Test Tema 80 #1

Actualizado el 13/04/2025

1. Señale el ámbito de aplicación del Reglamento (UE) 910/2014:

a) A los sistemas de identificación electrónica notificados por los Estados miembros y a los prestadores de servicios de confianza establecidos en la Unión

b) Exclusivamente a los sistemas de identificación electrónica notificados por los Estados miembros

c) A los prestadores de servicios de certificación de la Unión cuyos Gobiernos acepten formalmente el Reglamento

d) Exclusivamente a los sistemas de identificación electrónica de los Estados miembros, independientemente de que hayan sido notificados

2. La especificación PKCS que define el formato de las claves privadas es:

a) PKCS 1

b) PKCS 5

c) PKCS 8

d) PKCS 6

3. ¿Cuál de los siguientes atributos de un certificado X.509 es relevante para establecer la confianza en la autenticidad de lo que representa?

a) la longitud de la clave privada.

b) el algoritmo de hash.

c) el Distinguished Name.

d) la política de certificación asociada.

4. Los certificados electrónicos de representante que actualmente emite la FNMT-RCM son:

a) Sólo los de personas jurídicas.

b) Sólo para entidades sin personalidad jurídica y para personas jurídicas.

c) Para entidades sin personalidad jurídica, para personas jurídicas y para administrador único o solidario.

d) Sólo para entidades sin personalidad jurídica.

5. ¿Cuál de las siguientes garantías NO corresponde a una firma digital?

a) El emisor de la firma es real y existe

b) El emisor no puede negar que firmó el documento

c) Se puede descargar una copia del documento a través de un identificador

d) El documento no ha sido alterado desde su firma

6. Según el Reglamento (UE) 910/2014 del Parlamento europeo y del Consejo, indique en cuáles de los siguientes estados se puede encontrar un certificado cualificado de firma electrónica durante su periodo de validez:

a) Activo y revocado.

b) Activo, revocado y suspendido.

c) Activo, revocado y prorrogado.

d) Activo, revocado y extraviado.

7. La diferencia entre la cofirma y la contrafirma estriba en que:

a) La cofirma ocurre cuando el documento a firmar se considera validado con la firma de uno sólo de los dos firmantes y la contrafirma cuando el documento es válido sólo si lo firman los dos a la vez

b) La cofirma y la contrafirma son iguales si se hacen de forma electrónica ya que no hay manera de determinar en el tiempo el orden de los firmantes, sólo que hayan firmado

c) En la cofirma los dos firmantes pueden firmar en cualquier momento y se supone que están al mismo nivel de responsabilidad respecto de la firma del documento (por ejemplo, una pareja que se compra una casa y firma la hipoteca) mientras que en la contrafirma el orden de los firmantes es relevante y el que firma último valida la firma del que ha firmado primero (por ejemplo, un jefe que valida el acto administrativo que firma un subordinado)

d) La cofirma requiere de la firma de dos sujetos físicos o jurídicos mientras que la contrafirma requiere de la firma de la aplicación que genera los certificados del documento (portafirmas)

8. ¿Cuál de los siguientes formatos de firma permite la adición de sellos de tiempo periódicos para garantizar la integridad de la firma archivada?

a) AdES - T

b) AdES - XL

c) AdES - A

d) AdES C

9. Los certificados digitales(digital IDs) están definidos en:

a) RSA Public Key Structure

b) X.509v3 de ITU

c) RFC 1661 de IAB

d) Verisign doc 1992/21

10. Respecto a la firma electrónica, según el Reglamento eIDAS (Reglamento UE 910/2014), indique la afirmación INCORRECTA:

a) Firma electrónica cualificada es una firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica.

b) Una firma electrónica avanzada estará vinculada al firmante de manera única.

c) Una firma electrónica avanzada deberá permitir la identificación del firmante.

d) Una firma electrónica avanzada tendrá un efecto jurídico equivalente al de una firma manuscrita.

11. Indique cuál es la Directiva europea que queda derogada por el Reglamento (UE) 910/2014:

a) Directiva 95/46/CE

b) Directiva 1999/93/CE

c) Directiva 2000/31/CE

d) Directiva 2003/98/CE

12. Indique el puerto utilizado por el protocolo LDAP sobre SSL:

a) 563

b) 443

c) 336

d) 636

13. Conforme a la Ley 6/2020, de servicios electrónicos de confianza, el prestador de servicios de certificación que vaya a cesar en su actividad deberá comunicarlo a los clientes a los que preste sus servicios y al órgano de supervisión con una antelación mínima de:

a) Al menos seis meses.

b) Un año natural.

c) Al menos dos meses.

d) Al menos dos semanas.

14. Si Alice quiere transmitir un documento cifrado (sin autenticación) hacia Bob utilizando un algoritmo de clave asimétrica:

a) Debe cifrarlo con la clave pública de Bob

b) Debe cifrarlo con la clave privada de Bob

c) Debe cifrarlo con la clave privada de Alice

d) Debe cifrarlo con la clave pública de Alice

15. ¿Según el Reglamento (UE) 910/2014, cuál de éstos son requisitos de seguridad de los TSP (Trust Service Providers)?

a) Notificar las violaciones al Ministerio de Asuntos Económicos y Transformación Digital en un máximo de 24 horas.

b) Mantener una base de datos de certificados.

c) Publicar las revocaciones en un máximo de 24 horas tras la solicitud.

d) Todas las anteriores.

16. Según el Reglamento (UE) 910/2014 del Parlamento europeo y del Consejo, indique cuál de los siguientes tipos de firma electrónica tiene efecto jurídico equivalente al de una firma manuscrita:

a) Firma biométrica digitalizada.

b) Firma electrónica certificada.

c) Firma electrónica cualificada.

d) Firma electrónica avanzada.

17. Señale cómo se denomina el proceso que administra el almacenamiento en un sistema de directorio electrónico:

a) DSA

b) UPN

c) DSE

d) DAP

18. Indique cuál de las siguientes afirmaciones con respecto al sellado de tiempo es correcta:

a) Es una firma electrónica realizada por una TSA que nos permite demostrar que los datos suministrados han existido y no han sido alterados desde un instante específico en el tiempo.

b) Es una firma electrónica realizada por una TSA que nos permite demostrar que un documento electrónico ha sido firmado en un momento en el tiempo concreto.

c) Es una firma electrónica realizada por una TSA que garantiza fehacientemente la fecha y hora de una sede electrónica.

d) Es una firma electrónica sincronizada con el ROA que garantiza fehacientemente la fecha y hora de una sede electrónica.

