

Prova 1. Teòrica.

1-Avantatges de la certificació digital. (resposta A)

- A. Privadesa, integritat, autenticitat, confidencialitat, interoperabilitat, seguretat, validesa legal, accessibilitat.
- B. Privadesa, integritat, autenticitat, confidencialitat, seguretat, validesa legal, accessibilitat.
- C. Privadesa, integritat, autenticitat, confidencialitat, interoperabilitat, seguretat, validesa legal.
- D. Cap de les respostes anteriors és correcta.

Avantatges de la certificació digital

- Privadesa: garanteix la identificació de l'emissor. Només pot haver enviat la informació la persona que signa la comunicació.
- Integritat: la informació no es pot manipular durant la transmissió per part de cap persona no autoritzada.
- Autenticitat: garanteix que el document que ha rebut el receptor és l'original i pertany indiscutiblement a l'emissor. D'aquesta manera, ens permet garantir que l'emissor és el responsable del compromís adquirit per via telemàtica.
- Confidencialitat: una comunicació xifrada només pot ser llegida pel seu destinatari final i no pot haver estat manipulada.
- Interoperabilitat: es pot utilitzar un mateix certificat digital per autenticar-se en diferents plataformes i portals.
- Seguretat: és generat per un prestador de serveis de certificació reconegut i de confiança. Així mateix, en cas de pèrdua o robatori, es pot suspendre.
- Validesa legal: està emparat mitjançant la Llei 59/2003 de Signatura Electrònica, que en l'article 3 diu "la signatura electrònica reconeguda tindrà respecte a les dades consignades en forma electrònica el mateix valor que la signatura manuscrita en relació amb els consignats en paper".
- Accessibilitat: es pot accedir a la informació electrònica en qualsevol moment i es garanteix la perdurabilitat en el temps.

2-Quins són els mecanismes més comuns per gestionar el coneixement? (resposta C)

- A. Correu electrònic, programes amb dades personals i blogs.
- B. Comunitats virtuals i bases de dades.
- C. Correu electrònic, bases de dades, blogs i comunitats virtuals.
- D. Reunions, bases de dades i blogs.

Hi ha diversos mecanismes i eines per gestionar el coneixement. Els més comuns són l'e-Mail, les Bases de Dades, els Blogs i les Comunitats Virtuals.

3-Quines són les fases i l'ordre correcte per a la realització d'un projecte tecnològic? (resposta B)

- A. Cerca i selecció de la informació, identificació de la necessitat, generació de solucions, disseny del producte, organització i gestió dels treballs, planificació i execució i avaluació i perfeccionament.
- B. Identificació de la necessitat, cerca i selecció de la informació, generació de solucions, disseny del producte, organització i gestió dels treballs, planificació i execució i avaluació i perfeccionament.
- C. Cerca i selecció de la informació, identificació de la necessitat, generació de solucions, disseny del producte, organització i gestió dels treballs, avaluació i perfeccionament i planificació i execució.

D. Identificació de la necessitat, cerca i selecció de la informació, generació de solucions, disseny del producte, organització i gestió dels treballs, avaluació i perfeccionament i planificació i execució.

ETAPAS DE UN PROYECTO TECNOLÓGICO



4-En què consisteix la gestió del coneixement? (resposta A)

- A. En la implementació de processos i mecanismes que tenen per objectiu que el coneixement individual que posseeixen els/les professionals d'una organització, passi a formar part del coneixement col·lectiu de l'empresa.
- B. En la implementació de processos i mecanismes que tenen per objectiu que el coneixement col·lectiu que posseeixen els/les professionals d'una organització, passi a formar part del coneixement individual de cadascun.
- C. En la implementació de capacitats, habilitats i experiències individuals.
- D. Cap de les respostes anteriors és correcta.

Què és la Gestió del Coneixement? La Gestió del Coneixement consisteix en la implementació de processos i mecanismes que tenen per objectiu que el coneixement individual que posseeixen els/les professionals d'una organització, passi a formar part del coneixement col·lectiu de l'empresa.

5-Quins són els elements que intervenen en la gestió del coneixement? (resposta B)

- A. La cultura municipal, els membres del govern i les noves tecnologies.
- B. La cultura corporativa, els professionals, els processos i les noves tecnologies.
- C. Els processos i les noves tecnologies.

D. Cap de les respostes anteriors és correcta.

Com es Gestiona el Coneixement? Quatre són els elements que intervenen en la Gestió del Coneixement: la cultura corporativa, els/les professionals, els processos i les noves tecnologies.

