PARLAMENT DE CATALUNYA

QÜESTIONARI

PUBLICAT

28 GEN. 2026

PARLAMENT DE CATALUNYA · Departament de Recursos Humans ·

CONVOCATÒRIA: Procés de selecció per a cobrir una plaça de tècnic mitjà o tècnica mitjana d'informàtica del Parlament de Catalunya
Tècnic o tècnica de sistemes i seguretat de la informació (501-00005/15)

EXERCICI: Segon exercici de la primera prova

Informació general

- ✓ La durada d'aquest exercici és de quaranta minuts.
- ✓ Aquesta prova, de caràcter obligatori i eliminatori, consisteix a respondre un qüestionari tipus test de 20 preguntes més 2 de reserva, amb 3 respostes alternatives.
- ✓ La qualificació d'aquest exercici és de 0 a 15 punts. La puntuació mínima per a superar-lo és de 7,5 punts.
- ✓ Les preguntes sense resposta o amb més d'una resposta no es tenen en compte.
- ✓ Per a cada resposta errònia es descompta una tercera part del valor d'una resposta encertada.
- ✓ En cas que el tribunal qualificador acordi l'anul·lació d'alguna pregunta, s'inclourà, a l'efecte del càlcul de la qualificació resultant, la primera de les preguntes de reserva, i així successivament.
- ✓ Els aspirants no poden fer constar cap dada identificativa en les respostes. Si ho incompleixen, seran exclosos del procés selectiu.

Instruccions per a fer l'exercici

- ✓ Comproveu que el nom que encapçala els fulls dels codis de barres sigui el vostre i que el vostre DNI sigui correcte.
- ✓ Enganxeu una etiqueta del codi de barres al full de respostes, a l'espai indicat.
- ✓ Heu de transcriure a l'apartat ID del full de respostes les quatre darreres xifres del vostre codi de barres
- ✓ Si voleu canviar una resposta, només ho podeu fer amb el corrector líquid blanc, i heu de tapar totalment la resposta que voleu canviar, tant al full original com a la calca.

1) En un entorn corporatiu amb múltiples zones i serveis exposats, quina mesura té un impacte més directe en la reducció de la superfície d'atac externa?

a) Segmentació de xarxa mitjançant VLAN.

b) Implementació d'ACL restrictives.

c) Centralització del trànsit en un únic punt d'accés.

2) En un entorn de virtualització, quin avantatge específic introdueix la paravirtualització respecte a la virtualització completa en termes de rendiment i integració amb l'hipervisor?

a) Comunicació optimitzada amfitrió-hoste (*host-guest*) mitjançant programes controladors (*drivers*) específics.

b) Eliminació de la necessitat d'hipervisor.

c) Aïllament complet sense dependència del sistema hoste (*host*).

3) En el marc de l'ENS, quin criteri ha de prevaler a l'hora de definir i implantar mesures de seguretat en els sistemes d'informació de les administracions públiques?

a) L'adopció de mesures de seguretat proporcionals al nivell de risc i a la categoria del sistema.

b) L'aplicació homogènia d'un conjunt fix de mesures per a garantir un nivell de seguretat uniforme.

c) La priorització de la disponibilitat del servei per damunt de la confidencialitat i la integritat de la informació.

4) En un SOC amb monitoratge d'amenaces centralitzat, quin és el risc operatiu més crític si no s'aplica una correlació adequada d'esdeveniments entre diferents fonts de seguretat?

a) Incapacitat de detectar atacs avançats que es manifesten mitjançant patrons distribuïts.

b) Retard en l'actualització i distribució de signatures de seguretat.

c) Reducció de la capacitat de resposta automàtica davant d'incidents simples.

5) En un entorn corporatiu amb gestió centralitzada d'actualitzacions, quin és el risc més greu d'aplicar automàticament tots els pedaços de seguretat crítics sense una fase prèvia de validació?

a) Actualitzacions malicioses que possibilitin la inserció de programari maliciós (*malware*) no desitjat.

b) Introducció d'incompatibilitats o regressions que afectin serveis crítics de producció.

c) Necessitat de reinicis freqüents dels equips d'usuari.

6) Quin mecanisme permet alta disponibilitat en Exchange?

a) Database Availability Group (DAG).

b) Mail Distributed Box (MDB).

c) Mail Cloud Box (MCB).

7) Quin component és crític en un pla de contingència?

a) Inventari de serveis i punts d'accés.

b) Accés a les instal·lacions.

c) Definició d'RTO i RPO.

8) Quan copiem un fitxer NTFS a una altra partició NTFS, què passa?

a) Manté per defecte els permisos que té en origen.

b) Manté per defecte permisos de l'usuari que fa l'acció.

c) Hereta permisos de la destinació.

