element que intervinga en una política de seguretat.
E	Totes les anteriors.
F	Cap de les anteriors.

14. El control d'accés:

A	És un mecanisme de seguretat. CERT. Al costat dels mecanismes físics i els mecanismes d'autenticació, és una de les tres classes de mecanismes de seguretat citats en el tema 7.
B	En cas de ser discrecional pot implantar-se mitjançant llistes de control d'accés o mitjançant capacitats. CERT. Per a representar un control d'accés se sol utilitzar una matriu d'accés en la qual les files representaran els agents i les columnes els objectes. Cada component de la matriu contindrà les accions (o drets) admeses per a aqueixa combinació d'agent i objecte. Com les matrius solen ser disperses (és a dir, tenen un alt nombre de components buides) s'implanten per columnes o per files, utilitzant solament les components no buides. En implantar-se per columnes es genera una llista de control d'accés associada a cada columna/objecte. Això és el que ocorre en els sistemes de fitxers. Les paraules de protecció utilitzades en els sistemes UNIX són una versió compacta d'aquestes llistes. En els sistemes Windows actuals també s'utilitzen aquests tipus de llista. Cada fitxer manté la seua. Si s'implanta per files, cada agent mantindrà la llista d'operacions que podrà efectuar sobre cada objecte. Cadascuna d'aquestes "llistes" és una "capacitat".
C	No és un mecanisme físic. CERT. És un mecanisme de seguretat, però no d'aquesta classe.
D	Pot utilitzar-se per a implantar parcialment diferents polítiques de seguretat. CERT. La política especifica què fer però no com s'implantarà. La implantació recau en els mecanismes.
E	Totes les anteriors.
F	Cap de les anteriors.

15. En considerar els riscos…

A	Si no hi ha vulnerabilitats no podrà haver-hi atacs. CERT. Un atac comprèn el conjunt d'accions desenvolupades durant una amenaça. Per la seua banda, una amenaça implica l'aprofitament d'alguna vulnerabilitat.
B	Perquè no hi haja amenaces bastarà amb eliminar tots els usuaris del sistema. FALS. Perquè no hi haja amenaces s'haurà de garantir que no hi haja cap vulnerabilitat. No totes les vulnerabilitats depenen dels usuaris que puga tenir un sistema.
C	Una amenaça és la implantació d'un atac. FALS. Un atac és la "implantació" d'una amenaça.
D	Es dóna una vulnerabilitat quan un usuari malintencionat s'aprofita d'una amenaça. FALS. Es dóna una amenaça quan un usuari malintencionat s'aprofita d'una vulnerabilitat. Els termes clau d'aquesta afirmació estaven intercanviats.
E	Totes les anteriors.
F	Cap de les anteriors. Encara que l'apartat A s'ha de considerar cert, també és veritat que hi ha atacs "cecs" en els quals sense haver explorat prèviament si el sistema objectiu tenia alguna vulnerabilitat s'inicia d'igual manera un atac. D'altra banda, va a resultar impossible construir un sistema perfecte on no hi haja cap vulnerabilitat. PER TOT EL QUE S'HA DIT, EN AQUESTA QÜESTIÓ ES CONSIDERARAN CORRECTES TANT L'OPCIÓ "A" COM LA "F".

16. Sobre els tipus d'amenaces en sistemes distribuïts:

A	Són internes quan l'agent que les genera té accés físic a un ordinador del sistema. CERT. Aquesta és la característica que definia una amenaça interna.
B	Són internes quan l'agent que les genere és capaç de corrompre la TCB del sistema, modificant per a això els protocols de comunicació. FALS. Les amenaces internes guarden relació amb l'ordinador utilitzat per a generar l'amenaça (ha de formar part del sistema i es necessita accés físic a ell), però no la guarden amb l'objecte afectat per l'amenaça (fitxers, informació, recursos...)
C	Són externes quan l'agent que les provoque no és tècnicament expert. FALS. Aquestes serien les amenaces estructurades.
D	Són externes quan l'agent que les provoque sap com corrompre les comunicacions entre els agents amb accés físic al sistema. FALS. No és una definició vàlida per a les amenaces externes. Tant les internes com les externes depenen exclussivament de si es té accés físic (interna) o no (externa) a un dels ordenadors del sistema.
E	Totes les anteriors.
F	Cap de les anteriors.

