Test Tema 80 #2

Actualizado el 13/04/2025

1. El modelo de información del directorio LDAP:

a) Describe cómo puede protegerse la información contenida en el directorio LDAP frente a accesos no autorizados

b) Describe qué operaciones pueden ser realizadas sobre la información almacenada en el directorio LDAP

c) Define la estructura de la información almacenada en el directorio LDAP

d) Describe cómo se organizan y referencian los datos

2. Juan necesita presentar en papel un documento firmado electrónicamente, ¿es correcto que imprima el documento y lo presente donde sea oportuno?

a) Sí, porque en el documento en papel aparece la firma manuscrita impresa.

b) Sí, siempre que el documento impreso incluya un mecanismo de validación CSV, como por ejemplo usar un CVE.

c) No, porque la firma electrónica es sólo para documentos electrónicos. Si quiero presentarlo luego en papel tendré que firmarlo a mano encima.

d) Sí, siempre que al imprimir en papel añada el logotipo del organismo que lo emite, que funciona como un sello.

3. ¿Cuál de los siguientes NO es un formato de firma electrónica?

a) CAdES

b) HAdES

c) PAdES

d) XAdES

4. Entre los objetivos del proyecto STORK 2.0 (Secure idenTity acrOss boRders linKed) NO se encuentra:

a) Construcción de pilotos o demostradores de servicios de administración electrónica.

b) Estudio de las especificaciones técnicas comunes que permitan el reconocimiento europeo de las eID (identidades electrónicas) nacionales.

c) Desarrollo de tecnologías y servicios avanzados de eID que sirvan de base para la construcción de la identidad electrónica europea única (eueID) prevista para 2020.

d) Realización de estudios sobre la situación legal y técnica de los sistemas de identificación y firma electrónica utilizados en los Estados Miembros.

5. Según la Ley 6/2020, de servicios electrónicos de confianza, los certificados electrónicos cualificados:

a) Confieren, por si mismos, a la firma electrónica avanzada la misma eficacia jurídica que a la manuscrita en relación con los datos consignados en papel.

b) Tienen una validez de 6 años como máximo.

c) Pueden identificar a las personas físicas para las que se expidan certificados a través de un seudónimo.

d) Solo son válidos para las personas jurídicas.

6. El Directorio X.500:

a) Es una base de datos centralizada y accesible desde cualquier punto

b) Es una base de datos distribuida y accesible desde cualquier punto

c) Está diseñado para guardar nombres, direcciones, pero no la información necesaria para localizar y establecer comunicación con una persona o recurso

d) B y C son ciertas

7. Según la recomendación XMLDsig de W3C, la firma digital de tipo enveloped signature cumple que:

a) La firma y el documento firmado son dos ficheros diferentes.

b) El documento firmado va dentro de la firma.

c) La firma va al final del documento firmado como un elemento adicional.

d) La firma se inserta en el primer elemento XML del documento.

8. En relación con los efectos jurídicos de las firmas electrónicas, indique la respuesta correcta:

a) No se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a una firma electrónica por el mero hecho de ser una firma electrónica o porque no cumpla los requisitos de la firma electrónica cualificada.

b) Una firma electrónica cualificada tendrá un efecto jurídico equivalente al de una firma manuscrita.

c) Una firma electrónica básica, como usuario y contraseña, puede ser prueba en juicio.

d) Todas son verdaderas.

9. El proyecto STORK es un:

a) Proyecto para conseguir el reconocimiento paneuropeo de las identidades electrónicas y, en concreto, la aceptación del DNI electrónico e identificadores similares en Servicios de Administración Electrónica de otras administraciones europeas.

b) Proyecto para conseguir la interoperabilidad del documento de identificación nacional entre los estados de la Unión Europea.

c) Proyecto para conseguir la interconexión de las redes administrativas europeas.

d) Proyecto para conseguir el reconocimiento paneuropeo de la definición y metadatos requeridos del documento electrónico, con el fin último de la interconexión de registros administrativos.