19. El protocolo de acceso al directorio en X.500 es:

a) TCP/IP

b) LDAP

c) IMAP

d) DAP

20. ¿Qué elemento de X.500 es el conjunto de toda la información disponible en el Servicio de Directorio?

a) DIB

b) DSA

c) DUA

d) DISP

21. El Reglamento de Ejecución UE 2015/1502 define las especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de los medios de identificación electrónicos. En particular, define el factor de autenticación inherente como:

a) Aquél que se basa en un atributo físico de una persona física del cual el sujeto está obligado a demostrar su posesión.

b) Aquél en el que el sujeto está obligado a demostrar conocimiento del mismo.

c) Aquél en el que se utilizan dos o más factores para comprobar la identidad del sujeto.

d) Aquél en el que el sujeto está obligado a demostrar posesión del mismo.

22. Si quiero enviar un mensaje cifrado a otra persona utilizando claves asimétricas para evitar que sea leído por terceros:

a) Lo encriptaré con mi clave privada para que él lo descifre utilizando mi clave pública.

b) Lo encriptaré con su clave privada para que él lo pueda descifrar utilizando su clave pública.

c) Lo encriptaré con mi clave pública para que él lo descifre utilizando mi clave privada.

d) Lo encriptaré con su clave pública para que él lo pueda descifrar utilizando su clave privada.

23. El período de tiempo durante el que los prestadores cualificados de servicios electrónicos de confianza deberán conservar la información relativa a los servicios prestados de acuerdo con el artículo 24.2.h) del Reglamento (UE) 910/2014:

a) Será de 10 años desde la emisión del certificado.

b) Será de 5 años desde la extinción del certificado o la finalización del servicio prestado.

c) Será de 15 años desde la extinción del certificado o la finalización del servicio prestado.

d) Será de 10 años desde el inicio del servicio prestado.

24. Según se establece en el reglamento eIDAS, Reglamento (UE) 910/2014, en su artículo 22, las listas de confianza las publicará, firmadas o selladas electrónicamente, y en una forma apropiada para el tratamiento automático:

a) La Comisión Europea.

b) Cada Estado miembro de la Unión Europea.

c) El Parlamento Europeo.

d) El Consejo de la Unión Europea.

25. El Reglamento (UE) 910/2014 entra en vigor:

a) Al día siguiente de su publicación en el Diario Oficial de la Unión Europea (DOUE)

b) A los 20 días de su publicación en el Diario Oficial de la Unión Europea (DOUE)

c) A partir del 1 de enero de 2015

d) A partir del 1 de julio de 2016

26. Según el artículo 26 del Reglamento 910/2014: una firma electrónica que está vinculada al firmante de manera única, que permite la identificación del firmante, que ha 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, y que está vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable, es una:

a) Firma electrónica cualificada

b) Firma electrónica avanzada

c) Firma electrónica reconocida

d) Firma electrónica validada

27. Completa la frase: A diferencia de NIS, LDAP …

a) No está restringido a redes UNIX

b) Usa notación ASN.1

c) No soporta implementaciones de software libre

d) Se usa sobre TCP/IP

28. Respecto a los ficheros de firma electrónica y los documentos firmados electrónicamente, señale la respuesta correcta:

a) El documento firmado siempre va incluido en el fichero de firma, tanto en XAdES como en CAdES.

b) En CAdES, el documento puede no incluirse en el fichero de firma. Estas firmas se llaman explícitas.

c) El documento firmado se incluye en el fichero de firma en XAdES, y no se puede incluir en CAdES.

d) En XAdES, sólo se puede firmar de forma implícita, en la que el documento no se incluye en el resultado de firma y solamente se incluye una referencia al lugar en el que se encuentra.

29. Señale cuál de los siguientes no es uno de los contenidos de los certificados cualificados de firma electrónica según el Reglamento (UE) 910/2014:

a) El nombre del firmante o un seudónimo

b) Los datos de validación de la firma electrónica

c) La firma electrónica cualificada o el sello electrónico cualificado del prestador de servicios de confianza expedidor

d) La localización de los servicios que se pueden utilizar para consultar el estado de validez del certificado

30. ¿Cuál de las siguientes afirmaciones referentes a un sistema criptográfico de clave pública o asimétrico es falsa?

a) La clave privada del emisor es la usada para garantizar la confidencialidad.

b) La criptografía de clave pública se usa para la implantación de servicios de seguridad avanzados como: autenticidad (firma digital), no repudio e integridad entre otros.

c) El uso de criptografía de clave pública, para servicios de confidencialidad, proporciona un rendimiento muy inferior (caracteres cifrados/segundo) al proporcionado por los algoritmos simétricos.

d) La gestión de claves de los sistemas criptográficos asimétricos es más sencilla que la existente en los sistemas convencionales simétricos de clave secreta.

31. En relación con los prestadores de servicios de confianza cualificados, la Autoridad de Validación:

a) Presta un servicio de comprobación de la vigencia de un determinado certificado

b) Habitualmente coincide con la Autoridad de Certificación

c) Es la encargada de revocar el certificado antes de su caducidad cuando deja de tener validez

d) Es la encargada de verificar la identidad del titular de forma previa a la expedición del certificado

32. En relación con la identificación electrónica, señale la respuesta CORRECTA:

a) El Reglamento (UE) 910/2014 prevé los siguientes niveles de aseguramiento de sistemas de identificación electrónica: alto, sustancial, medio y bajo.

b) El Reglamento (UE) 910/2014 únicamente prevé la notificación de sistemas de identificación electrónica de nivel de aseguramiento alto.

c) 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, permite la videoconferencia, pero no la video-identificación.

d) El Reglamento de Ejecución (UE) 2015/1501 regula el conjunto mínimo de datos de identificación que representen de manera exclusiva a una persona física o jurídica.