17. Definicions correctes de tipus d'atac en sistemes distribuïts:

A	Denegació de servei: Obtenció d'accés sobre un servei violant una política activa. FALS. La definició correcta seria "inhabilitació de serveis per als usuaris que estan autoritzats per a utilitzar-los".
B	Accés: Descobriment desautoritzat de serveis i vulnerabilitats. FALS. La definició utilitzada va ser "obtenció d'accés sobre un servei o objecte, violant certa política".
C	Recol·lecció: Descobriment desautoritzat de serveis i vulnerabilitats, utilitzat posteriorment per a atacs d'accés o denegació de servei. CERT. Aquesta va ser la definició donada en el tema 7.
D	Denegació de servei: Inhabilitació de serveis per a usuaris desautoritzats. FALS. Els usuaris que no estiguen autoritzats mai haurien d'accedir a un servei. En la justificació de l'apartat A ja s'ha donat la definició correcta.
E	Totes les anteriors.
F	Cap de les anteriors.

18. Exemples d'atacs de "Recol·lecció d'informació":

A	"Ping of death". FALS. És un atac de tipus "denegació de servei".
B	Congestió SYN. FALS. És un atac de tipus "denegació de servei".
C	Corrupció de paquets. FALS. És un atac de "accés" ja que implica l'accés a la informació i la corrupció d'aquesta mentre és transmesa.
D	Denegació de servei. FALS. És el nom d'un altre dels tipus d'atac.
E	Totes les anteriors.
F	Cap de les anteriors.

19. Sobre els atacs "*man in the middle*":

A	És un exemple d'atac d'accés. CERT. Permet accedir a la informació transmesa d'una forma no autoritzada i prendre aquest fet com a base per a realitzar altres accions posteriorment.
B	S'utilitza per a suplantar a un agent autoritzat. CERT. Pot utilitzar-se per a aquesta fi.
C	Es pot implantar interceptant sessions en curs. CERT. Es pot implantar d'aquesta manera.
D	Permet corrompre l'estat del sistema, inserir nova informació o denegar el servei a alguns agents autoritzats. CERT. Són tres possibles conseqüències d'aquests atacs.
E	Totes les anteriors.
F	Cap de les anteriors.

20. Sobre els protocols criptogràfics:

QÜESTIÓ INVALIDADA. En les versions en castellà i valencià es va barrejar en maquetar la versió definitiva els apartats i enunciat de dues qüestions diferentes. L'enunciat d'aquesta qüestió hauria d'haver sigut "Sobre els codis MAC:". En aqueix cas la resposta correcta era la "C". Amb la combinació utilitzada, la veracitat o falsedat de cada apartat dependrà del protocol concret que s'assumisca en contestar pel que hi hauria més d'un apartat acceptable.

A	Verifiquen la integritat dels missatges.
B	Asseguren la confidencialitat de la comunicació.
C	Garanteixen el no repudi.
D	Permeten estalviar ample de banda, doncs el missatge sempre es transmet comprimit.
E	Totes les anteriors.
F	Cap de les anteriors.

21. El desplegament d'un servei distribuït consisteix a…

A	Instal·lar i configurar el programari en el sistema, resoldre les seues dependències i mantenir-ho en funcionament. CERT. Aquestes són les tasques principals a desenvolupar en el desplegament.
B	Garantir la seguretat del servei. FALS. Encara que la seguretat sempre és un aspecte a considerar en qualsevol etapa del cicle de vida del programari, no és tot el que va a fer-se en el desplegament.
C	Dissenyar i desenvolupar tots els seus components considerant la seua eficiència. FALS. Tant el disseny com el desenvolupament dels components han de concloure abans d'iniciar el desplegament.
D	Monitoritzar l'ús del servei, comptabilitzar els seus costos i gestionar el seu cobrament als usuaris. FALS. El desplegament d'un servei no consisteix exclusivament en la comptabilització i gestió econòmica.
E	Totes les anteriors.
F	Cap de les anteriors.

