1. ¿En qué año se celebró el primer convenio sobre ciberdelincuencia conocido como Convenio de Budapest?.

a) 2001. b) 2005. c) 2010.

2. "Actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos" es la definición de ciberdelincuencia que figura en:

a) El Convenio de Budapest.
b) El código Penal español reformado.
c) El protocolo Adicional del Convenio de Ciberdelincuencia.

3. Los datos relativos al origen, destino, ruta, hora, fecha, tamaño y duración de la comunicación se corresponde con el concepto de:

a) Datos informáticos.
b) Datos relativos al tráfico de una comunicación.
c) Ambas respuestas con correctas.

4. ¿Qué nombre recibe el protocolo para acceder al correo electrónico, grupo de noticias, y otros, desde móviles?:

a) MMS. b) WAP. c) GPRS.

5. ¿Cómo se denomina la unidad que, dentro de la investigación del cibercrimen, se dedica a la seguridad informática y los fraudes?:

a) Brigada Central de Investigación Tecnológica.
b) Brigada Central de Seguridad Informática.
c) Unidad Tecnológica y del Cibercrimen.

6. Para la Convención de Budapest, la obtención de una contraseña que permita acceder ilícitamente a datos de un sistema informático es:

a) Interferencia en el sistema. b) Abuso de los dispositivos. c) Acceso ilícito.

7. La Convención de Budapest, en relación con el concepto de pornografía infantil, entiende que es realizada sobre un menor de:

a) 16 años. b) 14 años. c) 18 años.

8. Señala una clasificación que se corresponda con algún grupo establecido por la Fiscalía General del Estado respecto a los delitos informáticos:

a) Delitos informáticos estrictamente considerados.
b) Delitos relacionados con infracciones al derecho a la propiedad intelectual y a los derechos afines.
c) Delitos en los que la actividad criminal entraña especial complejidad en su investigación.

9. La adquisición de un programa para entrar ilícitamente a un sistema informático, aunque no haya accedido ninguno:

a) No está penado en nuestro Código Penal.
b) Se recoge genéricamente en el artículo 197 del Código Penal.
c) Se pena en el artículo 197 ter de nuestro Código Penal.

10. La diferencia entre injuria y columnia estriba, entre otros matices, en:

a) Que se haga con o sin publicidad.
b) Que la acusación corresponda o no a un delito.
c) Que se realice, o no, por medio de sistemas informáticos.

11. Señala la respuesta que contenga una acción que, aunque delictiva, no pueda considerarse delito de pornografía infantil:

a) La utilización en una exhibición pornográfica de una persona mayor de edad discapacitada necesitada de atención especial.
b) La utilización para un espectáculo pornográfico de persona capacitada, pero mayor de 16 años.
c) Ambas conductas son consideradas delito de pornografía infantil.

12. ¿Qué distinción externa identifica fundamentalmente a los simpatizantes o colaboracionistas del grupo Anonymous?:

a) Tapan su cara con una bufanda negra.
b) El signo interrogante en sus vestimentas.
c) Una careta.

13. La grabación telefónica por parte del propio usuario de la línea, o autopinchazo en el argot telemático, tiene el nombre:

a) Hijacking. b) Ciberbulling. c) Bugging.

14. Se puede entender como pornografía infantil la siguiente acción:

a) La exhibición de una persona que parezca menor de edad comportándose de forma sexualmente explícita.
b) La imágenes de un menor de 18 años comportándose de forma sexualmente explicita.
c) Ambas respuestas son correctas.

15. ¿Está penada la simple asistencia a espectáculos pornográficos infantiles?:

a) Si.
b) No.
c) Solo en el caso de que se demuestre que se conocía en contenido previamente.

16. La Ley de Protección de Datos regula y controla:

a) Todo tipo de ficheros de datos.
b) Todos los ficheros de datos de carácter personal.
c) Exclusivamente ficheros de datos de carácter personal de acceso informático.

