Ajuntament de
PALAU-SOLITÀ
I PLEGAMANS

CONCURS-OPOSICIÓ TÈCNIC/A AUXILIAR INFORMÀTICA

Prova 1. Teòrica. Coneixements temari general i específic.

1. Que es considera un endpoint i com funciona la seguretat avançada als endpoints? (2 punts)

Es considera un endpoint qualsevol dispositiu que es comuniqui amb la xarxa informàtica, es a dir, qualsevol punt d'accés a la xarxa des de la que les persones usuàries poden interactuar. Alguns exemples de dispositius endpoints son els següents:

- Servidors, ordinadors d'escriptori i equips portàtils
- Smartphones i tablets.
- Impressores, escàners i altres perifèrics
- Càmeres de seguretat
- Robots i dispositius IoT.

La seguretat de endpoints va més enllà dels software antivirus tradicionals, implica la implementació de solucions centralitzades que ofereixen protecció davant amenaces cibernètiques mitjançant diversos mecanismes com anàlisi de malware, detecció d'intrusions i prevenció de fuga de dades, així com la detecció d'amenaces en temps reals.

La gestió centralitzada d'aquests dispositius permet una resposta ràpida davant possibles incidents i la implementació de polítiques de seguretat coherents, millorant així la visibilitat, simplificació de les operacions i permetent l'aïllament ràpid de possible amenaces.

Les solucions de seguretat per a endpoint, entre d'altres, inclouen tallafocs, sistemes de detecció d'intrusions, encriptació de dades, gestió de dispositius mòbils (MDM), xifrat de endpoints, correu electrònic i disc dur, seguretat proactiva per facilitar la navegació segura, protecció antivirus i antimalware, passarel·la de correu electrònic per protegir-se de la suplantació d'identitat i altres intents d'enginyeria social, control d'accés a la xarxa i aprenentatge automàtic per detectar vulnerabilitats.

La seguretat dels endpoints funciona examinant arxius, processos i sistemes a la cerca d'activitats sospitoses o malicioses, permeten als administradors supervisar, investigar i

Plaça de la Vila, 1
08184 Palau-solità i Plegamans
Tel. 93 864 80 56 · Fax 93 864 92 59
www.palauplegamans.cat

respondre a possibles amenaces, ajudant així a prevenir les infraccions abans que es produeixin.

El software client s'implementa a cada endpoint, aquest envia actualitzacions quan es necessari, autentica intents d'inici de sessió i administra les polítiques corporatives, a més també protegeix l'equip mitjançant el control d'aplicacions que impedeix que l'usuari descarregui o accedeixi a aplicacions no segures o que no estan autoritzades per l'organització, i també utilitza xifrat per evitar la pèrdua de dades.

2. Certificats Digitals en un Ajuntament – Tipologia, Instal·lació i Bones Pràctiques (2 punts)

1. Tipus de certificats digitals

1.1 Certificats de programari (software)

Els certificats de programari són fitxers digitals (habitualment .p12 o .pfx) que s'instal·len al sistema o navegador. Són utilitzats per signar documents o autenticar serveis digitals.

1.2 Certificats de hardware (targetes o tokens)

Són certificats continguts en dispositius físics com targetes intel·ligents o tokens USB, protegits per PIN. Són més segurs i habituals en el sector públic per a signatura qualificada.

Exemples habituals de certificats digitals

Dispositiu o certificat	Finalitat	Format o suport
Certificat de seu electrònica	Signatura de la seu i tràmits	Software (.pfx)
Certificat SSL/TLS	Connexió HTTPS per webs	Software (.crt/.key)
Certificat personal FNMT	Signatura de documents	.p12 o targeta
DNI electrònic	Autenticació personal	Hardware (targeta)
Token USB criptogràfic	Certificat personal o aplicacions	Hardware (USB)

2. Elements implicats

- Usuari o empleat públic
- Equip informàtic (ordinador, navegador)
- Sistema operatiu i navegador (Windows, Firefox...)
- Lectors de targetes o dispositius USB
- Sistema de gestió de certificats
- Equip TIC i suport informàtic

3. Instal·lació i configuració

3.1 Certificats de programari

- Importar al sistema (certmgr.msc o navegador)
- Assegurar instal·lació de la clau privada

- Comprovar que la CA arrel és de confiança
- Configurar navegador (Firefox té magatzem propi)

3.2 Certificats de hardware

- Instal·lar drivers del dispositiu (DNIe, CERES...)
- Instal·lar PKCS#11 en Firefox
- Validar accés al certificat amb lector i PIN
- Importar certificats de CA si cal

4. Bones pràctiques en entorns públics

- Control de caducitat i renovació proactiva
- Protecció del PIN i del dispositiu
- Revocació immediata en cas de pèrdua
- Gestió centralitzada de certificats en servidors
- Formació específica al personal
- Registre i inventari dels certificats corporatius