33. Respecto a los certificados X.509 v3:

a) Las extensiones se clasifican en críticas, no críticas y recomendables.

b) Las extensiones no críticas pueden ignorarse si no se pueden procesar o se decide no hacerlo.

c) Un certificado sólo puede contener una extensión de un determinado tipo.

d) No pueden definirse extensiones para uso privado.

34. El Reglamento (UE) 910/2014 que deroga la Directiva 1999/93/CE es aplicable a partir de:

a) Al día siguiente de su publicación en el Diario Oficial de la Unión Europea (DOUE)

b) 1 de enero de 2015

c) 1 de enero de 2016

d) 1 de julio de 2016

35. Cuando obtenemos un certificado eletrónico de firma en la nube, la clave privada generada se queda en:

a) El navegador de internet

b) La tarjeta criptográfica

c) El prestador de servicios

d) A y C

36. ¿Cuál de las siguientes opciones se corresponde con un estándar para la firma electrónica?

a) WAdES

b) XAdES

c) PDFSignES

d) TotalSIGN-XL

37. Según el artículo 4 de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, ¿cuál es el periodo máximo de vigencia de los certificados cualificados?

a) 2 años

b) 3 años

c) 4 años

d) 5 años

38. Una característica fundamental de XML Signature es que:

a) Puede firmar parte o la totalidad de un documento XML.

b) Puede firmar un documento RTF y convertirlo en un documento XML.

c) Solo puede firmar un documento XML completo.

d) Solo puede firmar documentos RTF.

39. El organismo responsable de X.500, como conjunto de estándares de redes informáticas sobre servicios de directorio, entendidos estos como bases de datos de direcciones electrónicas, es:

a) INTEF.

b) ITU-T.

c) IEEE.

d) UNE.

40. El árbol formado por las entradas del directorio, en LDAP, se llama:

a) Ltree

b) LDS

c) DIT

d) Todas son falsas

41. ¿Cuál de los siguientes es un requisito de seguridad aplicable a los prestadores de servicios de confianza TSP?

a) Adoptarán las medidas técnicas y organizativas adecuadas para gestionar los riesgos para la seguridad de los servicios de confianza que prestan.

b) En un plazo máximo de 48 horas tras tener conocimiento de ellas, notificarán al Ministerio de Asuntos Económicos y Transformación Digital como organismo supervisor y al organismo nacional competente en materia de seguridad de la información, o la autoridad de protección de datos, cualquier violación de la seguridad o pérdida de la integridad que tenga un impacto significativo en el servicio de confianza prestado o en los datos personales correspondientes.

c) Cuando la violación de seguridad o la pérdida de integridad puedan atentar contra una persona física o jurídica a la que se ha prestado el servicio de confianza, el TSP notificará también a la persona, en un plazo de 72 horas, la violación de seguridad o la pérdida de integridad.

d) Si una violación de la seguridad o pérdida de la integridad afecta a dos o más Estados miembros, el organismo de supervisión notificado informará al respecto únicamente a los organismos de supervisión de los demás Estados miembros de que se trate.

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

a) WAdES.

b) PdES.

c) XAdES.

d) CdES.

43. Indique cuál de las siguientes afirmaciones es VERDADERA:

a) En un criptosistema simétrico el conocimiento de la clave pública no permite calcular la clave privada.

b) En un criptosistema de clave pública el conocimiento de la clave pública permite calcular la clave privada.

c) En un criptosistema de clave privada el conocimiento de la clave pública permite calcular la clave privada.

d) En un criptosistema asimétrico el conocimiento de la clave pública no permite calcular la clave privada.

44. Entrust hace referencia a:

a) Un algoritmo criptográfico

b) Un mecanismo de intercambio de claves

c) Una infraestructura de clave pública (PKI)

d) Una función resumen

45. Señale la opción correcta con respecto al importe de las sanciones impuestas según la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza

a) Por la comisión de infracciones se impondrán al infractor las siguientes sanciones: Por la comisión de infracciones muy graves, una multa por importe de 300.001 hasta 500.000 euros. Por la comisión de infracciones graves, una multa por importe de 100.001 hasta 300.000 euros. Por la comisión de infracciones leves, una multa por importe de hasta 100.000 euros.

b) Por la comisión de infracciones se impondrán al infractor las siguientes sanciones: Por la comisión de infracciones muy graves, una multa por importe de 100.001 hasta 300.000 euros.Por la comisión de infracciones graves, una multa por importe de 30.001 hasta 100.000 euros. Por la comisión de infracciones leves, una multa por importe de hasta 30.000 euros.

c) Por la comisión de infracciones se impondrán al infractor las siguientes sanciones: Por la comisión de infracciones muy graves, una multa por importe de 150.001 hasta 300.000 euros. Por la comisión de infracciones graves, una multa por importe de 50.001 hasta 150.000 euros. Por la comisión de infracciones leves, una multa por importe de hasta 50.000 euros.

d) Ninguna de las anteriores es correcta

46. Señale la respuesta correcta. Según se establece en la Ley 6/2020, de servicios electrónicos de confianza, en su artículo 19, las multas establecidas al infractor serán de:

a) Por la comisión de infracciones muy graves, multa de 150.001 a 300.000 euros, por la comisión de infracciones graves, se impondrá al infractor multa de 50.001 a 150.000 euros y por la comisión de infracciones leves, se impondrá al infractor una multa por importe de hasta 50.000 euros.

b) Por la comisión de infracciones muy graves, multa de 60.001 a 600.000 euros, por la comisión de infracciones graves, se impondrá al infractor multa de 6.001 a 60.000 euros y por la comisión de infracciones leves, se impondrá al infractor una multa por importe de hasta 6.000 euros.

c) Por la comisión de infracciones muy graves, multa de 120.001 a 600.000 euros, por la comisión de infracciones graves, se impondrá al infractor multa de 12.001 a 120.000 euros y por la comisión de infracciones leves, se impondrá al infractor una multa por importe de hasta 12.000 euros.

d) Por la comisión de infracciones muy graves, multa de 150.001 a 600.000 euros, por la comisión de infracciones graves, se impondrá al infractor multa de 15.001 a 150.000 euros y por la comisión de infracciones leves, se impondrá al infractor una multa por importe de hasta 15.000 euros.