22. El SLA és…

A	Un contracte entre el proveïdor d'una infraestructura i el desenvolupador d'aplicacions distribuïdes. FALS. El SLA no afecta exclusivament als proveïdors d'infraestructura. No sempre serà un contracte. Almenys, no pot catalogar-se així en totes les legislacions.
B	Un contracte entre el desenvolupador d'un servei i els seus usuaris en el qual es consideren els aspectes de seguretat. FALS. Els agents implicats en aquest acord no són el desenvolupador i els usuaris, sinó el proveïdor d'un servei i els seus usuaris.
C	Un acord entre el proveïdor d'un servei i els seus usuaris en el qual es consideren principalment dos aspectes: rendiment i disponibilitat. CERT. Aquesta seria una definició acceptable per a un SLA. Intervenen el proveïdor de serveis i els clients d'aquest proveïdor. Els clients són els usuaris del servei. Els aspectes comunament considerats en l'acord són la disponibilitat i el rendiment del servei.
D	Un compromís entre tres propietats d'un servei distribuït: consistència, disponibilitat i tolerància al particionat de la xarxa. FALS. Les tres propietats esmentades són les citades en el teorema CAP. Aquest teorema no proporciona (ni guarda relació amb) la definició dels acords establits en un SLA.
E	Totes les anteriors.
F	Cap de les anteriors.

23. Cada instància d'un component d'un servei distribuït…

A	Pot iniciar-se i detenir-se amb independència de les altres instàncies. CERT. Si l'inici i atur d'una instància depenguera de l'estat de les altres (obligant a parar o arrancar totes elles de manera simultània), poc es guanyaria en tenir múltiples instàncies. Hi haurà múltiples instàncies per a augmentar la capacitat de servei i incrementar la disponibilitat. Ha d'existir certa llibertat per a poder iniciar noves instàncies quan la càrrega suportada es vaja incrementant i per a parar-les quan la càrrega disminuïsca.
B	Pot considerar-se una rèplica del component. CERT. La justificació de l'apartat anterior així ho suggereix. Cada instància aporta capacitat de servei addicional. També incrementa la disponibilitat, tolerant-se la fallada d'algunes d'elles.
C	Hauria de desplegar-se de tal manera que la seua probabilitat de fallada siga independent de la probabilitat de les altres instàncies. CERT. Cada instància ha de situar-se en un node diferent i cada node haurà de dependre de diferents fonts possibles de fallada: haurien d'estar en centres de dades diferents (o almenys en "racks" diferents en cas de situar-se en un mateix centre), tenir diferents punts d'accés a la xarxa de comunicacions... Així, en cas que hi haja algun problema físic (tall d'alimentació elèctrica en el centre, inundacions, avaria en la xarxa...) només afectarà a una o unes poques instàncies. Les altres superaran la situació de fallada.
D	Se situa amb independència de la ubicació de les instàncies d'altres serveis. CERT. També és conseqüència del que s'ha dit en els apartats anteriors. Cal reduir les dependències sobre qualsevol altre element del sistema.
E	Totes les anteriors.
F	Cap de les anteriors.

24. En la gestió del cicle de vida d'un servei cal considerar...

A	Quants programadors participen en el desenvolupament dels components. FALS. Aquests detalls de l'etapa de desenvolupament no afecten a la gestió del cicle de vida del servei. Aquesta gestió afecta al SERVEI no als programes utilitzats en els servidors. Un servei podrà iniciar-se, parar-se, reprendre's, patir actualitzacions i variar el nombre d'instàncies que donen suport a cada component en funció de la càrrega que haja de suportar-se. Totes aquestes accions són les rellevants en el cicle de vida del servei.
B	Com actualitzar els components i quan i com caldrà afegir o eliminar rèpliques de cada component. CERT. Aquestes són algunes de les accions a tenir en compte.
C	Els protocols d'enllaç i de xarxa utilitzats per a intercomunicar els components. FALS. Aquests protocols són responsabilitat del subsistema de comunicacions, en els seus nivells 2 i 3, respectivament. Normalment els serveis s'implantaran a nivell d'aplicació dins de l'arquitectura de nivells del sistema de comunicacions.
D	Si els components han sigut implantats sota un model multi-fil o un model de programació asincrónica. FALS. Generalment, això no afecta a les accions importants dins del cicle de vida del servei (enumerades en la justificació del primer apartat d'aquesta qüestió).
E	Totes les anteriors.
F	Cap de les anteriors.

25. Aspectes que han de decidir-se durant el desplegament d'un servei distribuït:

A	De quin altres serveis depèn i quins SLA es requereix de cadascun d'ells.
B	L'ordre d'inici dels components del servei.
C	Quantes instàncies tindrà cada component.
D	En quins nodes s'instal·larà i executarà cada instància.
E	Totes les anteriors. Tots els aspectes citats en els apartats anteriors han de ser considerats a l'hora de desplegar un servei, per senzill que aquest arribe a ser.
F	Cap de les anteriors.