6-Quins són tots els factors d'autenticació que marca l'ENS? (resposta C)

- A. Es poden combinar els dos següents: Contrasenyes i elements biomètrics.
- B. Només un dels tres següents: Alguna cosa que se sap, alguna cosa que es té, alguna cosa que s'és.
- C. Es poden combinar els tres següents: Alguna cosa que se sap, alguna cosa que es té, alguna cosa que s'és.
- D. Es poden combinar els tres següents: Contrasenyes, tokens i elements biomètrics.

Contenido

- 1 Medidas de seguridad
- 2 Selección de medidas de seguridad
- 3 Marco organizativo [op]
- 4 Marco operacional [op]
- 4.1. Purificación [op,2f]
- 4.2. Control de acceso [op,acc]
- 4.2.1. Identificación [op,acc,1]
- 4.2.2. Requisitos de acceso [op,acc,2]
- 4.2.3. Separación de funciones y tareas [op,acc,3]
- 4.2.4. Proceso de gestión de derechos de acceso [op,acc,4]
- 4.2.5. Mecanismo de autenticación [op,acc,5f]
- 4.2.6. Acceso local [op,acc,6]
- 4.2.7. Acceso remoto [op,acc,7]
- 4.3. Explotación [op,exp]
- 4.3.1. Inventario de activos [op,exp,1]
- 4.3.2. Configuración de seguridad [op,exp,2]
- 4.3.3. Gestión de la configuración [op,exp,3]
- 4.3.4. Mantenimiento [op,exp,4]
- 4.3.5. Gestión de cambios [op,exp,5]
- 4.3.6. Protección frente a código dañino [op,exp,6]
- 4.3.7. Gestión de incidentes [op,exp,7]
- 4.3.8. Registro de la actividad de los usuarios [op,exp,8]
- 4.3.9. Registro de la gestión de incidentes [op,exp,9]
- 4.3.10. Protección de los registros de actividad [op,exp,10]
- 4.3.11. Protección de claves criptográficas [op,exp,11]
- 4.4. Servicios externos [op,ext]
- 4.4.1. Contratación y acuerdos de nivel de servicio [op,ext,1]
- 4.4.2. Gestión diaria [op,ext,2]
- 4.4.3. Medios alternativos [op,ext,3]
- 4.5. Continuidad del servicio [op,cont]
- 4.5.1. Monitorización del sistema [op,mon,1]
- 4.5.2. Detección de intrusiones [op,mon,2]
- 4.5.3. Sistema de métricas [op,mon,3]
- 5. Medios de protección [op]
- 6. Osearrollo y cumplimiento de las medidas de seguridad
- 7. Interpretación

ANEXO III AUDITORIA DE LA SEGURIDAD

4.3.5. Mecanismo de autenticación [op,acc,5f]

dimensiones	
nivel	ICAT
	bajo medio alto
	simple +

Los mecanismos de autenticación frente al sistema se adecuan al nivel del sistema atendiendo a las consideraciones que siguen, pudiendo usarse los siguientes factores de autenticación:

- "algo que se sabe": contraseñas o claves concertadas.
- "algo que se tiene": componentes lógicos (tales como certificados software) o dispositivos físicos (en expresión inglesa, tokens).
- "algo que se es": elementos biométricos.

Los factores anteriores pueden utilizarse de manera aislada o combinarse para generar mecanismos de autenticación fuerte.

La guía CN-SITC desarrollará los mecanismos concretos adecuados para cada nivel.

Las instancias del factor o los factores de autenticación que se utilicen en el sistema, se denominarán credenciales.

Antes de proporcionar las credenciales de autenticación a los usuarios, estos deberán haberse identificado y registrado de manera fehaciente ante el sistema o ante un proveedor de identidad electrónica reconocido por la Administración. Se contemplarán varias posibilidades de registro de los usuarios:

- Mediante la presentación física del usuario y verificación de su identidad acorde a la legislación vigente, ante un funcionario habilitado para ello.
- De forma telemática, mediante DNI electrónico o un certificado digitalmente cualificado.
- De forma telemática, utilizando otros sistemas admitidos legalmente para la identificación de los ciudadanos de los contemplados en la normativa de aplicación.