10. ¿Cuál de los siguientes tipos de información no está contenida obligatoriamente en un certificado digital X.509?

a) La clave pública del titular.

b) Datos personales de identificación del titular.

c) La URL del directorio LDAP contenedor de claves públicas.

d) La firma electrónica de la Autoridad de Certificación que emitió el certificado.

11. ¿A qué hace referencia el estándar LDAP?

a) Compresión de datos

b) Directorio electrónico

c) Certificados de clave pública

d) Protocolo de transporte OSI

12. ¿Cuál de las siguiente afirmaciones es cierta respecto a la firma electrónica?

a) La firma de documento se encuentra siempre dentro del documento original.

b) En los certificados de persona jurídica la identificación de la persona solicitante se incluye en el certificado electrónico.

c) La extinción de un certificado sólo puede ser por resolución judicial que lo ordene.

d) La extinción o suspensión de la vigencia de un certificado electrónico tendrá efectos retroactivos.

13. ¿Qué grupos de operaciones están definidas en el modelo funcional de LDAP?

a) De consulta, de actualización y de búsqueda

b) De búsqueda, de actualización y de control

c) De consulta, de actualización y de autenticación y control

d) De comparación, de consulta y de búsqueda

14. Infraestructura de PKI. La autoridad de certificación raíz:

a) No utiliza certificados digitales.

b) Utiliza un certificado digital firmado por otra autoridad de certificación.

c) Utiliza un certifica digital autofirmado por ella misma.

d) Utiliza un certificado digital emitido por la Administración Pública.

15. ¿Cuál de éstas es la codificación en formato binario de un certificado X.509v3?

a) DER

b) CERT

c) PME

d) Ninguno de los anteriores

16. De acuerdo con la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, señale la respuesta CORRECTA:

a) Para su identificación, los interesados podrán utilizar sistemas basados en certificados electrónicos cualificados de firma y sello electrónico expedidos por prestadores incluidos en las diferentes listas mantenidas por las Administraciones públicas.

b) Se podrán utilizar, para la identificación del interesado, sistemas de clave concertada y cualquier otro sistema, bajo determinadas condiciones y previa autorización por parte del Ministerio del Interior.

c) La aceptación de alguno de los sistemas de identificación por la Administración General del Estado no servirá para acreditar frente a todas las Administraciones Públicas la identificación electrónica de los interesados en el procedimiento administrativo.

d) Cuando los interesados utilicen un sistema de firma previsto en la Ley, su identidad se entenderá ya acreditada mediante el propio acto de la firma.

17. ¿Qué elemento NO forma parte del Servicio X.500 de OSI?

a) Agente de usuario del directorio (DUA)

b) Agentes del sistema de directorio (DSA)

c) Árbol de información del directorio (DIT)

d) Sistema de almacenamiento del directorio (DMS)

18. ¿A quién corresponde la potestad sancionadora según la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza?

a) La imposición de sanciones por el incumplimiento de lo previsto en esta Ley corresponderá, en el caso de infracciones muy graves, a la persona titular del Ministerio de Asuntos Económicos y Transformación Digital, y en el de infracciones graves y leves, a la persona titular de la Secretaría General de Administración Digital.

b) La imposición de sanciones por el incumplimiento de lo previsto en esta Ley corresponderá, en el caso de infracciones muy graves, a la persona titular del Ministerio de Asuntos Económicos y Transformación Digital, y en el de infracciones graves y leves, a la persona titular de la Secretaría de Estado de Digitalización e Inteligencia Artificial.

c) La imposición de sanciones por el incumplimiento de lo previsto en esta Ley corresponderá, en el caso de infracciones muy graves y graves, a la persona titular del Ministerio de Asuntos Económicos y Transformación Digital, y en el de infracciones leves, a la persona titular de la Secretaría de Estado de Digitalización e Inteligencia Artificial.

d) La imposición de sanciones por el incumplimiento de lo previsto en esta Ley corresponderá, en el caso de infracciones muy graves y graves, a la persona titular del Ministerio de Asuntos Económicos y Transformación Digital, y en el de infracciones leves, a la persona titular de la Secretaría General de Administración Digital.