47. Los certificados de clave pública:

a) Que se ajustan a la recomendación X.509 v.2 no admiten extensiones.

b) Ocupan más de 100 kbytes.

c) Que se ajustan a la recomendación X.509 v.3 sólo admiten como algoritmo de cifrado el RSA (Rivest Shamir Adleman).

d) Fueron propuestos por Diffie y Hellman en su artículo en que establecieron las bases de los criptosistemas de clave pública.

48. ¿Cuál es el plazo máximo de validez de los certificados de firma electrónica del DNI?

a) 30 meses

b) 4 años

c) 5 años

d) 10 años

49. El certificado X.509 no:

a) Fue definido por el antes denominado CCITT (actualmente ITU) en la recomendación X.509

b) En esta recomendación se define un modelo seguro para suministrar el servicio de autenticación a los usuarios del Directorio X.500 basado en criptografía de clave pública

c) La recomendación X.509 [CCI88] define un modelo de certificado en sintaxis ASN.1

d) Todas las respuestas anteriores son ciertas

50. Relativo a la firma digital, indique la opción incorrecta:

a) XMLDSig es una sintaxis XML para la generación de firma digital

b) XMLDSig sólo se utiliza para firmar documentos XML

c) XML Advanced Electronic Signatures (XAdES) cumple la directiva europea sobre firma electrónica

d) Las respuestas 'a' y 'c' son verdaderas

51. Según establece la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, el período de vigencia de los certificados cualificados no será superior a:

a) Dos años.

b) Cinco años.

c) Cuatro años.

d) La Ley 6/2020 no establece explícitamente un período máximo de validez para este tipo de certificados.

52. Según la recomendación X.509 v.3:

a) La autenticación simple conlleva el uso exclusivo de contraseñas transmitidas en claro.

b) La autenticación robusta (strong) de un sentido conlleva siempre el empleo de funciones resumen (hash).

c) La autenticación robusta (strong) de dos sentidos comporta siempre el uso de credenciales obtenidas mediante técnicas criptográficas.

d) La autenticación robusta (strong) de tres sentidos debe incorporar siempre sellos de tiempo.

53. Cuál es la forma correcta de crear un sello electrónico según la normativa sobre administración electrónica:

a) Resolución del Ministro publicado en BOE

b) Resolución del Ministro publicado en sede

c) Resolución de la subsecretaría publicado en la Sede

d) Resolución del Consejo de Ministros publicado en BOE

54. El organismo que elabora una Lista de confianza de prestadores de servicios de certificación (TSL) correspondiente a los prestadores que expiden certificados reconocidos y que están establecidos y supervisados en España, conforme a la normativa europea, es:

a) La FNMT como autoridad de certificación con la AEAT como autoridad de registro.

b) La AEAT como autoridad de certificación con la FNMT como autoridad de registro.

c) El Ministerio de Asuntos Económicos y Transformación Digital.

d) -

55. 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 (firma) junto 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.

56. ¿Qué norma comunitaria regula actualmente la identificación y la firma electrónica?

a) Directiva 2013/40/UE del Parlamento Europea y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información

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

c) Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica

d) Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior

57. Señalar cuál de las siguientes NO es una ventaja del uso de directorios LDAP para la autenticación de usuarios:

a) La mayoría de aplicaciones comerciales permiten su integración fácilmente.

b) Están optimizados para las búsquedas, que es la operación más repetida a la hora de gestionar los usuarios.

c) Permiten implantar sin ningún mecanismo adicional Single Sign On, ya que todas las aplicaciones pueden tener la autenticación a través del LDAP.

d) La replicación con los directorios /etc/passwd está automatizada, y por tanto la integración con las aplicaciones comerciales.

58. El perfil XAdES que permite la posibilidad de resellado periódico de tiempos de los documentos archivados es el:

a) T

b) XL

c) C

d) A

59. ¿Cuál de los siguientes sistemas de firma electrónica utilizan las Administraciones Públicas para la actuación administrativa automatizada, con objeto de su identificación electrónica y para la autenticación de los documentos electrónicos que produzcan?

a) Sello electrónico

b) Código seguro de verificación

c) Todos los anteriores

d) Ninguno de los anteriores

60. En relación con los portales y sedes electrónicas, señale la opción CORRECTA:

a) En el ámbito estatal, la creación o supresión de portales de Internet se llevará a cabo exclusivamente por orden de la persona titular del ministerio correspondiente.

b) Las sedes electrónicas se identificarán obligatoriamente mediante certificados cualificados de autenticación de sitio web.

c) El establecimiento de una sede electrónica no conlleva la responsabilidad del titular respecto de la integridad, veracidad y actualización de la información y los servicios a los que pueda accederse a través de la misma.

d) La supresión de portales requerirá la previa comunicación al Ministerio de Política Territorial y Función Pública y al Ministerio de Asuntos Económicos y Transformación Digital.

61. Indique la opción verdadera respecto a los certificados X.509v3:

a) El formato de certificados X.509 es un estándar del ITU-T.

b) Uno de sus elementos es el número de serie del certificado, un número secuencial que recomienza cada 1 de enero.

c) Emplean un formato llamado ASN-3 para la transmisión de datos.

d) Son válidos de forma permanente salvo que se incluyan en una lista de anulación de certificados (CRLs).

62. En el estándar X.509, ¿qué procedimiento de autenticación utilizaría cuando el origen y el destino no tienen relojes sincronizados?

a) autenticación a 1 vía

b) autenticación a 2 vías

c) autenticación a 3 vías

d) autenticación a 4 vías

63. Sobre los servicios cualificados de entrega electrónica certificada es FALSO que deban cumplir el siguiente requisito técnico:

a) Ser prestados por uno o más prestadores cualificados de servicios de confianza.

b) Asegurar con un alto nivel de fiabilidad la identificación del remitente.

c) Estar protegidos el envío y recepción de datos por una firma electrónica cualificada o un sello electrónico cualificado de tal forma que se impida la posibilidad de que se modifiquen los datos sin que se detecte.

d) Indicar claramente al emisor y al destinatario de los datos cualquier modificación de los datos necesarios a efectos del envío o recepción de los datos.