Nivel BAJO

- a) Como principio general, se admitirá el uso de cualquier mecanismo de autenticación sustentado en un solo factor.
- b) En el caso de utilizarse como factor "algo que se sabe", se aplicarán reglas básicas de calidad de la misma.
 - c) Las credenciales se activarán una vez estén bajo el control efectivo del usuario.
 1. Las credenciales se activarán una vez estén bajo el control exclusivo del usuario.
 2. El usuario reconocerá que las ha recibido y que conoce y acepta las obligaciones que implica su tenencia, en particular, el deber de custodia diligente, protección de su confidencialidad e información inmediata en caso de pérdida.
 3. Las credenciales se cambiarán con una periodicidad marcada por la política de la organización, atendiendo a la categoría del sistema al que se accede.
 4. Las credenciales se retirarán y serán deshabilitadas cuando la entidad (persona, equipo o proceso) que autentica termina su relación con el sistema.

7-Quins d'aquests principis NO correspon a l'Esquema Nacional d'Interoperabilitat? (resposta B)

- A. La interoperabilitat com a qualitat integral.
- B. Seguretat integral.
- C. Caràcter multidimensional de la interoperabilitat.
- D. Enfocament de solucions multilaterals.

Article 4. Principis bàsics de l'Esquema Nacional d'Interoperabilitat.

L'aplicació de l'Esquema Nacional d'Interoperabilitat s'ha de desplegar d'acord amb els principis generals que estableix l'article 4 de la Llei 11/2007, de 22 de juny, i amb els principis específics de la interoperabilitat següents:

- a) La interoperabilitat com a qualitat integral.
- b) Caràcter multidimensional de la interoperabilitat.
- c) Enfocament de solucions multilaterals.

0-14

8-Quines categories s'avaluen en una auditoria en relació a l'Esquema Nacional d'Interoperabilitat? (resposta A)

- A. Marc organitzatiu, operacional i mesures tècniques.
- B. Marc organitzatiu, operacional i funcional.
- C. Marc organitzatiu, mesures tècniques i de seguretat.
- D. Mesures de protecció, tècniques i de seguretat.

Adequació a l'Esquema Nacional d'Interoperabilitat

Per a l'adequació a l'ENI és d'interès la Guia d'auditoria de compliment de l'ENI que té per objectiu facilitar que es pugui realitzar una valoració del compliment de les mesures d'interoperabilitat, assenyalant una llista de controls sobre l'Esquema Nacional d'Interoperabilitat. Aquests controls s'estructuren en tres categories seguint el model de l'ENS:

- › **Marco organitzatiu**, referit a aquells controls el compliment dels quals exigeix mesures horitzontals, com els aspectes jurídics, de polítiques d'actuació o determinades decisions, freqüentment referides a la governança de la interoperabilitat.
- › **Marco operacional**, referit a aquells controls el compliment dels quals requereix l'adopció de pràctiques, procediments i mesures alineades amb l'administració de la interoperabilitat com un conjunt, incloent el disseny, la implementació, la configuració i explotació de sistemes interoperables.
- › **Mesures tècniques**, que suposen requisits concrets que permeten garantir la interoperabilitat, incloent formats, vocabularis o protocols.

9-Les metadades de gestió de documents serveixen per: (resposta C)

- A. Identificar, autenticar i contextualitzar documents.
- B. Identificar, autenticar i contextualitzar a les persones, els processos i els sistemes que els creen, gestionen, mantenen i utilitzen.
- C. Les respostes A i B són correctes.
- D. Cap de les respostes anteriors és correcta.

Metadades de gestió de documents

La definició genèrica de 'metadada', segons figura en l'Esquema Nacional d'Interoperabilitat, és "dada que defineix i descriu altres dades". Existeixen diferents tipus de metadades segons la seva aplicació.

L'article article 42 del Reial decret 1671/2009², de 6 de novembre, en desenvolupar les disposicions comunes sobre els documents electrònics, defineix 'metadada' com "qualsevol tipus d'informació en forma electrònica associada als documents electrònics, de caràcter instrumental i independent del seu contingut, destinada al coneixement immediat i automatizable d'alguna de les seves característiques, amb la finalitat de garantir la disponibilitat, l'accés, la conservació i la interoperabilitat del propi document".

El Reial decret 4/2010 defineix també 'metadada de gestió de documents' com a "informació estructurada o semiestructurada que fa possible la creació, gestió i ús de documents al llarg del temps en el context de la seva creació. Les metadades de gestió de documents serveixen per identificar, autenticar i contextualitzar documents, i de la mateixa manera a les persones, els processos i els sistemes que els creen, gestionen, mantenen i utilitzen".

