Consell Comarcal Berguedà

PROVA TEORICOPRÀCTICA

DNI:_____

PERSONAL FUNCIONARI TÈCNIC/A AUXILIAR DE GESTIÓ _ INFORMÀTICA

Aquesta prova tindrà una **puntuació màxima de 50 punts**, per superar la prova la puntuació mínima serà de 25 punts.

Temps màxim: 120 minuts

S'ha de desar el document a l'escriptori de l'ordinador amb el nom:

PROVA TEORICOPRACTICA_DNI (Ex. PROVA PRACTICA_12345678A)

Nota: Les respostes han de ser breus i concisses. Cal argumentar totes les respostes.

EXERCICI 1 (25 punts)

El Consell Comarcal del Berguedà ha realitzat recentment una auditoria en ciberseguretat els resultats de la qual mostren alguns punts de possibles millores. En aquest context, respon les següents preguntes.

a) **L'auditoria destaca que el Consell Comarcal disposa únicament d'un antivirus tradicional instal·lat als equips de treball. Consideres que aquesta mesura és suficient per protegir els sistemes? Quines millores podries implementar per incrementar la seguretat dels equips? (5 punts)**

Un antivirus tradicional és una mesura de seguretat necessària, però actualment no és suficient per protegir els equips d'un consell comarcal davant de les amenaces informàtiques actuals. Aquest tipus d'antivirus es basa principalment en la detecció de virus coneguts mitjançant signatures, de manera que pot no detectar amenaces noves, atacs sense fitxers (fileless), ransomware avançat o comportaments maliciosos desconeguts.

*Una de les principals millores que implementaria seria la substitució o complement de l'antivirus amb una solució **EDR (Endpoint Detection and Response)**. Un EDR monitoritza de manera contínua l'activitat dels equips, detecta comportaments anòmals o sospitosos, permet investigar els incidents de seguretat i pot aplicar mesures de resposta, com ara l'aïllament d'un equip compromès per evitar que l'atac es propagui a la resta de la xarxa.*

*A més de l'EDR, també implantaria **altres mesures complementàries**, com ara mantenir el sistema operatiu i les aplicacions sempre **actualitzades**, aplicar el principi del **mínim privilegi** als usuaris, utilitzar **autenticació multifactor** en els serveis que ho permetin, realitzar **còpies de seguretat** periòdiques i **formar els treballadors** en la detecció de correus fraudulents i altres tècniques d'enginyeria social.*

La combinació d'aquestes mesures permetria augmentar la capacitat de prevenció, detecció i resposta davant incidents de seguretat, reduint el risc que una amenaça afecti els serveis i la informació del Consell Comarcal.

b) L'auditoria recull el fet que els diferents sistemes del Consell Comarcal (servidors, firewall, punts d'accés inal•làmbrics, etc.) generen fitxers de registre (logs), per separat. Quin sistema podries implementar per controlar aquests logs de forma centralitzada i eficient? Posa un exemple d'una solució existent que disposi d'aquesta funcionalitat. (5 punts)

*Per gestionar els registres de manera centralitzada implementaria un sistema **SIEM (Security Information and Event Management)**. Aquest tipus de solució permet recollir els logs generats pels diferents dispositius i sistemes del Consell Comarcal, com ara servidors, tallafocs, punts d'accés Wi-Fi, equips de xarxa o aplicacions, i emmagatzemar-los en un únic repositori.*

A més de centralitzar els registres, un SIEM els normalitza i correlaciona per detectar patrons o comportaments anòmals que podrien indicar un incident de seguretat. També permet configurar alertes automàtiques, generar informes, facilitar les tasques d'auditoria i conservar els registres durant el temps necessari per complir els requisits legals o de seguretat.

La implantació d'un SIEM facilita la detecció precoç d'atacs, la investigació d'incidents i la resposta davant possibles amenaces, ja que evita haver de consultar els logs de cada sistema de manera individual.

*Com a exemple de solució existent es pot citar **Wazuh**, una plataforma de codi obert molt utilitzada per a la monitorització de la seguretat i la gestió centralitzada de logs. També són exemples **Microsoft Sentinel**, **Splunk Enterprise Security**, **IBM QRadar** o **Elastic Security**, tots ells amb funcionalitats de SIEM.*

c) A l'auditoria es parla de conscienciar al personal sobre els riscos del *phishing*. Descriu què és el *phishing* junt amb un exemple aplicable a l'entorn del Consell Comarcal. Descriu també quines accions es poden fer per conscienciar el personal. (5 punts)

*El phishing és una **tècnica d'enginyeria social** mitjançant la qual un ciberdelinqüent intenta enganyar una persona perquè **reveli informació confidencial**, com ara credencials d'accés, dades personals o bancàries, **o bé perquè descarregui un fitxer maliciós o accedeixi a una pàgina web fraudulenta**. Normalment, el phishing es duu a terme a través del correu electrònic, tot i que també es pot produir mitjançant SMS, trucades telefòniques o missatges instantanis.*

Un exemple aplicable a un consell comarcal seria la recepció d'un correu electrònic aparentment enviat pel departament d'informàtica o per un proveïdor habitual, en què s'informa que el compte de correu està a punt de caducar i es demana a l'usuari que faci clic en un enllaç per validar les seves credencials. Si l'empleat introdueix l'usuari i la contrasenya en aquesta pàgina fraudulenta, l'atacant pot obtenir accés als serveis corporatius.