5. Exemple pràctic a un ajuntament

Ús habitual dels certificats en un entorn municipal:

Ús	Certificat	Format	Dispositiu
Seu electrònica	Certificat de representació	Software (.pfx)	Servidor web
Tràmits online	Certificat SSL	.crt/.key	Web en DMZ
Accés policies	Targeta T-CAT	Hardware	Lector + PIN
Firma d'alcalde	Certificat personal FNMT	.p12	PC d'alcaldia
Web services externs	Certificat aplicació	.pfx	Servidor intermediari

3. Enumera quantes més millor, les funcions de l'Alcalde en un Ajuntament, d'acord amb la Llei 7/1985, de 2 d'abril, reguladora de les bases del règim local (articles 21 i 22). (2 punts)

L'Alcalde és el President de la Corporació i exerceix les següents atribucions:

a) Dirigir el govern i l'administració municipal.
b) Representar l'Ajuntament.
c) Convocar i presidir les sessions del Ple, de la Junta de Govern Local i de qualsevol altre òrgan municipal, així com decidir els empats amb vot de qualitat.
d) Dirigir, inspeccionar i impulsar els serveis i obres municipals.
e) Dictar bans, decrets i resolucions.

f) Nomenar i cessar els Tinents d'Alcalde i membres de la Junta de Govern Local.
g) Organitzar els serveis administratius de l'Ajuntament d'acord amb les normes organitzatives aprovades pel Ple.
h) Exercir la prefectura superior de tot el personal, inclosa la imposició de sancions, llevat de la separació del servei dels funcionaris, que correspon al Ple.
i) Exercir accions judicials i administratives en cas d'urgència.
j) Adoptar mesures necessàries en casos de catàstrofe o risc greu.
k) Autoritzar, disposar despeses dins els límits del seu àmbit, ordenar pagaments i rendir comptes.
l) Aprovar l'oferta d'ocupació pública i les bases de les proves de selecció i de concursos.
m) Desenvolupar la gestió econòmica conforme al pressupost aprovat.
n) Contractar dins dels límits establerts per la llei.
ñ) Otorgar llicències, excepte les que corresponguin al Ple.
o) Imposar sancions per infraccions de les ordenances.
p) Aprovar projectes d'obres i serveis dins dels límits del seu àmbit.
q) L'exercici de qualsevol altra competència que li atribueixin les lleis.

4. Funcionament d'un centre d'atenció a l'usuari I – Gestió d'incidències, passes a seguir per la seva resolució. Conceptes de primer Nivell de suport. Concepte de Nivell de Servei, eines i protocols. (2 punts)

A. Assistència a l'usuari

El primer contacte amb el servei de suport tècnic és el suport de nivell 1 o help desk, suport front-end o assistència de primera línia de suport que facilita informació relacionada amb el programari i serveis que l'ens disposa per realitzar les tasques diàries de cada servei intern. Encara que aquest servei el sol dur a terme un equip intern, de vegades es pot subcontractar el servei a proveïdors externs, hi ha serveis que no depenen del mateix ens i que son eines gestionades per altres organismes o ens que tenen el seu suport tècnic. Les tasques i funcions habituals de l'help desk són:

- Recollir les incidències diàries per mitjà d'un gestor d'incidències.
- Atendre les consultes per telèfon o correu electrònic dels clients quan l'usuari estigui bloquejat.
- Registrar l'activitat de trucades i correus electrònics.
- La gestió de tot tipus de programes o sistemes operatius que utilitzen els usuaris.
- Resolució de problemes bàsics de programari, maquinari i xarxa.
- Procurar l'assistència necessària que se sol·liciti sobre productes o serveis de l'ens o l'organisme on s'està donant suport.
- Estar al corrent de tot el que passa al organisme i els canvis que succeeixen dins de la mateix.
- Transmetre problemes de més dificultat que no poden ser resolts pel help desk a el suport de segon nivell.

B. Suport informàtic

El suport de segon nivell, T2 o L2 en el segon nivell de suport tècnic informàtic dins d'una empresa. Els clients són redirigits a aquest nivell després d'un primer contacte amb help desk i que aquest no hagi pogut solucionar la incidència per no tenir coneixements o eines necessàries per a això. El suport de segon nivell ajuda als clients a resoldre problemes més tècnics, normalment en remot, a través de trucada telefònica o per xat en línia. Les funcions que realitzen els tècnics de suport nivell 2 són:

- Trobar solucions als problemes dels clients i, si no és possible, recopilar tota la informació pertinent sobre el problema per transferir-lo a l'nivell T3.
- Completar amb més informació i elements la incidència inicial.
- Tancar o reassignar consultes a altres nivells.
- Supervisar les eines disponibles per a la solució d'incidents.
- Examinar la informació disponible per al suport de primer nivell, entre d'altres.