64. ¿Cuál de las siguientes afirmaciones en relación a la firma digital es cierta?

a) Ofrece plenas garantías de la integridad, confidencialidad y no repudio del documento firmado.

b) Se puede conseguir mediante protocolos de cifrado de clave secreta.

c) El DSS (Digital Signature Standard) está adoptado como una norma por ISO/IEC (International Standards Organization/International Electrotechnical Commission).

d) La firma ciega (Blind signature) se obtiene firmando directamente el correspondiente mensaje, en vez del resumen de éste.

65. En lo que se refiere a las Firmas Digitales, ¿cuál de las siguientes afirmaciones es falsa?

a) Si una firma digital es válida para un documento es válida para otro distinto.

b) Sólo puede ser generada por su legítimo titular.

c) Es públicamente verificable.

d) La forma más extendida de calcular firmas digitales consiste en emplear una combinación de cifrado asimétrico y funciones resumen.

66. Hablando de X500 y X.500, indique la respuesta correcta

a) X500 es un protocolo precursor de LDAP

b) X.500 es un protocolo precursor de LDAP

c) X500 es un atributo monovaluado

d) X.500 es un atributo multivaluado

67. El dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas, y sue le aportar aceleración hardware para operaciones criptográficas, se denomina:

a) PKI (Public Key Infrastructure).

b) Token criptográfico.

c) HSM (Hardware Security Module).

d) Pen Orive.

68. ¿Cuál de los siguientes formatos de firma electrónica no incorpora elementos que permiten definir una firma longeva?

a) AdES-BES

b) AdES-A

c) AdES-XL

d) -

69. Según el Reglamento (UE) 910/2014, un dispositivo cualificado de creación de firma electrónica es aquel que al menos ofrece una serie de garantías. ¿Cuál de las siguientes no es una garantía exigida para dichos dispositivos?

a) Que los datos de creación de firma electrónica utilizados para la creación de firma electrónica solo puedan aparecer una vez en la práctica

b) Que exista la seguridad razonable de que los datos de creación de firma electrónica utilizados para la creación de firma electrónica no pueden ser hallados por deducción y de que la firma está protegida con seguridad contra la falsificación mediante la tecnología disponible en el momento

c) Que los datos de creación de la firma electrónica utilizados para la creación de firma electrónica puedan ser protegidos por el firmante legítimo de forma fiable frente a su utilización por otros

d) Que el dispositivo de creación de firma esté certificado al menos con el nivel de seguridad EAL4+.

70. Indique la opción correcta respecto a LDAP:

a) Emplea un formato llamado Python para la transmisión de datos.

b) Cada entrada tiene un DN (Distinguished Name) como identificador único.

c) La versión actual es LDAPv2, y se encuentra definido en el estándar 4511 del ITU-T y del ISO/IEC.

d) Open DS, ApacheDS y Red Hat Directory Server son alternativas no basadas en LDAP.

71. La RFC del IETF que hace referencia al modelo de directorio LDAP es:

a) RFC 3161
b) RFC 4510
c) RFC 4120
d) RFC 6101

72. ¿Cuántos niveles de seguridad define el proyecto STORK?

a) 3
b) 4
c) 5
d) 6

73. La firma digital garantiza:

a) La autenticidad, la integridad y el no repudio en destino.
b) La autenticidad, la integridad y el no repudio en origen.
c) La autenticidad, la integridad y la confidencialidad.
d) La confidencialidad.

74. Un documento firmado digitalmente incluye la huella digital:

a) De la clave del firmante, cifrada con su clave pública.
b) De la clave pública del firmante, cifrada con su clave privada.
c) Del documento firmado, cifrada con la clave del firmante.
d) Del documento firmado, cifrada con la clave pública del firmante.

75. Según la normativa de firma electrónica, el período de validez de los certificados cualificados no podrá ser superior a:

a) Un año
b) Dos años
c) Tres años
d) Cinco años

76. 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) Cuatro años.
c) Cinco años.
d) La Ley 6/2020 no establece explícitamente un período máximo de validez para este tipo de certificados.

77. 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.

78. En relación al software criptográfico GPG, es cierto que:

a) Son las siglas de Great Privacy Group.
b) Es una versión propietaria de PGP.
c) Cifra los mensajes usando pares de claves individuales asimétricas generadas por los usuarios.
d) Usa tres algoritmos: IDEA, AES y 3DES.

79. Señale cuál de los siguientes estándares de firma electrónica clasifica las firmas en despegadas (detached), envolventes (enveloping) y envueltas (enveloped), según en qué sitio del propio fichero de firma se guarde el documento original:

a) CAdES.

b) XAdES.

c) PAdES.

d) -

80. ¿Qué mecanismos de comprobación de identidad establece la ley 6/2020 y su desarrollo en la Orden ETD/465/2021 para la emisión de certificados electrónicos cualificados?:

a) Presencial, remota por vídeo o firma legitimada notarialmente.

b) Exclusivamente presencial ante una oficina de registro autorizada.

c) Presencial o mediante la firma del interesado, legitimada en presencia notarial.

d) Presencial, mediante llamada telefónica, video llamada, zoom o similar.

81. 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) 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

d) Las firmas electrónicas cualificadas tendrán una validez de 48 meses

82. Respecto a los servicios de directorio se puede afirmar que:

a) LDAP define el modelo completo de servicio de directorio

b) X.500 es un protocolo de acceso a un servicio de directorio LDAP

c) LDAP es un protocolo de acceso a servicios de directorio X.500

d) Ninguna de las anteriores es correcta

83. Indica cuál de las siguientes definiciones de firma electrónica es la que aparece en el Reglamento (UE) 910/2014

a) es el resultado de obtener por medio de mecanismos o dispositivos un patrón que se asocie biunívocamente a un individuo y a su voluntad de firmar.

b) los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar

c) es el documento electrónico que acredita electrónicamente la identidad personal de su titular y permite la firma de documentos.

d) es el conjunto de datos únicos, como códigos o claves criptográficas privadas, que el firmante utiliza para firmar documentos.

84. ¿A quién corresponde elaborar una lista de prestadores de servicios electrónicos de confianza?

a) Al Ministerio de Asuntos Económicos y Transformación Digital.

b) Al Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática.

c) A la Secretaría General de Administración Digital.

d) Ninguna de las anteriores es cierta.

85. ¿Cuáles son los niveles de seguridad de los sistemas de identificación electrónica que define el Reglamento (UE) 910/2014?

a) Bajo, medio y alto.

b) Básico, medio y alto.

c) Básico, sustancial y alto.

d) Bajo, sustancial y alto.