19. Un servicio de directorio electrónico NO se caracteriza por:

a) ser flexible

b) Aceptar cierta inconsistencia temporal de la información en su replicación

c) Ser estático

d) Poder ser consultado y actualizado en línea

20. Los certificados cualificados de firma electrónica contendrán:

a) Al menos el nombre del firmante o un seudónimo; si se usara un seudónimo, se indicará claramente.

b) Los datos relativos al inicio y final del período de validez del certificado.

c) La localización de los servicios que pueden utilizarse para consultar el estado de validez del certificado cualificado.

d) Todas son verdaderas.

21. En relación a los servicios de directorio, señale la opción FALSA:

a) LDAP está basado en el estándar X.500.

b) eDirectory es un servicio de directorio desarrollado por Novell que está soportado por múltiples plataformas incluyendo Windows, NetWare, Linux.

c) Se accede con mucha frecuencia mediante operaciones de escritura, mientras que las operaciones de lectura son mucho menos frecuentes.

d) Un servicio de directorio es una herramienta que almacena y organiza de una manera clara y efectiva la información relativa a los usuarios, aplicaciones, archivos, impresoras y otros recursos accesibles dentro de una red.

22. En el ámbito de la Unión Europea, ¿tiene validez jurídica la firma electrónica?

a) Solamente si es firma reconocida

b) Solamente si es firma cualificada

c) Siempre será admisible como prueba en el procedimiento judicial

d) Ninguna de las anteriores es correcta

23. De los siguientes, indique la opción que contiene los modelos correctos contemplados por LDAP:

a) información; direccionamiento; observable; estructural

b) información; direccionamiento; objetivable; estructural

c) información; direccionamiento; seguridad; estructural

d) información; direccionamiento; seguridad; funcional

24. Indique cuál de las siguientes afirmaciones sobre directorios no es correcta:

a) La arquitectura X.500 se basa en la réplica de bases de datos distribuidas

b) El DAP es el protocolo de acceso al directorio X.500

c) X.500 fue diseñado como una versión simplificada de LDAP

d) Los programas acceden al directorio usando las APIs del X/Open Directory Service

25. De acuerdo con la Ley 6/2020 de servicios electrónicos de confianza, ¿cuál es el plazo máximo de validez de los certificados reconocidos para firma electrónica?

a) 3 años

b) 4 años

c) 5 años

d) 6 años

26. Según el Reglamento europeo de identificación electrónica y servicios de confianza (UE 910/2014), los prestadores cualificados de servicios de confianza que gestionen los datos de creación de firma electrónica en nombre del firmante:

a) Deben asegurar que los datos de creación de firma no se duplican bajo ningún concepto.

b) Podrán duplicar los datos de creación de firma únicamente con objeto de efectuar una copia de seguridad de dichos datos.

c) Podrán duplicar los datos de creación de firma únicamente con objeto de efectuar una copia de seguridad de dichos datos, sólo si la seguridad de los conjuntos de datos duplicados es del mismo nivel que para los conjuntos de datos originales.

d) Podrán duplicar los datos de creación de firma únicamente con objeto de efectuar una copia de seguridad de dichos datos, sólo si la seguridad de los conjuntos de datos duplicados es del mismo nivel que para los conjuntos de datos originales y además el número de conjuntos de datos duplicados no supera el mínimo necesario para garantizaria continuidad del servicio.

27. ¿Qué elemento NO forma parte de la norma X.500 de OSI?

a) Agente de usuario del directorio (DUA)

b) Árbol de información del directorio (DIT)

c) Dominio de nombres de directorio (DND)

d) Base de información del directorio (DIB)

28. Según la Ley 6/2020, de servicios electrónicos de confianza, ¿cuál de las siguientes NO es causa de extinción de la vigencia de un certificado?

a) Expiración del período de validez que figura en el certificado.

b) Solicitud formulada por el firmante, la persona física o jurídica representada por este, un tercero autorizado, el creador del sello o el titular del certificado de autenticación de sitio web.

c) Resolución judicial o administrativa que lo ordene.

d) Cese en la actividad del prestador de servicios de confianza cuando la gestión de los certificados electrónicos expedidos por aquel sea transferida a otro prestador de servicios de confianza.