9) Què és l'*split tunneling*?

a) Separar el trànsit corporatiu i d'Internet per dins de la VPN.

b) Permetre que una part del trànsit vagi per Internet i l'altra part, per la VPN.

c) Trànsit amb dos tipus de xifratge: un de feble (128 bits) i un de fort (512 bits).

10) Què defineix un CPD TIER III?

a) Redundància N+1 parcial i manteniment sense aturada.

b) Redundància N+1 complet i manteniment sense aturada.

c) Disposar de connexió a tres subministraments elèctrics amb camins diferents.

11) Quin concepte defineix "*edge computing*"?

a) Situar els serveis al núvol i garantir-ne l'accessibilitat.

b) Evitar l'accés als serveis per mitjà d'un WAF.

c) Processar dades prop de l'origen per a reduir latència.

12) Quin principi de seguretat estableix que els usuaris només han de disposar dels permisos necessaris per a complir les seves funcions en un context determinat?

a) *Least privilege.*

b) *Zero trust.*

c) *Full access.*

13) Quin és el principal benefici d'implementar un sistema de gestió de diaris (*logs*) centralitzats en una infraestructura IT?

a) Limitar l'automatització dels processos de monitoratge per a evitar falsos positius.

b) Permetre la detecció d'incidències, la correlació d'esdeveniments i l'anàlisi transversal de l'activitat dels sistemes.

c) Reduir el consum de recursos dels sistemes origen mitjançant l'eliminació de registres locals.

14) En l'aplicació d'un pla de resposta a incidents de seguretat, quin és el risc més crític si no s'hi inclou una fase d'anàlisi postincident?

a) La pèrdua de traçabilitat i de la relació de serveis implicats.

b) La repetició d'incidents similars per no corregir vulnerabilitats i causes arrel.

c) El fet de no poder correlacionar incidents distribuïts en sistemes diferents.

15) Quin és un risc que assumeix l'usuari quan fa ús de connexions wifi?

a) Possibilitat d'interferències de ràdio que provoquin desconnexions intermitents.

b) Compromís de credencials mitjançant atacs d'intermediari (*man-in-the-middle*).

c) Limitació del nombre de dispositius que poden connectar-se simultàniament.

16) Quin missatge DHCP envia el servidor?

a) Discover.

b) Offer.

c) Request.

17) Quin mecanisme permet la recuperació del contingut i la configuració d'un servidor crític en el menor temps possible?

a) Copiar fitxers a mà.

b) Tenir les cintes custodiades fora de l'organització.

c) *Bare-metal recovery.*

18) Durant la gestió d'un incident de seguretat, quin objectiu ha de prioritzar-se a l'hora de definir i aplicar accions correctives després de la contenció inicial?

a) Restaurar el servei tan ràpidament com sigui possible, independentment de la causa.

b) Limitar les accions correctives als sistemes directament afectats.

c) Corregir les vulnerabilitats identificades segons l'impacte i la probabilitat d'explotació.

19) Quin és el risc més rellevant associat a l'ús de dispositius criptogràfics (com targetes intel·ligents o HSM) si no es gestionen adequadament dins d'un sistema de signatura electrònica?

a) Increment del temps necessari per a generar signatures.

b) Compromís de les claus criptogràfiques i invalidació de signatures generades.

c) Incompatibilitat de formats de document específics.

20) En un procés d'anàlisi informàtica forense, quina és la fita més crítica durant la recollida i preservació de proves digitals per a garantir-ne la validesa legal i tècnica?

a) Assegurar la integritat de les proves mitjançant còpies forenses verificades i cadena de custòdia.

b) Aïllar els sistemes afectats per a garantir l'obtenció d'evidències i reduir el temps d'investigació.

c) Garantir la cadena de custòdia treballant directament sobre els sistemes afectats.

PREGUNTES DE RESERVA

21) En un entorn de servidors de producció, quina pràctica contribueix millor a garantir la traçabilitat, l'estabilitat del servei i la reducció del risc operatiu?

a) Permetre l'accés habitual amb comptes privilegiats per a agilitar la resolució d'incidències.

b) Documentar, registrar i desplegar els canvis mitjançant procediments controlats i auditables.

c) Documentar i desplegar els canvis mitjançant eines de versionament.

22) Quin vector d'atac està directament relacionat amb tècniques d'enginyeria social?

a) Saturació deliberada de serveis per DDoS.

b) Campanyes de correu electrònic dissenyades per a induir l'usuari a executar accions no legítimes.

c) Explotació de vulnerabilitats de tipus "*zero-day*".