86. Señale el plazo en que deben ser auditados los prestadores cualificados de servicios de confianza:

a) Al menos cada 12 meses

b) El Reglamento no trata la supervisión de los prestadores cualificados de servicios de confianza, dejando tal cuestión a la regulación nacional de cada Estado miembro

c) Al menos cada 18 meses

d) Al menos cada 24 meses

87. Según la Ley 6/2020, de servicios electrónicos de confianza, los prestadores de servicios de certificación que expidan certificados cualificados deberán conservar registrada por cualquier medio seguro toda la información y documentación relativa a un certificado cualificado al menos durante:

a) 5 años.

b) 10 años.

c) Permanentemente.

d) 15 años.

88. La Ley 6/2020, de servicios electrónicos de confianza, establece como sanción por la comisión de infracciones graves:

a) Multa por importe de 50.001 a 150.000 euros.

b) Multa por importe de hasta 50.000 euros.

c) Multa por importe de 150.001 a 300.000 euros.

d) Multa por importe de 50.001 a 100.000 euros.

89. En una PKI basada en certificados X.509v3:

a) Los certificados son firmados por otros usuarios a través de conexiones regidas por la confianza entre ellos.

b) Los certificados deben estar avalados por una Autoridad de Certificación.

c) No se puede acreditar la identidad de sitios web.

d) -

90. En relación con LDAP (Lightweight Directory Access Protocol), si quisiéramos intercambiar, importar o exportar datos de directorio, ¿qué formato usaríamos?

a) DEFL (Data Exchange Format for LDAP).

b) LDIF (LDAP Data Interchange Format).

c) XmLDAP (XML for LDAP).

d) DSML (Directory Syntax Markup Languaje).

91. Según la Ley 59/2003, de 19 de diciembre, de firma electrónica, un certificado electrónico es:

a) Un documento redactado en soporte electrónico que incorpora datos que estén firmados electrónicamente.

b) Un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad.

c) Un conjunto de datos asociados a un mensaje, resultantes de aplicar una función hash y un cifrado, que permite asegurar la identidad del firmante y la integridad del mensaje.

d) Un conjunto de datos asociados a un mensaje, resultantes de aplicar una función hash, que permite asegurar que el mensaje no fue modificado

92. En relación con el servicio de directorio X.500, señalar la falsa:

a) Cada entrada del Directorio, tiene un identificador único llamado RDN.

b) La parte común de todas las entradas u objetos, se llama Suffix.

c) El conjunto de objetos, constituyen un DMD o dominio de gestión.

d) X.500 no define nada sobre la interfaz de usuario.

93. El campo extensions en un certificado X.509:

a) Permite añadir nuevos campos al certificado sin modificar su definición ASN.1

b) Presentan información sobre claves certificadas y políticas

c) Presentan información adicional sobre el propietario del certificado y sobre su emisor

d) Todas las respuestas anteriores son ciertas

94. Para los niveles de seguridad de los sistemas de identificación definidos en el Reglamento (UE) 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, NO es cierto:

a) Se tienen en cuenta tanto el proyecto europeo STORK como la norma ISO 29115.

b) El nivel sustancial de STORK requiere un registro presencial al menos una vez, y la credencial electrónica se entrega como certificado hardware.

c) El modelo QAA (Quality, Authentication, Assurance) diferencia los factores asociados al proceso de registro y entrega de la credencial, y factores asociados al proceso de autenticación electrónica con dicha credencial.

d) El DNIe se corresponde con un nivel 4 de QAA.

95. Indique cuál de los siguientes no es un servicio LDAP:

a) READ

b) COMPARE

c) ADD

d) ABANDON

96. En la estructura de un certificado X.509 v3 NO es obligatorio:

a) El número de serie.

b) La validez no antes de.

c) El identificador único de emisor.

d) El emisor.

97. Señalar cuál de las siguientes es una obligación impuesta a los prestadores cualificados de servicios de confianza:

a) Ser auditados, al menos cada 24 meses, corriendo con los gastos que ello genere, por un organismo de evaluación de la conformidad

b) Elegir en cada país al organismo de supervisión que garantice que se cumple con lo establecido en el Reglamento (UE) 910/2014, de 23 de julio de 2014

c) Incluir atributos específicos adicionales en los certificados cualificados de firmas electrónicas

d) Utilizar la etiqueta de confianza "UE" para indicar de manera simple, reconocible y clara los servicios de confianza cualificados que prestan

98. ¿Cuál de los siguientes es un protocolo de directorio?

a) MIME

b) LDAP

c) SMNP

d) BGP

99. En relación a los certificados X.509:

a) Se codifican mediante la notación ASN.1

b) Permite el uso en sus campos de nombres X.500 y DNS

c) Se han definido extensiones que permiten incluir información específica

d) Todas las anteriores son ciertas

100. ¿En qué nivel de la pila OSI se sitúa el protocolo LDAP?

a) Aplicación

b) Transporte

c) Red

d) Sesión

101. Con respecto a la auditoría de los prestadores cualificados de servicios de confianza establecida en el Reglamento (UE) 910/2014, los prestadores cualificados de servicios de confianza enviarán el informe de evaluación de la conformidad correspondiente al organismo de supervisión tras su recepción en el plazo de:

a) tres días hábiles

b) cinco días hábiles

c) diez días hábiles

d) diez días naturales

102. ¿A qué corresponden las siglas STORK?

a) Secure Transport Over bRoad toKens

b) Security idenTity acrOss boRders linKed

c) Safe idenTity fOr Roaming Knowledge

d) Safe noTes stOring encRypted Keys

103. Los certificados digitales:

a) Basados en la recomendación X.509 v.2 admiten extensiones, que pueden llevar una bandera de criticidad.

b) Definidos en el programa PGP (Pretty Good Privacy) son compatibles con los X.509 v.3.

c) De atributos vinculan al titular con su clave pública y sus atributos.

d) Basados en la recomendación X.509 v.3 pueden incorporar como extensiones los atributos que constan en un certificado de atributos.