10-Quin servei es necessita per gestionar els dispositius mòbils? (resposta B)

- A. Exchange
- B. MDM
- C. VALid
- D. DRAC

11-Quines mesures de seguretat física cal tenir en compte en un CPD? (resposta D)

- A. Directives d'equip i/o usuari.
- B. Control d'accés a la sala.
- C. Sistema contra incendis i inundacions i control de temperatura i humitat.
- D. Les respostes B i C són correctes.

12- Quina és la funció del departament de Tecnologies de la Informació i Comunicació? (resposta D)

- A. Dissenyar, programar, planificar, executar i coordinar els programes a dur a terme dins del seu àmbit, proposant noves línies d'actuació als seus superiors.
- B. Elaborar els informes adients per les activitats desenvolupades, així com efectuar el seguiment d'aquestes, elaborant la memòria i pressupost anual del departament.
- C. Assessorar i donar suport tècnic només a nivell extern (institucions i usuaris en general) proporcionant informació sobre la matèria de la seva especialitat.
- D. Les respostes A i B són correctes.

FUNCIONS GENÈRIQUES:

- Dissenyar, programar, planificar, executar i coordinar els programes a dur a terme dins del seu àmbit, proposant noves línies d'actuació als seus superiors.
- Proposar el pressupost, gestionar i fer el seguiment de l'execució de les partides pressupostàries assignades determinant possibles desviacions i proposant ampliacions o modificacions de crèdit.
- Elaborar els informes adients per les activitats desenvolupades, així com efectuar el seguiment d'aquestes, elaborant la memòria i pressupost anual del departament.
- Assessorar i donar suport tècnic tant a nivell intern (la Corporació en general) com a nivell extern (institucions i usuaris en general) proporcionant informació sobre la matèria de la seva especialitat.

13- Quin servei dels següents NO ofereix el portal de l'AOC? (resposta B)

- A. Representa.
- B. Observatori TIC.
- C. e-NOTUM.
- D. iARXIU.

14- L'administració digital es caracteritza per tenir: (resposta A)

- A. Un abast global.
- B. Un abast individual.
- C. Un abast residual.
- D. No té cap abast.



Pregunta 2

CÓDIGO DE ADMINISTRACIÓN ELECTRÓNICA

§ 1

Nota del autor

Última modificación: 16 de diciembre de 2019

La transformación digital de la Administración, que da lugar a la denominada administración electrónica, o según el lenguaje más reciente, a la administración digital, es ineludible y se caracteriza por su alcance global, de forma que su plena realización requiere

15- Quins d'aquests noms corresponen a tipus de proves que podem trobar en els projectes informàtics de programari? (resposta A).

- A. Proves unitàries, funcionals, d'integració, de sistemes, de càrrega, d'acceptació, de regressió, de "fum".
- B. Proves unitàries, funcionals, d'integració, de sistemes, de càrrega, d'acceptació, de regressió.
- C. Proves unitàries, funcionals, d'integració, de sistemes, d'acceptació, de regressió, de "fum".
- D. Proves unitàries, funcionals, d'integració, de sistemes, de càrrega, de regressió, de "fum".

Tipus de proves

Existeixen molts tipus de proves que han de cobrir les especificacions d'un projecte informàtic a través dels procediments i dels casos de prova.

Tot seguit es presenta un resum d'aquests tipus de proves:

- **Tipus de proves unitàries.** Tenen les característiques següents:
 - Són el tipus de proves de més baix nivell.
 - Es duen a terme a mesura que es va desenvolupant el projecte.
 - Les efectuen els mateixos programadors.
 - Tenen com a objectiu la detecció d'errors en les dades, en els algorismes i en la lògica d'aquests.
 - Les proves unitàries es podran dur a terme segons un enfocament estructural o segons un enfocament funcional.
 - El mètode utilitzat en aquest tipus de proves és el de la capsula blanca o el de capsula negra.
- **Tipus de proves funcionals.** D'aquestes proves cal destacar:
 - Són les encarregades de detectar els errors en la implementació dels requeriments d'usuari.
 - Les duren a terme els verificadors i els analistes, és a dir, persones diferents a aquelles que han programat el codi.
 - S'efectuen durant el desenvolupament del projecte.
 - El tipus de mètode utilitzat és el funcional.
- **Tipus de proves d'integració.** Les seves característiques són les següents:
 - Es duren a terme posteriorment a les proves unitàries.
 - També les efectuen els mateixos programadors.
 - Es duen a terme durant el desenvolupament del projecte.
 - S'encarreguen de detectar errors de les interfícies i en les relacions entre els components.
 - El mètode utilitzat és el de capsula blanca, el de disseny descendent i el de *bottom-up*.