26. Un descriptor de desplegament inclou…

A	Les garanties de seguretat del servei a desplegar. FALS. Les garanties de seguretat no solen especificar-se en el descriptor de desplegament.
B	El SLA oferit als futurs usuaris del servei a desplegar. FALS. El desplegament es realitzarà tenint en compte el SLA, però el SLA no està inclòs en el descriptor de desplegament.
C	La configuració de cadascuna de les instàncies a desplegar, el node on situar cadascuna i una descripció de les dependències internes i externes a resoldre. CERT. Aquest és el conjunt d'informació inclòs en el descriptor de desplegament.
D	El codi de cadascun dels components del servei. FALS. El descriptor conté la configuració de les diferents instàncies però generalment no inclou el codi de cada component.
E	Totes les anteriors.
F	Cap de les anteriors.

27. Els components d'un servei necessiten actualitzar-se per a…

A	Eliminar vulnerabilitats.
B	Millorar la seua eficiència.
C	Eliminar errors de programació.
D	Ampliar la seua funcionalitat i adaptar-se a noves configuracions.
E	Totes les anteriors. Tots els apartats anteriors són exemples vàlids de raons que condueixen a actualitzar un component.
F	Cap de les anteriors.

28. El desplegament en un sistema IaaS:

A	Està automatitzat. N'hi ha prou amb emplenar les plantilles de desplegament i el sistema s'encarrega de tot. FALS. Arribarà a automatitzar-se en els futurs sistemes PaaS, però no està automatitzat en cap sistema IaaS.
B	És responsabilitat del proveïdor d'infraestructura. FALS. Si fóra responsabilitat del proveïdor, els usuaris d'un sistema IaaS obtindrien la imatge que el desplegament està automatitzat per a ells. No és així.
C	És responsabilitat de l'administrador del sistema IaaS. FALS. En un sistema IaaS el rol d'administrador no està clarament delimitat. Algunes tasques d'administració les realitza el proveïdor i unes altres les realitza el client d'aquest tipus de serveis.
D	El proveïdor IaaS proporciona el nombre sol·licitat de màquines virtuals i el desenvolupador del servei s'encarrega del seu desplegament. CERT. En estar repartit d'aquesta manera resulta impossible automatitzar el desplegament d'un servei distribuït en un sistema IaaS.
E	Totes les anteriors.
F	Cap de les anteriors.

29. En un sistema PaaS, el desplegament se suposa que...

A	Està automatitzat. N'hi ha prou amb emplenar les plantilles de desplegament i el sistema s'encarrega de tot. CERT. Aquest és un dels seus principals avantatges enfront dels sistemes IaaS.
B	No és responsabilitat del PaaS. És responsabilitat del proveïdor SaaS. FALS. Sí que és responsabilitat del PaaS. És la diferència entre una plataforma i una infraestructura. La plataforma automatitza el desplegament.
C	No és responsabilitat del PaaS. És responsabilitat del IaaS subjacent. FALS. Sí que és responsabilitat del PaaS. És la diferència entre una plataforma i una infraestructura. La plataforma automatitza el desplegament.
D	El proveïdor PaaS proporciona el nombre sol·licitat de màquines virtuals i el desenvolupador del servei s'encarrega del seu desplegament. FALS. El proveïdor d'una plataforma no s'encarrega de la gestió de màquines virtuals. Això és responsabilitat del proveïdor de la infraestructura.
E	Totes les anteriors.
F	Cap de les anteriors.

30. Si s'automatitzara la gestió del cicle de vida d'un servei distribuït…

A	El servei s'adaptaria sense problemes als canvis en la càrrega suportada, consumint un volum òptim de recursos, reduint el seu cost.
B	El servei podria considerar-se elàstic.
C	Es garantiria (amb els límits del SLA acordat) la disponibilitat del servei.
D	S'oferiria un rendiment i funcionalitat concordes amb la seua SLA.
E	Totes les anteriors. Tot el que es comenta en els apartats anteriors és conseqüència de l'automatització en la gestió del cicle de vida d'un servei.
F	Cap de les anteriors.