104. El estándar conocido como ISO/IEC 9594-1:2020 se corresponde con:

a) LDAP

b) UIT-T X.500

c) HTML

d) SQL

105. La Resolución de 20 de octubre de 2022, de la Secretaría General de Administración Digital, establece las condiciones de uso de firma electrónica no criptográfica en las relaciones de los interesados con los órganos administrativos de la AGE:

a) Para sistemas categorizados, según ENS, de categoría básica y aquellos de categoría media en los que no sea necesaria la firma electrónica avanzada por normativa.

b) Para sistemas en los que la identificación no requiera un registro fehaciente o que tramiten solicitudes que no precisen identificar al interesado.

c) Para sistemas que se hayan categorizado según ENS como de categoría básica y que precisen garantizar el consentimiento y no repudio del interesado.

d) Para la firma de documentos electrónicos que no estén incluidos en los supuestos establecidos en el art 11.2 de la ley 39/2015.

106. ¿Qué extensión emplea la versión v3 del protocolo LDAP para establecer una conexión segura?:

a) RFC 6101.

b) TLS.

c) SSL.

d) Ipsec.

107. La abreviatura DN en la sintaxis LDAP hace referencia a:

a) Distinguished Name.

b) Domain Name.

c) Digital Nomenclator.

d) Detailed Name.

108. 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, en lo relativo a la conservación de la grabación:

a) La copia de la grabación del vídeo se considera datos de carácter personal y por lo tanto no puede conservarse en cumplimiento con el Reglamento (UE) 2016/679

b) Se conservará una copia de la grabación del vídeo durante un periodo mínimo de tiempo de 15 años desde la extinción de la vigencia del certificado obtenido por este medio.

c) Se conservarán todas las pruebas de los procesos de identificación incompletos que no hayan llegado a término por sospecha de intento de fraude durante un plazo de 15 años

d) Ninguna de las anteriores es correcta

109. En el contexto de una infraestructura de clave pública X.509, el protocolo OCSP permite comprobar...

a) la caducidad de un certificado.

b) la identidad del titular del certificado.

c) la correspondencia entre la clave pública y la privada.

d) la validez del certificado.

110. ¿Cuál es la afirmación falsa si hablamos de LDAP?

a) Usa TCP/IP

b) Reemplaza a X.500

c) El protocolo usa ASN.1 y los mensajes se codifican y transmiten usando BER

d) Permite la operación MODIFY

111. ¿Tiene la firma electrónica el mismo valor ante la ley que la firma manuscrita?

a) Sí, siempre

b) No, en ningún caso

c) Sí, si es firma electrónica avanzada

d) Sí, si es firma electrónica cualificada

112. Indique la sentencia verdadera sobre el protocolo LDAP:

a) Utiliza por defecto el puerto TCP 392.

b) Está basado en el protocolo de directorio X.400.

c) EL DN (Distinguished Name) identifica unívocamente una entrada.

d) Hace uso de toda la pila OSI.

113. Los prestadores cualificados de servicios electrónicos de confianza, según lo dispuesto en 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, deberán utilizar un producto de identificación remota por vídeo que cumpla los requisitos mínimos de seguridad indicados en el anexo F.11 de la Guía de Seguridad de las TIC CCN-STIC-140, del Centro Criptológico Nacional de categoría Alta.

a) Desde el día siguiente al de su publicación en el BOE, el 7 de mayo de 2021

b) Desde el 1 de julio de 2022

c) El cumplimiento de los requisitos de seguridad se demostrará mediante certificaciones, informes o pruebas en laboratorios o entidades especializadas, que se revisarán por un organismo de evaluación de la conformidad, quien incluirá el resultado en el informe de evaluación de la conformidad.

d) Las guías CCN-STIC se trata de recomendaciones y por tanto no es obligatorio cumplir con dichos requisitos de seguridad

114. ¿Cuál de las siguientes respuestas es verdadera respecto a X.500?

a) X.500 es un protocolo que especifica un modelo para conectar servicios de directorio locales para formar un directorio global distribuido, de forma que el usuario percibe el directorio completo como accesible de su servidor local

b) X.500 fue inicialmente un sistema propietario de Novell, pero en la actualidad ha sido cedido para dominio público por un procedimiento estratégico de la compañía para acabar con sistemas incompatibles desarrollados por empresas rivales

c) X.500 ha sido desarrollado por ANSI para su implementación en el ejército americano por petición del DoD, pero en realidad no ha sido utilizado por éste por falta de seguridad, y en la actualidad, al ser un protocolo publicado ha sido adoptado por diversos organismos

d) X.500 es el protocolo de directorio más extendido, por lo que puede considerarse un estándar de facto, pero aunque se estima próxima su adopción por ISO para incorporarlo a la definición estándar de OSI, aún no se ha dado este paso

115. Si exportamos un certificado incluyendo su clave privada desde el navegador MS Edge, ¿qué extensión tendrá el fichero resultante?

a) .p12

b) .cer

c) .jks

d) .pfx

116. En el estándar XADES de firma electrónica, el perfil que incluye un TimeStamp a las referencias de las CRLs, es:

a) XADES-X

b) XADES-T

c) XADES-XL

d) XADES-C

117. Con respecto a X.500 y LDAP, indicar la respuesta incorrecta:

a) X.500 utiliza ASN.1 para la formación de los mensajes, y LDAP utiliza cadenas de caracteres simples para la representación de Distinguished Names

b) LDAP no posee el servicio de modificación REMOVE perteneciente a DAP

c) X.500 y LDAP funcionan sobre la pila de protocolos OSI y TCP/IP respectivamente

d) Un dominio de gestión de directorio está formado, como mínimo, por: 1 DSA, 1 DUA y 1 esquema (visión externa del dominio)

118. Los certificados de sede electrónica incluirán como contenido:

a) Lo que disponga el Esquema Nacional de Seguridad.

b) La denominación de sede electrónica y el número de identificación fiscal de la autoridad de certificación.

c) Su contenido no está definido en ninguna norma.

d) La denominación del nombre del dominio y el nombre descriptivo de la sede.