17. Quedan excluidos del ámbito de aplicación de la LOPD:

a) Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea, aunque tenga servidores informáticos que sirvan de almacenamiento temporal de datos instalados en territorio español para transmitir los datos fuera de España.
b) A los ficheros sometidos a la normativa sobre protección de materias clasificadas.
c) A ninguno de los dos anteriores.

18. A los ficheros con fines exclusivamente estadísticos les es de aplicación:

a) La legislación estatal o autonómica sobre esta materia.
b) La LOPD.
c) Ninguna normativa específica.

19. ¿De qué tiempo dispone el administrador de un fichero de datos personales para mostrar los datos de un solicitante de acceso, caso de que la Agencia de Protección de Datos admita una solicitud?:

a) De seis meses. b) De 15 días. c) De 10 días.

20. A los ficheros policiales correspondientes al DNI, administrados por la policía nacional:

a) Les son de aplicación el régimen general de la LOPD.
b) Deben ser comunicados al Registro de Protección de datos y tratados y almacenados como ficheros específicos.
c) Se les aplica una ley específica sobre esta materia.

21. Los puestos de trabajo desempeñados en la Agencia de Protección de Datos son:

a) El funcionamiento de las administraciones públicas .
b) Personal contratado al efecto.
c) Ambos tipos de trabajadores coexisten en la Agencia de Protección de datos.

22. ¿Qué se requiere para que se pueda apreciar el concepto de flagrante delito en la entrada de un domicilio sin consentimiento del titular?

a) Peligrosidad, acción antijurídica y vulntariedad.
b) Inmediatez temporal, espacial y personal.
c) Gravedad del hecho y disponibilidad del autor del delito.

23. Para que una comunicación esté protegida jurídicamente, es necesario que:

a) Dichas comunicaciones contengan carácter íntimo.
b) Su vulneración vaya acompañada de la difusión de dicha comunicación.
c) Ninguna de las dos opciones anteriores son correctas.

24. ¿Qué delitos atentan particular y fundamentalmente contra el derecho al honor protegido en el artículo 18 de nuestra constitución?:

a) Las amenazas y coacciones. b) El allanamiento de morada. c) Las calumnias y las injurias.

25. La consideración de la prueba digital se extiende al concepto de:

a) Toda información de valor probatorio de un hecho considerado como delito informático.
b) Toda información de valor probatorio contenida en un soporte de datos informáticos o transmitidos por estos medios.
c) Toda información de valor probatorio contenida en un soporte informático o transmitida por estos medios, siempre que trate de delitos informáticos.

26. ¿Cuánto tiempo están obligadas las compañías de telecomunicaciones a guardar los datos generados en las comunicaciones telemáticas?:

a) Un año. b) Dos años. c) Seis meses.

27. En relación al volcado de información de un ordenador para hacer un backup con el objeto de analizar los datos contenidos en él sin peligro de que su manipulación puedan perderse del original:

a) Tanto la intervención como el volcado de datos necesitan de presencia del secretario judicial que levante acta del hecho.
b) Ni la intervención del ordenador ni el volcado de sus actos necesitan de dicha presencia.
c) La intervención del ordenador sí necesita de la presencia del secretario judicial en el registro en el que se realice, pero no así el volcado de dichos datos.

28. Si se manipulase el contenido de una prueba digital protegida por un número hash, ¿qué sucedería?:

a) Que dicha prueba es nula de pleno derecho si se llega a comprobar esa manipulación cotejándola con la original.
b) La integridad de la cadena de custodia se basa exclusivamente en la buena fe de los funcionarios actuantes, por lo que, si no se detecta esa manipulación, la prueba es válida.
c) Que varía el contenido del número hash y detecta la manipulación, lo que invalidaría la prueba.

29. El derecho a la intimidad personal se hace extensivo también:

a) Al núcleo familiar.
b) Exclusivamente a los menores que convivan en la unidad familiar.
c) A la familia.

30. ¿En qué plazo se debe producir la cancelación de datos, a petición de un ciudadano por parte del administrador del fichero que los contiene?:

a) En 15 días. b) En 10 días naturales. c) En tres meses.