31. Els patrons arquitectònics bàsics…

A	Descriuen quants components pot tenir un servei. FALS. Els components que haurà de tenir un servei es consideraran en el seu disseny. Un patró arquitectònic especifica de quina manera interactuaran dos components.
B	Proporcionen una guia completa per a decidir quantes instàncies de cada component caldrà desplegar. FALS. El nombre d'instàncies que hauran de desplegar-se dependrà de la càrrega suportada a cada moment i de la qualitat de servei compromesa en el SLA. Això no afecta a un patró arquitectònic.
C	Descriuen els patrons bàsics de comunicació. CERT. Aquest és l'objectiu d'un patró arquitectònic.
D	Proporcionen el SLA més senzill possible per a cada servei. FALS. Un patró arquitectònic no contempla els acords que puguen establir el proveïdor i el client d'un servei.
E	Totes les anteriors.
F	Cap de les anteriors.

32. El patró petició/resposta...

A	Intercomunica a dos agents si és bàsic.
B	És un patró doblement sincrònic.
C	Evita la concurrència en l'agent client.
D	Un defecte en el servidor bloquejarà al client si aquest últim ja havia enviat la seua petició.
E	Totes les anteriors. Els aspectes esmentats en aquests apartats caracteritzen a aquest patró
F	Cap de les anteriors.

33. Semàntiques en cas de reinici del servidor en el patró petició/resposta...

A	La semàntica "almenys una vegada" seria recomanable en cas d'utilitzar operacions idempotents. CERT. Les operacions idempotents sempre generen el mateix resultat, independentment del nombre de vegades que arriben a executar-se. Per tant, convé que aquestes operacions s'executen almenys una vegada. Si s'executaren més d'una no es generarà cap mal comportament ni es generarà cap inconsistència en l'estat dels servidors.
B	La semàntica "almenys una vegada" és la que ha d'utilitzar-se en cas que també puga fallar el client. FALS. Si el servidor no poguera gestionar adequadament les repeticions de les peticions fetes pels clients, aquesta semàntica podria arribar a generar inconsistències en l'estat. Per tant, depèn de com es comporte el servidor davant missatges repetits. Que falle o no el client i en quin moment arribe a fallar no sempre condiciona la semàntica assumida. De fet, si el client fallara podria arribar-se a perdre l'última petició que pretenia iniciar mentre va fallar. En aquest cas hauria resultat més fàcil seguir una semàntica "com a màxim una vegada".
C	La semàntica "com a màxim una vegada" realitza almenys una reexpedició de la petició. FALS. Les reexpedicions s'utilitzaran en la semàntica "almenys una vegada". Són innecessaris en la semàntica "com a màxim una vegada".
D	La semàntica "com a màxim una vegada" és la que ha d'utilitzar-se quan no es replique el servidor. FALS. Tant una semàntica com l'altra dependran del tipus d'operació a executar. El fet que el servidor estiga replicat no condiciona l'ús d'una semàntica o una altra.
E	Processador, Causal. Aquesta opció estava originalment mal (són models de consistència del parcial anterior) i es va modificar en l'examen passant a ser "Totes les anteriors".
F	Processador, Causal, "*Cache*", FIFO. Aquesta opció estava originalment mal (són models de consistència del parcial anterior) i es va modificar en l'examen passant a ser "Cap de les anteriors".

34. El patró PUSH-PULL...

A	És un patró doblement sincrònic. FALS. És un patró asincrònic. No exigeix el bloqueig de l'emissor ni del receptor.
B	És un patró de comunicació bidireccional. FALS. És un patró unidireccional. Els missatges sempre s'envien des del socket PUSH i van a parar al socket PULL.
C	Assumeix consistència causal. FALS. No assumeix ni exigeix cap tipus de consistència predeterminat.
D	És un patró de comunicació unidireccional. CERT.
E	Totes les anteriors.
F	Cap de les anteriors.

35. El patró PUSH-PULL...

A	Limita l'escalabilitat en introduir bloquejos perllongats en cas de relacionar en una cadena a múltiples components. FALS. No introdueix bloquejos, per ser asincrònic.
B	És un patró asincrònic. CERT. Ja s'ha comentat en l'apartat A de la qüestió anterior.
C	Assumeix consistència seqüencial. FALS. No assumeix ni exigeix cap model de consistència predeterminat.
D	Exigeix una semàntica "almenys una vegada". FALS. No exigeix cap semàntica de lliurament d'operacions. Tampoc és clar que els components a intercomunicar seguisquen sempre un model client/servidor. Per a fer això ja existeix el patró petició/resposta.
E	Totes les anteriors.
F	Cap de les anteriors.