119. Según el Reglamento (UE) 910/2014, un dispositivo cualificado de creación de firma electrónica es aquel que al menos ofrece una serie de garantías. ¿Cuál de las siguientes no es una garantía exigida para dichos dispositivos?

a) Que los datos de creación de firma electrónica utilizados para la creación de firma electrónica solo puedan aparecer una vez en la práctica;

b) Que exista la seguridad razonable de que los datos de creación de firma electrónica utilizados para la creación de firma electrónica puedan ser hallados por deducción y de que la firma está protegida con seguridad contra la falsificación mediante la tecnología disponible en el momento

c) Que los datos de creación de la firma electrónica utilizados para la creación de firma electrónica puedan ser protegidos por el firmante legítimo de forma fiable frente a su utilización por otros.

d) Que los dispositivos cualificados de creación de firmas electrónicas no alterarán los datos que deben firmarse ni impedirán que dichos datos se muestren al firmante antes de firmar.

120. Según la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, ¿cual es una obligación de los prestadores cualificados de servicios electrónicos de confianza?

a) Constituir un seguro de responsabilidad civil por importe mínimo de 1.500.000 euros. Si presta más de un servicio cualificado de los previstos en el Reglamento (UE) 910/2014, se añadirán 500.000 euros más por cada tipo de servicio.

b) Constituir un seguro de responsabilidad civil por importe mínimo de 1.500.000 euros, excepto si el prestador pertenece al sector público. Si presta más de un servicio cualificado de los previstos en el Reglamento (UE) 910/2014, se añadirán 500.000 euros más por cada tipo de servicio.

c) Constituir un seguro de responsabilidad civil por importe mínimo de 1.000.000 euros. Si presta más de un servicio cualificado de los previstos en el Reglamento (UE) 910/2014, se añadirán 250.000 euros más por cada tipo de servicio.

d) Constituir un seguro de responsabilidad civil por importe mínimo de 1.000.000 euros, excepto si el prestador pertenece al sector público. Si presta más de un servicio cualificado de los previstos en el Reglamento (UE) 910/2014, se añadirán 250.000 euros más por cada tipo de servicio.

121. En el entorno de la firma electrónica y la identidad electrónica, STORK identifica:

a) Un proyecto financiado por la Comisión Europea para establecer la interoperabilidad de las identidades electrónicas de los Estados Miembros.

b) A la PKI desplegada por la Comisión Europea para la futura carta de identidad electrónica europea.

c) La implementación opensource realizada por la Comisión Europea de un cliente de firma electrónica.

d) El consorcio de fabricantes e industria Europea relacionado con la firma electrónica e identidad electrónica.

122. El proyecto CERES:

a) Establece cómo deben de ser los certificados que se usen para realizar la firma electrónica.

b) Hace que se pueda usar a la Fábrica Nacional de la Moneda y Timbre de forma gratuita por todos los españoles.

c) Se define en el ámbito de la relación de los ciudadanos con las administraciones y éstas entre sí.

d) Designa a la Fábrica Nacional de la Moneda y Timbre como autoridad de certificación para cualquier transacción electrónica.

123. Señale la respuesta CORRECTA en relación a la firma digital:

a) Es un certificado electrónico que asocia una clave pública con la identidad de su propietario.

b) Se sirve de la criptografía asimétrica para garantizar la confidencialidad y la integridad del mensaje enviado.

c) Permite al receptor de un mensaje verificar la autenticidad del origen del mensaje y su integridad.

d) Es el criptograma resultante de aplicar una función hash al mensaje y cifrarlo con la clave pública del firmante.

124. Señale la respuesta correcta que identifica los nuevos tipos de certificados según el Reglamento (UE) 910/2014 (eIDAS):

a) Certificados cualificados de firma electrónica, certificados cualificados de sello, certificados cualificados de autenticación web

b) Certificados cualificados de firma electrónica, certificados cualificados de sesión, certificados cualificados de cifrado, certificados cualificados de persona jurídica, y de persona física

c) Certificados cualificados de firma electrónica, certificados cualificados de Órgano, certificados cualificados de autenticación web y componentes

d) Certificados cualificados de autenticación, certificados cualificados de cifrado, certificados cualificados de firma y certificados cualificados de sello

125. Señale cuál de las siguientes expresiones sobre los estándares de servicio de directorio es incorrecta:

a) El estándar LDAP es un desarrollo de IETF, mientras que el estándar X.500 es de ITU-T

b) LDAP utiliza la notación ASN.1 para codificar el envío y recepción de peticiones y respuestas

c) En una implementación de directorio basada en X.500 la información se almacena conceptualmente en forma de objetos

d) Para simplificar a X.500, LDAP se diseñó para implementarse sobre arquitecturas de red OSI

126. ¿Cuál de las siguientes es una implementación del protocolo LDAP?

a) eDirectory

b) iPlanet

c) Active Directory

d) Todos lo son

127. ¿Qué servicio proporciona a los usuarios el servicio de directorio X.500?

a) Dar facilidades para consultar información acerca de objetos accesibles en una red

b) Facilitar direcciones y nombre de usuarios accesibles en una red

c) Realizar las funciones de direccionamiento y nomenclatura de usuarios de un sistema de tratamiento de mensajes según la norma X.400

d) Controlar las peticiones de registro de usuario por medio de agentes de sistema (DSA) y mantenimiento de la base de información de directorio (DIB)

128. ¿Cuál NO es una extensión válida para certificados?

a) .PFX

b) .DER

c) .P7B

d) Todas lo son

129. ¿Qué es un certificado digital?

a) Es un conjunto de datos asociados a un mensaje que permite asegurar la identidad del firmante y la integridad del mensaje.

b) Es un fichero digital emitido por una tercera parte de confianza que garantiza la vinculación entre la identidad de una persona o entidad y su clave pública.

c) Es una contraseña que se utiliza para acceder a documentos protegidos.

d) Es un software que permite verificar la validez de una firma electrónica.

130. Indique cuál de los siguientes no es uno de los requisitos que deben cumplir los servicios cualificados de entrega electrónica certificada según el Reglamento (UE) 910/2014:

a) Ser prestados por uno o más prestadores cualificados de servicios de confianza

b) Garantizar la identificación del destinatario antes de la entrega de los datos

c) Indicar mediante un sello cualificado de tiempo electrónico la fecha y hora de envío, recepción y eventual modificación de los datos

d) Proteger el envío y la recepción de datos por una firma electrónica cualificada o un sello electrónico cualificado de un prestador cualificado de servicios de confianza