29. Señale cuál de las siguientes opciones son tipos de cambios (chagetype) del formato ldif:

a) dn, objectClass, dc y top.

b) add, delete, moddn y modify.

c) new, del, change y tree.

d) -

30. El período de validez de los certificados cualificados no podrá ser superior a:

a) Tres años

b) Diez años

c) Dos años

d) Cinco años

31. Con respecto a la seguridad:

a) PGP basa su modelo en la existencia de una entidad de certificación

b) Si la entidad de certificación es de reconocido prestigio, no se necesita entidad de registro en PKI

c) El certificado digital contiene sólo la clave pública, no los datos del sujeto

d) Ninguna de las anteriores

32. Un archivo .PFX, de uso en certificados electrónicos:

a) Contiene la clave privada.

b) Cumple la sintaxis PKCS #21.

c) Está codificado en un formato no binario.

d) No se puede convertir a formato .PEM.

33. Marque la característica CORRECTA de LDAPv3:

a) Emplea ASN.1 para la representación de la información.

b) No soporta SASL para la capa de autenticación.

c) Define la estructura de la base de datos relacional que debe dar soporte al directorio.

d) Soporta el protocolo TLS para la transmisión segura de los datos.

34. Cuál de las firmas XAdES añade referencias a datos de verificación (certificados y listas de revocación) a los documentos firmados:

a) XAdES-BES

b) XAdES-T

c) XAdES-C

d) XAdES-EPES

35. Indique cuál de los siguientes términos NO corresponde a uno de los perfiles de firma PADES definidos en la norma técnica ETSI TS 102 778:

a) PADES-BES

b) PADES-STD

c) PADES-EPES

d) PADES-LTV

36. ¿Cómo se llama la Secretaría de Estado con competencia en materia de telecomunicaciones y a qué Ministerio está adscrita?

a) Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales del Ministerio de Asuntos Económicos y Transformación Digital

b) Secretaría de Estado de Telecomunicaciones y Sociedad de la Información del Ministerio de Asuntos Económicos y Transformación Digital

c) Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales del Ministerio de Ciencia e Innovación

d) Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital

37. Tras la entrada en vigor de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, qué normativa ha sido derogada?

a) Reglamento (UE) 910/2014

b) Ley 59/2003, de 19 de diciembre, de firma electrónica

c) Real Decreto 1553/2005

d) B y C son ciertas

38. ¿Cuál de los siguientes perfiles de XAdES incluye los certificados y listas de revocación (consultas OCSP o CRLs) para poder verificar el documento firmado en el futuro incluso si las fuentes originales no estuvieran disponibles?

a) XAdES-X.

b) XAdES-X-L.

c) XAdES-C.

d) Esta funcionalidad no se soporta en XAdES.

39. Señale la afirmación FALSA:

a) El Reglamento (UE) 910/2014 no prevé la emisión de certificados de firma electrónica a favor de personas jurídicas o entidades sin personalidad jurídica

b) Con la aprobación de la Ley 6/2020, de servicios electrónicos de confianza, queda derogado el Reglamento 910/2014

c) Con la aprobación de la Ley 6/2020, de servicios electrónicos de confianza, queda derogada la Ley 59/2003, de firma electrónica

d) A partir del 1 de julio de 2016 dejarán de emitirse certificados de firma electrónica de personas jurídicas y entidades sin personalidad jurídica, pudiendo en su lugar expedirse certificados de sello electrónico o certificados de firma de persona física representante

40. ¿Cuál de los siguientes elementos no es obligatorio en una firma CAdES-BES?

a) Definición del tipo de contenido

b) Resumen del mensaje

c) Sello de tiempo

d) Atributos identificativos del certificado del firmante

41. ¿Cuál no es una aplicación de LDAP?

a) Gestión de configuración

b) Seguridad

c) Correo Electrónico

d) Transmisión de ficheros

42. Los DN, en LDAP, se representan en:

a) XML

b) HTML

c) Texto plano

d) ASN.1

43. Los prestadores de servicios de certificación con carácter previo al cese definitivo de su actividad, ¿qué gestión deberán realizar?

a) Comunicarlo al organo de supervisión

b) Comunicarlo a sus clientes

c) Realizar la transferencia de los clientes a otro prestador cualificado

d) A y B son correctas

44. El Reglamento (UE) 910/2014, otorga la equivalencia funcional con la firma manuscrita respecto de los datos consignados en forma electrónica a:

a) La firma electrónica cualificada.

b) La firma electrónica avanzada.

c) La firma electrónica reconocida.

d) La firma electrónica autenticada.