C. Resoldre problemes amb Bases de Dades

Finalment, hi ha els especialistes de suport informàtic de nivell 3, que són el s professionals més capacitats per proporcionar serveis tècnics. Aquest suport nivell 3 també és anomenat suport de back-end o suport d'alt nivell. És el nivell més alt de suport en un sistema de suport tècnic, responsable de resoldre els problemes més difícils. Les funcions de l'equip que compon el suport tècnic informàtic de nivell 3 són:

- Administrar, actualitzar i desenvolupar bases de dades.
- Gestionar la xarxa i la infraestructura tècnica que fan servir empresa i clients.
- Realitzar reparacions al servidor.

D. Procediments i Eines per garantir un suport tècnic Alt.

Seguretat: A mesura que les amenaces cibernètiques evolucionen , eines amb mesures de seguretat robustes com la xifratge de punta a punta són essencials.

Facilitat d'ús: Interfícies intuïtives que requereixen una formació mínima
Son crucials per a l'adopció i l'eficàcia.

Suport mòbil: Les eines han de satisfer una varietat de dispositius, incloent-hi telèfons intel·ligents i tauletes.

F. Funcions essencials en un servei de suport tècnic.

Transmissió de dades segura
Comptabilitat Multi plataforma.
Funcionalitats de transferència de fitxers.
Compartició de pantalla en temps real.
Control remot.

Gravació de sessions.
Xat per comunicació instantània.

G. Eines de gestió d'incidències.

Thigh VNC AnyDesk, Teamviwer: Eines de control remot.

GLPI: Eina de gestió de serveis entres elles sistema de gestió d'incidències de codi obert.

Portal ATOM: Plataforma per notificar incidències d'equipaments digitals de la Generalitat.

5. Preguntes sobre el Directori Actiu (2 punts)

a) Què és el Directori Actiu i per a què serveix?

El Directori Actiu és un servei de xarxa de Microsoft que permet la gestió centralitzada de recursos, usuaris i dispositius en una xarxa. Serveix per autenticar i autoritzar tots els usuaris i equips en una xarxa de domini de Windows, assegurant que només els usuaris autoritzats tinguin accés als recursos.

b) Quina diferència hi ha entre un usuari de domini i un usuari local?

Un usuari de domini és un compte d'usuari que es crea i es gestiona en el Directori Actiu i pot accedir a recursos en tota la xarxa de domini. Un usuari local és un compte d'usuari que es crea i es gestiona en un ordinador específic i només pot accedir als recursos d'aquest ordinador.

c) Què és un controlador de domini?

Un controlador de domini és un servidor que respon a les sol·licituds d'autenticació de seguretat dins d'un domini de Windows. Emmagatzema les dades del Directori Actiu i gestiona les interaccions entre els usuaris i el domini.

d) Què són les Unitats Organitzatives (OU) i quin ús tenen?

Les Unitats Organitzatives (OU) són contenidors dins del Directori Actiu que s'utilitzen per organitzar usuaris, grups, equips i altres unitats organitzatives. Permeten aplicar polítiques de grup i delegar permisos administratius de manera més eficient.

e) Quines eines es poden utilitzar per gestionar usuaris en un entorn de domini?

Algunes eines que es poden utilitzar per gestionar usuaris en un entorn de domini inclouen la Consola de Gestió del Directori Actiu (ADUC), PowerShell, i altres eines de tercers com Hyena o ManageEngine ADManager Plus.

f) Què és una política de grup (GPO)?

Una política de grup (GPO) és una característica del Directori Actiu que permet als administradors definir configuracions de seguretat i comportament per als usuaris i equips dins d'un domini. Les GPO es poden aplicar a nivell de domini, unitat organitzativa o grup de seguretat.

g) Com es crea un usuari nou en el Directori Actiu?

Per crear un usuari nou en el Directori Actiu, es pot utilitzar la Consola de Gestió del Directori Actiu (ADUC). Cal fer clic amb el botó dret a la unitat organitzativa on es vol crear l'usuari, seleccionar 'Nou' i després 'Usuari'. A continuació, s'introdueixen les dades de l'usuari i es defineixen les propietats del compte.

h) Què és una política de contrasenya i com s'aplica?

Una política de contrasenya és una configuració que defineix els requisits de complexitat, longitud i caducitat de les contrasenyes dels usuaris. S'aplica mitjançant polítiques de grup (GPO) i es pot configurar a nivell de domini o unitat organitzativa.