Per conscienciar el personal es poden dur a terme diverses accions:

- *Organitzar **sessions de formació** periòdiques sobre ciberseguretat i enginyeria social.*
- *Realitzar **campanyes simulades de phishing** per avaluar el comportament dels treballadors i reforçar-ne l'aprenentatge.*
- *Difondre **guies o recomanacions** amb els indicadors d'un correu sospitós, com ara errors ortogràfics, remitents desconeguts, enllaços estranys o peticions urgents d'informació.*
- *Establir un procediment senzill perquè els empleats puguin comunicar correus sospitosos al servei d'informàtica.*
- ***Recordar periòdicament les bones pràctiques**, com ara no obrir fitxers adjunts d'origen desconegut, verificar les peticions inusuals per un altre canal i no facilitar mai les credencials a través del correu electrònic.*

d) Un altre punt de millora que es descriu és el relatiu a la gestió de les contrasenyes. Els auditors han detectat que part del personal reaprofita la mateixa contrasenya en diferents sistemes, i han trobat llibretes escrites a mà als calaixos del personal que contenen credencials. Aquestes persones ho han justificat dient que no poden recordar tantes contrasenyes si, a més, les han de modificar periòdicament i han de tenir una certa complexitat. Quina solució pots aportar a aquest problema? (5 punts)

La situació descrita representa un risc important per a la seguretat del Consell Comarcal. Reutilitzar la mateixa contrasenya en diferents serveis fa que, si una d'elles es veu compromesa, un atacant pugui intentar utilitzar-la per accedir a altres sistemes corporatius. A més, guardar les credencials en llibretes o notes físiques facilita que qualsevol persona no autoritzada pugui obtenir-les.

*Una bona solució és implantar un **gestor de contrasenyes corporatiu**. Aquest tipus d'eina permet emmagatzemar totes les credencials de manera xifrada, de manera que els usuaris només han de recordar una única contrasenya mestra. A més, molts gestors poden generar automàticament contrasenyes llargues, aleatòries i diferents per a cada servei, reduint el risc associat a la reutilització de credencials.*

*Aquesta mesura s'hauria de complementar amb una **política de contrasenyes adequada**, que exigeixi una longitud suficient i eviti l'ús de contrasenyes febles o conegudes. També és recomanable no obligar a canvis periòdics de contrasenya de forma indiscriminada, sinó exigir-los quan hi hagi indicis de compromís o quan la política de seguretat així ho requereixi, ja que els canvis massa freqüents poden afavorir males pràctiques com l'ús de contrasenyes previsibles o l'anotació en paper.*

*Sempre que sigui possible, també implantaria **l'autenticació multifactor (MFA)**, de manera que, encara que una contrasenya fos robada, l'atacant necessitaria un segon factor d'autenticació per accedir al sistema.*

*Finalment, és important complementar les mesures tècniques amb **accions de conscienciació** perquè el personal entengui els riscos de compartir, reutilitzar o emmagatzemar les contrasenyes de forma insegura i conegui les eines corporatives disponibles per gestionar-les de manera segura.*

e) Més enllà dels beneficis tècnics que aportaria implantar millores en ciberseguretat, existeix alguna obligació legal en aquest àmbit? En cas afirmatiu, descriu breument la norma o normes que ho regula. (5 punts)

***La principal norma és l'Esquema Nacional de Seguretat (ENS)**, regulat pel Reial decret 311/2022, que estableix els principis i les mesures mínimes de seguretat que han d'aplicar les administracions públiques i les entitats que presten serveis al sector públic. L'ENS obliga a implantar mesures organitzatives, operatives i de protecció, gestionar els riscos, controlar els accessos, protegir la informació, registrar els incidents de seguretat i garantir la disponibilitat dels serveis.*

Addicionalment Reglament General de Protecció de Dades (RGPD) i Llei orgànica 3/2018, de protecció de dades personals i garantia dels drets digitals (LOPDGDD).

EXERCICI 2 (25 punts)

a) Quin procediment de contractació és el més adequat per als següents objectes de contracte? En quina tipologia es classifiquen en cada cas? (5 punts)

- **Adquisició de 10 portàtils per un valor total de 8.000€ IVA inclòs.**

  Contracte menor. Subministraments.