45. Suponga que recibe una firma electrónica avanzada de tipo XAdES-T sin una asociación específica a ninguna política de firma concreta y que ha verificado con éxito el formato de la firma y su integridad. En esta situación, la evaluación de la validez de dicha firma electrónica según la norma ETSI TS 101 903 v1.3.2 da como resultado:

a) Firma inválida.

b) Validación incompleta de la firma.

c) Firma válida.

d) Firma suspendida.

46. La entidad encargada de la generación de los sellos de tiempo es:

a) Time Public Key Infraestructure

b) Time Certificate Authority

c) Time Stamp Authority

d) Time Scrow Infraestructure

47. Indique la respuesta correcta que resume el funcionamiento de la firma digital con criptografía de clave pública, garantizando autenticidad del origen, el no repudio en origen y la integridad:

a) El emisor calcula un hash del mensaje, lo cifra con su clave pública y transmite el criptograma resultante (firmjunto al mensaje. El receptor utiliza la clave privada del emisor para descifrar el criptograma.

b) El emisor calcula un hash del mensaje, lo cifra con su clave privada y trasmite el criptograma resultante (firma) junto al mensaje. El receptor utiliza su clave privada para descifrar el criptograma

c) El emisor calcula un hash del mensaje, lo cifra con su clave pública y transmite el criptograma resultante (firma) junto al mensaje. El receptor utiliza su clave privada para descifrar el criptograma

d) El emisor calcula un hash del mensaje, lo cifra con su clave privada y transmite el criptograma resultante (firma) junto al mensaje. El receptor utiliza la clave pública del emisor para descifrar el criptograma

48. La Tercera Parte de Confianza (TPC) de un entorno de clave pública, que se encarga de legitimar la relación de una clave pública con la identidad de un usuario o servicio es:

a) Autoridad de Certificación (AC)

b) Autoridad de Validación (AV)

c) Autoridad de Registro (AR)

d) Autoridad de Revocación (AR)

49. Si el usuario A desea enviar un documento firmado digitalmente por él al usuario B:

a) El usuario A debe enviar el documento acompañado del documento cifrado con la clave pública de B.

b) El usuario A debe enviar el documento acompañado del resultado de aplicar la función hash al documento y éste cifrado con la clave pública de B.

c) El usuario A debe enviar el documento acompañado del resultado de aplicar la función hash al documento y éste cifrado con la clave privada de A.

d) El usuario A debe enviar el documento cifrado con la clave pública de B acompañado del resultado de aplicar la función hash al documento y todo cifrado con la clave privada de A.

50. Son sistemas de firma para la actuación administrativa automatizada:

a) El sello electrónico.

b) El código seguro de verifcación.

c) Los dos anteriores.

d) Ninguno de los anteriores.

51. Entre los requisitos de la firma electrónica avanzada no se encuentra:

a) Que esté vinculada al firmante de manera única y permita su identificación.

b) Que haya sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo.

c) Que haya sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, siempre bajo su control exclusivo.

d) Que esté vinculada con los datos firmados de modo que detecte cualquier modificación ulterior.

52. La organización de la información en un servicio de directorio es:

a) relacional

b) indexada

c) jerárquica

d) en colas

53. El Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior establece:

a) La norma reguladora de los certificados de sede electrónica en la Unión Europea.

b) Cinco años como el periodo máximo de vigencia de los certificados electrónicos.

c) La plena prohibición del uso de seudónimos en el uso de las transacciones electrónicas.

d) La regulación del certificado de sello electrónico y su uso en los servicios públicos.