- **Tipus de proves de sistemes.** En destaca:
 - La seva finalitat és detectar errors en l'assoliment dels requeriments.
 - Les duren a terme els verificadors i els analistes, és a dir, persones diferents a aquelles que han programat el codi.
 - S'efectuen en una fase de desenvolupament del programari.
 - El tipus de mètode utilitzat és el funcional.
- **Tipus de proves de càrrega.** Les seves característiques principals són:
 - S'efectuen un cop acabat el desenvolupament, però abans de les proves d'acceptació.
 - També les realitzen analistes i verificadors.
 - Es comprova el rendiment i la integritat de l'aplicació ja acabada amb dades reals i en un entorn que també simula l'entorn real.
 - Es realitzen amb un enfocament funcional.
- **Tipus de proves d'acceptació.** Els aspectes més importants d'aquestes proves són els següents:
 - El seu objectiu és la validació o acceptació de l'aplicació per part dels usuaris.
 - És per això que les duren a terme els clients o els usuaris finals de l'aplicació.
 - Aquestes proves es duren a terme una vegada finalitzada la fase de desenvolupament. És possible fer-ho en la fase prèvia a la finalització i a la transferència o en la fase de producció, mentre els usuaris ja fan servir l'aplicació.
 - El tipus de mètode utilitzat també és el funcional.
 - Inclouen diferents tipus de prova. Entre altres, les proves alfa i les proves beta. En aquestes, el client realitza les proves a l'entorn del desenvolupador, al primer cas, i, al segon cas, en el propi entorn del client.
- **Tipus de proves de sistema.** Les característiques principals d'aquestes proves són:
 - Es realitzen després de les proves d'acceptació i amb el sistema ja integrat a l'entorn de treball.
 - La seva finalitat, precisament, és comprovar que aquesta integració és correcta.
 - L'enfocament utilitzat, lògicament, és el de capsa negra.
 - Les realitzen verificadors i analistes.
 - Inclou diferents tipus de prova. Entre altres, proves de rendiment, de resistència, de robustesa (davant entrades incorrectes), de seguretat, d'usabilitat i d'instal·lació.
- **Tipus de proves de regressió.** Les seves característiques principals són:
 - La seva finalitat és detectar possibles errors introduïts en haver realitzat canvis al sistema, bé per millorar-lo, bé per corregir altres errors.
 - Consisteixen bàsicament en repetir proves ja realitzades amb èxit abans de realitzar el canvi. Per tant, inclourà tant proves de capsa blanca com de capsa negra.
- **Tipus de proves "de fum".** Són proves ràpides de les funcions bàsiques d'un programari que normalment es realitzen després d'un canvi en el codi abans de registrar aquest codi modificat en la documentació del projecte.

16- Quins d'aquests estàndards corresponen a les xarxes WIFI i WIMAX?
(resposta A)

- A. WI-FI: 802.11 – WIMAX: 802.16.
- B. WI-FI: 802.16 – WIMAX: 802.11.
- C. WI-FI: 802.14 – WIMAX: 802.16.
- D. WI-FI: 802.16 – WIMAX: 802.14.

WiFi / WiMAX

WiFi

Wireless Fidelity (WiFi) es una norma que ha sido creada por el Instituto de Ingenieros Electrónicos y Eléctricos (IEEE) para reemplazar el equivalente de la capa física y lógica del estándar Ethernet (IEEE 802.3), por una tecnología que permita conexión inalámbrica en espacios reducidos. El estándar WiFi ha sido definido en la norma IEEE 802.11 y se creó como una tecnología de rápido despliegue, orientada a conectar equipos móviles y portátiles, reduciendo las complicaciones que presenta la utilización de cables para interconectar equipos de usuarios. Su ambiente de aplicación es de redes de área local, logrando distancias máximas de 150 metros en promedio.

Actualmente se utilizan 5 versiones de la norma que son: IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11a y IEEE 802.11ac (WiFi 5G) con velocidades de 11 Mbps, 54 Mbps, 300 Mbps, 54 Mbps y 1 Gbps respectivamente. La última versión, IEEE 802.11ac, ha sido aprobada en Enero 2014, por lo que aún no ha sido desplegada masivamente.