Prova 2. Pràctica. Coneixements professionals

A l'Ajuntament de Palau-solità i Plegamans hi ha varis edificis connectats fer fibra òptica privada a la Casa Consistorial on estan els servidors. Entre aquests edificis hi ha el de la prefectura de la policia local el qual és molt crític ja que aquest servei sempre ha de donar resposta a la ciutadania. L'edifici de la policia local està connectat al de la Casa Consistorial per fibra òptica privada mitjançant un switch on estan connectats la resta de switch de l'edifici. Per aquesta fibra passen diversos serveis: sortida a Internet, xarxa privada, telefonia IP i càmeres de trànsit mitjançant varies VLAN.

Enumera plans de contingència a diferents nivells per garantir la continuïtat operativa dels serveis TIC essencials per a la prefectura de la policia local, tot assegurant una resposta ràpida i estructurada en cas d'incident tecnològic o de infraestructura.

Pla de Contingència TIC - Servei de Policia Local

1. Objectiu

Garantir la continuïtat operativa dels serveis TIC essencials per a la prefectura de la policia local, tot assegurant una resposta ràpida i estructurada en cas d'incident tecnològic o de infraestructura.

2. Àmbit d'aplicació

Aplica a la connexió i serveis TIC entre:
- Casa Consistorial (data center principal)

- Prefectura de la policia local

Serveis afectats:
- Xarxa de dades
- Telefonia IP
- Càmeres de trànsit
- Accés als servidors municipals
- Sistemes de seguretat i vigilancia
- Sortida a Internet

3. Riscos identificats

Risc	Impacte	Probabilitat	Mesures de contingència
Tall de connexió de fibra	Molt alt	Mitjana	Connexió redundant (fibra alternativa / 4G / radioenllaç)
Fallida del switch principal	Alt	Mitjana	Switch redundant en alta disponibilitat
Tall elèctric a l'armari de comunicacions	Molt alt	Alta	SAI + generador local + alerta remota
Fallida del servidor central	Alt	Baixa	Clúster Alta Disponibilitat + replicació remota
Ciberatac o ransomware	Molt alt	Mitjana	Antivirus, firewall, còpies de seguretat
Fallada de la telefonia IP	Alt	Mitjana	App SIP com a alternativa, centraleta local redundant
Caiguda del sistema de videovigilància	Mitjà	Mitjana	Gravació local temporal + sincronització posterior al núvol

4. Mesures de contingència per servei

Xarxa i infraestructura
- Fibra òptica redundant per recorreguts diferents.
- Connexió 4G/5G/ Radioenllaç o satèlit configurada amb failover automàtic.
- Supervisió contínua de l'estat dels enllaços.
- VLAN separades i priorització de trànsit (QoS).

Tall elèctric a l'armari de comunicacions
- Instal·lació d'un SAI (UPS) amb capacitat per alimentar switchs, punts d'accés i NVR durant 30-60 minuts.
- Connexió a generador elèctric de l'edifici (o generador portàtil específic per a emergències).
- Sensors de monitoratge remot de temperatura i energia.
- Alertes automàtiques a l'equip TIC i als responsables de manteniment.

Telefonia IP
- Centraleta telefónica / Servidor SIP redundant o funcionalitat local al firewall/ATA.
- Aplicació mòbil SIP com a alternativa per a telèfons crítics.
- Configuració de fallback a números mòbils en cas de caiguda de les línies de l'operador

Càmeres i videovigilancia
- Servidor NVR local a l'edifici de la policia amb còpia temporal.
- Càmeres amb targeta SD per gravació autònoma si cau la xarxa.
- Sincronització automàtica amb el servidor central quan torni la connexió.

Servidors i dades
- Servidors virtualitzats amb alta disponibilitat (HA) i rèplica al servidor remot al núvol.
- Còpies de seguretat automatitzades a local i al núvol.
- Proves mensuals de restauració i accés a còpies fora de línia.

5. Personal i protocols

Formació i simulacres
- Formació específica per al personal TIC i policial.
- Simulacres anuals de tall de serveis i resposta.
- Protocol d'escalat d'incidències per a cada cas.

Documentació i accés
- Manual d'actuació en cas de fallida TIC.
- Fitxes d'emergència en paper amb contactes i instruccions mínimes.
- Fitxes de servei mínim per continuar operant fora de línia si cal.

6. Monitoratge i resposta
- Sistema de monitoratge actiu 24/7 (Zabbix/PRTG).
- Alertes per correu i SMS a tècnics.
- Log d'incidències i temps de resposta.
- Reunions trimestrals de revisió i millora del pla.

7. Conclusions
El present pla assegura que la prefectura de la policia local pugui continuar oferint servei a la ciutadania en tot moment, minimitzant l'impacte de qualsevol fallada tecnològica, especialment amb l'addició de mesures contra talls elèctrics.