54. Indique cuál de las siguientes afirmaciones no es correcta según lo establecido en el Reglamento (UE) 910/2014:

a) Las firmas electrónicas cualificadas tendrán un efecto jurídico equivalente al de una firma manuscrita.

b) Una firma electrónica cualificada basada en un certificado cualificado emitido en un Estado miembro será reconocida como firma electrónica cualificada en los demás Estados miembros.

c) Las firmas electrónicas cualificadas tendrán una validez de 48 meses.

d) No se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a una firma electrónica por el mero hecho de ser una firma electrónica.

55. Según establece la Ley 6/2020, de servicios electrónicos de confianza, los certificados electrónicos cualificados pueden tener un periodo máximo de validez de:

a) Dos años

b) Tres años

c) Cuatro años

d) Cinco años

56. ¿Qué es una firma secuencial?

a) Un documento que incluye las firmas de varios usuarios, todas ellas sobre el mismo documento original

b) Un documento que incluye las firmas de varios usuarios, cada una de ellas incluyendo las firmas anteriores en el tiempo

c) Un documento que incluye la firma de un usuario, y uno o varios documentos originales

d) Un documento que contiene un documento original, la firma de uno o varios usuarios, y uno o varios sellos de tiempo

57. El perfil de XAdES en el que se añaden los certificados a los documentos firmados es:

a) XAdES LTA-Level

b) XAdES B-Level

c) XAdES LT-Level

d) XAdES T-Level

58. En relación al servicio de directorio LDAP, es CIERTO:

a) LDAP representa la información mediante estructuras ASN.1.

b) La unidad básica de información almacenada en el directorio es el atributo.

c) La operación Abandon permite cerrar la sesión.

d) LDAP utiliza TCP/IP en lugar de los protocolos OSI.

59. Según la recomendación X.509 v.3:

a) Un usuario puede tener a lo sumo un certificado de atributos por cada certificado de clave pública.

b) Los certificados de atributos deben ser generados por Autoridades de Certificación.

c) Para su validez, los certificados de atributos deben estar siempre acompañados de un certificado de clave pública.

d) Los certificados de atributos contienen idénticos campos que subcampos tiene el campo de extensiones de los certificados de clave pública.

60. Entre las siguientes opciones, ¿cuál es un estándar para firma electrónica?

a) WAdES

b) PdES

c) XAdES

d) CdES

61. En los servicios de directorio:

a) varias entradas pueden compartir un DN

b) las operaciones de actualización de LDAP no son atómicas

c) LDAP utiliza habitualmente la pila de protocolos TCP / IP

d) LDAP no se describe en términos de ASN.1

62. Cuando se obtiene un certificado electrónico cualificado en tarjeta, la clave privada generada se queda en:

a) El navegador de internet

b) La tarjeta criptográfica

c) A y B

d) B y el proveedor de servicios

63. Indique cuál de los siguientes no es uno de los requisitos que debe cumplir una firma electrónica avanzada según el Reglamento (UE) 910/2014:

a) Estar vinculada al firmante de manera única

b) Haber sido creada utilizando un dispositivo avanzado de creación de firmas electrónicas

c) Haber sido creada utilizando datos de creación de firma que el firmante puede utilizar, con un alto nivel de confianza, bajo su exclusivo control

d) Estar vinculada con los datos firmados, de modo tal que cualquier modificación ulterior de los mismos sea detectable

64. Referente a la Recomendación del W3C: XML Signature Syntax and Processing, ¿cuál es la afirmación INCORRECTA?

a) Sólo es posible indicar el uso del algoritmo C14N en el elemento ds:SignedInfo.

b) Explica tres posibles formas de aplicación de la firma: detached, enveloping y enveloped.

c) Permite firmar documentos en cualquier formato, no sólo en formato XML.

d) Es la base para la definición de XAdES.