36. En desplegar un patró PUSH-PULL en ZMQ...

A	Els sockets PUSH es configuraran amb les adreces dels sockets PULL. FALS. Depèn de quin siga el component estable.
B	Els sockets PULL es configuraran amb les adreces dels sockets PUSH. FALS. Depèn de quin siga el component estable.
C	Tant els sockets PUSH com els PULL es configuraran amb les adreces dels sockets de l'altre tipus. FALS. Depèn de quin siga el component estable. És difícil que tots dos components siguen estables i necessiten una configuració com la comentada en aquest apartat.
D	Els sockets de tipus menys estable es configuraran amb l'adreça del socket de tipus més estable. Quin tipus serà més estable dependrà del servei a desplegar. CERT. Aquesta va ser la regla a seguir explicada en les classes.
E	Totes les anteriors.
F	Cap de les anteriors.

37. El patró PUB-SUB...

A	És un patró de comunicació bidireccional. FALS. En un patró de comunicació unidireccional. Els missatges són sempre emesos pel socket PUB i entregats en els sockets SUB.
B	Utilitza comunicació sincrònica. FALS. Utilitza comunicació asincrònica.
C	En desplegar-ho se solen configurar els sockets PUB amb les adreces dels sockets SUB. FALS. Per ser un patró dissenyat per a fer difusions, és més lògic que el component estable siga l'emissor i que siga responsabilitat dels subscriptors/receptors el configurar-se amb l'adreça d'aquest component estable. Si es fera al contrari, el publicador hauria de reconfigurar-se cada vegada que s'afegira un nou subscriptor.
D	S'utilitza per a difondre missatges des del socket SUB als sockets PUB. FALS. Com ja s'ha explicat en el primer apartat, la comunicació unidireccional segueix el sentit contrari. Des de PUB cap a SUB.
E	Totes les anteriors.
F	Cap de les anteriors.

.

38. Una arquitectura petició/resposta avançada pot implantar-se utilitzant una cua de comunicació intermèdia (o agent "bróker"). En aquesta arquitectura...

A	El "bróker" sol utilitzar dos sockets ROUTER.
B	Els servidors (o treballadors) poden substituir els seus sockets REP per sockets REQ.
C	Els servidors (o treballadors) poden substituir els seus sockets REP per sockets DEALER.
D	Tindrà una recuperació delicada quan falle el "bróker", ja que sol ser el component estable en aquest patró arquitectònic.
E	Totes les anteriors. Com s'ha pogut veure en pràctiques i en el tema 9 de teoria, tots els apartats anteriors són certs.
F	Cap de les anteriors.

39. En una arquitectura client/servidor avançada pot necessitar-se un mecanisme per a detectar i rebutjar peticions duplicades si…

QÜESTIÓ ANUL·LADA. En alguns grups de teoria no es va explicar la semàntica "exactament una vegada". La resposta correcta era la "D" i podia deduir-se de la fulla de la presentació del tema 9 en la qual s'explicava aquest mecanisme de detecció i rebuig de peticions duplicades.

A	S'utilitza una semàntica "almenys una vegada" i la petició és idempotent.
B	S'utilitza una semàntica "almenys una vegada" i el servidor no està replicat.
C	S'utilitza una semàntica "exactament una vegada" i la petició és idempotent.
D	S'utilitza una semàntica "exactament una vegada" i la petició no és idempotent.
E	Totes les anteriors.
F	Cap de les anteriors.

40. Alguns problemes de l'arquitectura PUB/SUB són...

A	Pèrdua de missatges en subscriptors lents o amb inici tardà en la seua subscripció. CERT. Aquests són els dos problemes principals d'aquest patró arquitectònic. En el tema 9 es van descriure algunes solucions per a cada problema.
B	Desplegament difícil. No resulta fàcil decidir quins agents poden considerar-se estables. FALS. El component estable sempre serà el publicador/difusor.
C	Utilitza un patró de comunicació bidireccional sincrònic que difícilment pot escalar. FALS. Utilitza un patró unidireccional asincrònic fàcilment escalable.
D	Ha d'usar un agent intermediari que podrà fallar. FALS. L'agent intermediari o "bróker" es podria necessitar en un patró petició/resposta avançat però no s'ha dit en cap moment (ni té sentit) que puga necessitar-se per a un patró publicació/subscripció.
E	Totes les anteriors.
F	Cap de les anteriors.