- **Gestor d'expedients electrònics en modalitat SaaS per quatre anys, amb un valor estimat de 100.000€ IVA inclòs**

  Procediment obert simplificat. Serveis.

- **Formació sobre protecció de dades, amb una durada d'un dia i un valor estimat de 500€ IVA inclòs**

  Pagament menor (o contracte menor). Serveis.

b) Un alcalde d'un ajuntament del Berguedà truca al Consell Comarcal perquè necessita suport per sol•licitar certificats digitals per ell, en la seva condició d'Alcalde, per una administrativa i per poder fer còpies autèntiques mitjançant actuació administrativa automatitzada. A més, et diu que ell necessita poder signar des del telèfon mòbil. Quins tipus de certificats del Consorci AOC recomanes que demani? (5 punts)

Alcalde: ***T-CAT P amb càrrec.***

Administrativa: ***T-CAT (o T-CAT P).***

Còpies autèntiques amb AAA: ***Segell electrònic de nivell mig (certificat d'aplicació).***

c) El Consell Comarcal del Berguedà disposa d'un portal web desenvolupat amb Drupal, allotjat en un servidor virtual privat (VPS) contractat a un proveïdor extern. Explica quina política de gestió d'actualitzacions consideres adequada per garantir la seguretat i la disponibilitat del servei. Descriu quins elements s'han d'actualitzar, quines comprovacions prèvies i posteriors cal realitzar i quins riscos pot comportar no mantenir el sistema correctament actualitzat. (5 punts)

Cal establir una ***política d'actualitzacions periòdica*** *per garantir la seguretat del portal web. Tot i que el VPS estigui allotjat en un proveïdor extern, s'han de definir clarament les responsabilitats de manteniment.*

S'han d'actualitzar el ***nucli de Drupal****, els* ***mòduls****, els* ***temes*** *i, si correspon, el* ***sistema operatiu*** *del VPS i el programari de suport (PHP, servidor web i base de dades).*

Abans d'actualitzar cal fer una ***còpia de seguretat****, comprovar possibles incompatibilitats i, si és possible, provar els canvis en un entorn de proves. Un cop finalitzada*

*l'actualització, s'ha de **verificar que el portal funciona correctament** i revisar els registres per detectar incidències.*

*No mantenir el sistema actualitzat pot permetre **l'explotació de vulnerabilitats** conegudes, provocar **accessos no autoritzats**, comprometre les dades o afectar la disponibilitat del servei. Per això és important aplicar les actualitzacions de seguretat tan aviat com sigui possible.*

d) Analitza el següent codi en Python:

```
def programa(valors):
    suma = 0
    for element in valors:
        suma += element
    return suma / len(element)

dades = [10, 20, 30, 40]
resultat = programa(dades)
print(f"El resultat és {resultat}")
```

- **Identifica l'error del codi i explica per què es produeix (2 punts)**

  A la instrucció return suma / len(element), s'utilitza element (que és un enter corresponent a l'últim element recorregut pel bucle) en lloc de la llista valors. Això provoca un error perquè len() no es pot aplicar a un enter (TypeError).

- **Corregeix l'error per tal que el programa funcioni corretament (1 punts)**

  return suma / len(valors)

- **Explica breument quina és la funcionalitat del programa un cop corregit (2 punts)**

  El programa rep una llista de nombres, en suma tots els elements mitjançant un bucle for, calcula la mitja dividint la suma pel nombre d'elements de la llista i mostra el resultat per pantalla.

e) El Consell Comarcal vol prescindir dels servidors físics presents a les seves instal·lacions. Un d'ells és un Windows Server 2016 que proporciona, principalment, les funcionalitats de servidor de fitxers i de directori actiu. És possible traslladar aquestes funcionalitats al núvol? En cas afirmatiu, quines solucions de mercat equivalents existeixen? Quines avantatges i inconvenients comporta la migració d'aquests serveis al núvol? (5 punts)

***Sí, és possible migrar aquestes funcionalitats al núvol**. Per al servei de fitxers es poden utilitzar solucions com **SharePoint Online** o **Azure Files**, mentre que per a la gestió d'identitats i autenticació es pot utilitzar **Microsoft Entra ID**, o bé un entorn híbrid que combini el directori local amb el núvol.*

*Entre els principals avantatges hi ha la reducció del maquinari propi, una **major disponibilitat** dels serveis, la facilitat **d'accés des de qualsevol ubicació**, les còpies de seguretat gestionades pel proveïdor i la possibilitat **d'escalar els recursos** segons les necessitats.*

*Com a inconvenients, cal considerar la **dependència de la connexió a Internet**, el **cost recurrent de les subscripcions**, la necessitat de planificar la migració per evitar interrupcions del servei i la possible incompatibilitat d'algunes aplicacions antigues amb les solucions al núvol. També és important revisar els aspectes de seguretat, protecció de dades i compliment de la normativa vigent.*