65. Un prestador de servicios de certificación, ¿durante qué período de tiempo tiene que conservar la información relativa a los certificados reconocidos expedidos, de manera que puedan verificarse las firmas efectuadas con los mismos, de acuerdo a lo dispuesto en la Ley 6/2020, de servicios electrónicos de confianza?

a) Al menos durante 15 años contados desde la extinción del certificado

b) Al menos durante 15 años contados desde la expedición del certificado.

c) Un máximo de 15 años contados desde la extinción del certificado

d) Un máximo de 15 años contados desde la expedición del certificado

66. Respecto a los servicios de Directorio Electrónico, la norma X.500 de la UIT-T define cuatro tipos de clases de objetos de acuerdo a su funcionalidad:

a) Auxiliar, Estructural, Simplificada, Alias.

b) Estructural, Simplificada, Auxiliar, Alias.

c) Abstracta, Esquemática, Estructural, Alias.

d) Abstracta, Estructural, Auxiliar, Alias.

67. Indique cómo se denomina el formato binario que permite almacenar una cadena de certificados y una clave privada en un único archivo cifrado:

a) PKCS#7

b) PKCS#10

c) PKCS#11

d) PKCS#12

68. Según la Ley 6/2020, de servicios electrónicos de confianza, los certificados electrónicos cualificados:

a) Tienen una validez de tres años como máximo.

b) Pueden identificar a las personas físicas para las que se expidan certificados a través de un seudónimo.

c) Dejan de tener validez cuando expiran, y/o son revocados, por resolución judicial o por fallecimiento del firmante.

d) Confieren, por sí mismos, a la firma electrónica avanzada la misma eficacia jurídica que a la manuscrita.

69. Señale cuál de las siguientes formas de actuación es la especificada para los sistemas de validación de certificados de clave pública ITU-T X.509 v3:

a) Si el sistema no reconoce una extensión crítica, debe ignorar la extensión y emitir un mensaje advirtiendo la existencia de una extensión crítica no procesable.

b) Si el sistema reconoce una extensión no crítica, debe procesar la extensión y emitir un mensaje indicando su cumplimiento o no.

c) Si el sistema no reconoce una extensión no crítica, debe ignorar la extensión.

d) Si el sistema reconoce una extensión no crítica, es aceptable tanto ignorar como procesar la extensión (dependerá de la implementación concreta del sistema).

70. Los requisitos de seguridad aplicables a los prestadores de servicios de confianza:

a) Son diferentes para los prestadores de servicios de confianza cualificados y para los no cualificados.

b) Notificarán al organismo de supervisión en un plazo máximo de 48 horas, de cualquier violación de seguridad o pérdida de integridad.

c) En caso de que una violación de la seguridad afecte a dos o más Estados miembros, el organismo de supervisión notificado informará al respecto a los organismos de supervisión de los demás Estados miembros y a ENISA.

d) Todas son verdaderas.

71. De acuerdo al Reglamento (UE) 910/2014 sobre identificación electrónica y servicios de confianza (eIDAS), los dispositivos cualificados de creación de firma electrónica:

a) Podrán alterar los datos que deben firmarse si así lo requiere el proceso.

b) Impedirán que dichos datos se muestren al firmante antes de firmar.

c) Garantizarán razonablemente la confidencialidad de los datos de creación de firma electrónica utilizados para la creación de firmas electrónicas.

d) Podrán aparecer los datos de creación de firma electrónica utilizados para la creación de firma electrónica tantas veces como sea necesario en la práctica.

72. ¿Requieren de firma electrónica los documentos electrónicos emitidos por las Administraciones Públicas que se publiquen con carácter meramente informativo, así como aquellos que NO formen parte de un expediente administrativo?

a) No, pero es necesario identificar el origen de estos documentos

b) Sí, siempre

c) Únicamente en los casos en que deban ser objeto de publicación

d) Únicamente si se firman por el titular de un órgano administrativo

73. Señale la correcta:

a) El protocolo X.500 es un estándar de la IETF

b) El estándar de certificados digitales X.509 v3 introdujo el concepto de extensión

c) El protocolo LDAP de la ITU dispone su información relacionada jerárquicamente

d) Ninguna de las anteriores

74. Según el Principio de Reconocimiento Mutuo que establece el Reglamento (UE) 910/2014, se reconocerá en un Estado miembro, a efectos de la autenticación transfronteriza para un servicio en línea, el medio de identificación electrónica expedido en otro Estado miembro, siempre que:

a) El nivel de seguridad de este medio de identificación electrónica corresponda a un nivel igual o superior al requerido por el organismo del sector público para acceder a dicho servicio en línea, independientemente del nivel de seguridad del medio de identificación.

b) El medio de identificación esté expedido según los incluidos en la lista publicada por la Comisión.

c) Las respuestas A) y B) son correctas.

d) Este reconocimiento se producirá a más tardar 6 meses después de que la Comisión publique la lista.