Al usar un medio compartido no guiado es importante tener en cuenta la seguridad de la información (Se deben aplicar técnicas de seguridad como WEP, WPA, WPA2, IPsec, Filtrado de MAC, etc.), y se debe analizar cada implementación en particular para poder identificar fuentes de interferencia, obstáculos en la transmisión, clientes esperados y esquemas de autenticación. La asociación Wi-Fi Alliance esta encargada de asegurar la compatibilidad total entre dispositivos certificados.

WiMAX

Worldwide Interoperability for Microwave Access (WiMAX) es una tecnología basada en el estándar IEEE 802.16, que ha sido diseñada principalmente como tecnología de "última milla", y se puede utilizar en enlaces de acceso, enlaces MAN y enlaces WAN. WiMAX permite brindar servicios de acceso de banda ancha, en cualquier momento, en cualquier lugar. Esta tecnología proporciona un esquema en el cual se pueden transportar otras tecnologías como IP, TDM, T1/E1, ATM, Frame Relay y voz, lo que posibilita su uso tanto en entornos de grandes redes corporativas como en ISPs que requieran utilizar enlaces inalámbricos para sus redes internas. WiMAX implementa diferentes niveles de calidad de servicio y diferentes canales de comunicación en cada enlace de radio, permitiendo también establecer comunicaciones sin visión directa entre las antenas (NLoS).

17- Quin d'aquests mètodes de planificació NO s'utilitza per representar gràficament un projecte? (resposta C)

- A. Diagrama de Gantt
- B. Mètode PERT
- C. Principi de Pareto
- D. Mètode Roy

Els mètodes més utilitzats per representar gràficament un projecte són:

- ✓ Gantt
- ✓ PERT
- ✓ Roy

18- De les respostes següents, quins es consideren tipus de còpies de seguretat? (resposta B)

- A. Anuals, mensuals, setmanals i diàries.
- B. Completa, incremental i diferencial.
- C. Les respostes A i B són correctes.
- D. Cap de les respostes anteriors és correcta.

– **Copia de seguridad completa:** como sugiere su nombre, este tipo de backup hace un respaldo completo de todos archivos del nuestro equipo.

El backup abarca el 100% de las informaciones, por lo que normalmente requiere más tiempo en realizarse y ocupa más espacio.

Si uno está seguro que quiere protegerlo todo por igual es la mejor solución.

– **Copia de seguridad diferencial:** únicamente contiene los archivos que han cambiado desde la última vez que se hizo la copia. Por lo tanto se incluyen sólo los archivos nuevos y/o modificados.

– **Copia de seguridad incremental:** se hace una copia de todos los archivos que han sido modificados desde que fue ejecutado el último backup completo, diferencial o incremental.

Es el método más rápido para realizar copias de seguridad.

19- En veu IP es mesura la qualitat del servei (QoS) amb els paràmetres següents: (resposta D)

- A. Ample de banda
- B. Latència
- C. Pèrdua de paquets
- D. Tots les respostes anteriors són correctes.

Calidad del servicio [editar]

Para mejorar el nivel de servicio, se ha apuntado a disminuir los anchos de banda utilizados, para ello se ha trabajado bajo las siguientes iniciativas:

- La supresión de silencios, otorga más eficiencia a la hora de realizar una transmisión de voz, ya que se aprovecha mejor el ancho de banda al transmitir menos información.
- Compresión de cabeceras aplicando los estándares RTP/RTCP.

Para la medición de la calidad de servicio QoS, existen cuatro parámetros como el ancho de banda, retraso temporal (delay), variación de retraso (jitter) y pérdida de paquetes.

20-Són principis bàsics, entre d'altres, de l'administració electrònica: (resposta A)

- A. El principi d'igualtat, accessibilitat, cooperació i neutralitat tecnològica.

- B. El principi d'igualtat, accessibilitat, cooperació i no neutralitat tecnològica.
- C. El principi d'igualtat, accessibilitat, informació restringida i neutralitat tecnològica.
- D. El principi d'igualtat, accessibilitat, publicitat de les dades de caràcter personal i neutralitat tecnològica.

Preguntes de reserva:

21-Quina de les característiques següents NO és pròpia d'un projecte? (resposta B)

- A. Necessita organització.
- B. És una activitat contínua i repetitiva.
- C. Necessita inversió de recursos.
- D. Té una finalitat específica.

22-Quin d'aquests tràmits o serveis NO es gestiona des del portal de l'EACAT? (resposta D)

- A. Via Oberta.
- B. Comunicacions a l'ORGT.
- C. Revocacions de certificats digitals.
- D. Totes les respostes anteriors són incorrectes.