75. ¿Cuál de los siguientes términos no está relacionado con un directorio LDAP?

a) DIT

b) WMI

c) DN

d) RDN

76. La firma digital de un mensaje o documento, garantiza:

a) La autenticación del emisor e integridad del mensaje.

b) La autenticación del emisor y confidencialidad del envío.

c) Autenticación, confidencialidad e integridad.

d) Confidencialidad del envío e integridad del mensaje.

77. Una ciudadana de nacionalidad argentina necesita presentar en papel un documento firmado electrónicamente, ¿es correcto que imprima el documento y lo presente donde sea oportuno?

a) Sí, siempre que al imprimir en papel añada el logotipo del organismo que lo emite, que funciona como un sello.

b) Sí, porque en el documento en papel aparece la firma manuscrita impresa.

c) Sí, siempre que el documento impreso incluya un mecanismo de validación CSV, como por ejemplo usar un CVE.

d) No, porque la firma electrónica es sólo para documentos electrónicos. Si quiere presentarlo luego en papel tendrá que firmarlo a mano encima.

78. En la Ley 6/2020, de servicios electrónicos de confianza, se indica que la prestación de servicios electrónicos de confianza no cualificados:

a) Está sujeta a autorización previa por parte del organismo europeo de supervisión

b) Está sujeta a autorización previa por parte del Ministerio de Asuntos Económicos y Transformación Digital

c) No está sujeta a autorización previa.

d) Está sujeta a autorización previa por parte de la Secretaría de Estado de Digitalización e Inteligencia Artificial

79. En relación con un Prestador de Servicios de Certificación (PSC) es cierto que:

a) Es una persona jurídica que expide certificados

b) Es una persona física o jurídica que expide certificados

c) Es una persona física o jurídica que expide certificados u otros servicios relacionados con la firma electrónica

d) Es una persona jurídica que expide certificados u otros servicios relacionados con la firma electrónica

80. ¿Cuál de los siguientes campos NO se encuentra en un certificado electrónico que siga el estándar X.509?

a) Nombre del certificador.

b) Período de validez.

c) Clave pública del sujeto.

d) Clave privada del sujeto.

81. Indique la respuesta correcta: El CSV es…

a) Una organización que establece estándares de usabilidad de aplicaciones.

b) Consejo Superior de Vigilancia: contribuye a la mejora de la ciberseguridad española.

c) Un tipo de firma de un documento electrónico.

d) Una aplicación móvil multiplataforma.

82. Según la Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados, el proceso de identificación se interrumpirá o no se considerará válido cuando concurran las siguientes circunstancias. Señale la opción FALSA:

a) Existan indicios de falta de correspondencia entre el titular del documento y el solicitante

b) Existan indicios de uso de archivos pregrabados

c) Existan indicios de que el solicitante está siendo coaccionado o intimidado

d) Existan indicios de que para la transmisión de vídeo no se han utilizado varios dispositivos

83. Indique la afirmación correcta respecto a XAdES-T:

a) Contiene la forma básica de firma que cumple los requisitos legales de la Directiva para firma electrónica avanzada, información sobre la política de firma (opcional) y añade un campo de sellado de tiempo para proteger contra el repudio.

b) Es la forma básica de firma a la que se la ha añadido información sobre la política de firma.

c) Añade a la forma básica de firma la posibilidad de timestamping periódico de documentos archivados para prevenir que puedan ser comprometidos debido a la debilidad de la firma durante un periodo largo de almacenamiento.

d) Añade sellos de tiempo a las referencias introducidas por XAdES-C para evitar que pueda verse comprometida en el futuro una cadena de certificados.