31. ¿Qué contenido tiene el <u>Protocolo Adicional al Convenio de Budapest</u> promulgado en el año 2003 y al que España se ha adherido en el año 2015?:

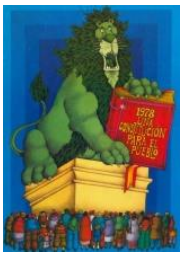
a) Ciberdelito relativo a la pornografía infantil.
b) Delitos informáticos relativos al tráfico ilícito de órganos humanos.
c) Xenofobia y racismo a través de Internet.

32. Señala la <u>respuesta que contenga</u> un país no europeo adherido al Convenio de Budapest sobre ciberdelincuencia:

a) Sudáfrica. *b) Colombia.* *c) Rusia.*

33. Se considera delincuencia informática o ciberdelincuencia:

a) Toda acción penal cuyo desarrollo se ha efectuado por medio de un ordenador.
b) Todo delito tipificado en nuestro ordenamiento penal en la que interviene un sistema informático.
c) Ninguna de las dos respuestas son correctas.



34. Para el <u>Convenio de Budapest</u>, ¿qué consideración tienen los programas diseñados para que un sistema informático ejecute una función?:

a) Software base de un sistema informático.
b) Datos relativos al tráfico informático.
c) Datos informáticos.

35. ¿Qué <u>siglas</u> pertenecen exclusivamente a las telecomunicaciones por medio de móviles?:

a) 3G. *b) IP.* *c) TCP.*

36. El <u>acceso legítimo</u>, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas dirigidas a un sistema informático es, para el convenio de Budapest:

a) Acceso ilícito. *b) Interpretación ilícita.* *c) Interferencia de datos.*

37. Para la <u>Convención de Budapest</u>, el llamado abuso de los dispositivos se encuadra dentro del bloque de delitos:

a) Delitos contra la confidencialidad y la integridad y la disponibilidad de los datos y sistemas informáticos.
b) Delitos informáticos estrictamente considerados.
c) Delitos relacionados con el contenido.

38. ¿Qué edad establece, como mínima, la <u>Convención de Budapest</u> para considerar pornografía infantil acciones sexuales sobre una persona?:

a) 18 años. *b) 16 años.* *c) 14 años.*

39. Los <u>descubrimientos y revelación de secretos</u> están recogidos en el Código Penal español en los artículos :

a) 197 y siguientes. *b) 264 y concordantes.* *c) 278 y 279.*

40. El <u>acceso ilícito a los datos de un sistema informático</u>, sin intención de usarlo para descubrir su contenido:

a) No está penado en nuestro Código Penal.
b) Se recoge en el artículo 197 bis del Código Penal.
c) Se pena en el artículo 197 ter de nuestro Código Penal.

41. ¿Qué <u>acciones</u> se castigan en el artículo 248 del Código Penal?:

a) Las estafas. *b) Los sabotajes y daños.* *c) El descubrimiento de secretos.*

42. Uno de los <u>siguientes delitos</u> no tiene, ni puede tener nunca, la consideración de delito informático, aunque en el transcurso de su ejecución se haya utilizado algún tipo de tecnología de la información y de las comunicaciones:

a) El delito de homicidio.
b) El delito de falsificación documental.
c) El delito de calumnia.

43. ¿Cuál fue el <u>motivo fundamental</u> para que el grupo Anonymous intensificase sus acciones de sabotaje a los sistemas de telecomunicaciones?:

a) El caso Wikileaks.
b) La caída de las Torres Gemelas en Nueva York.
c) La entrada de EE UU en la Guerra de Irak.

44. El <u>acoso infantil en Internet</u>, con la finalidad de realizar abusos sexuales con la victima, recibe el nombre de:

a) Childgrooming. *b) Hoax.* *c) Ciberbulling.*

45. Los <u>delitos contra la propiedad intelectual</u> cometidos utilizando sistemas y recursos de Internet se encuadran en la siguiente catalogación de la Fiscalía General del Estado:

a) Delitos en los que se atentan los propios sistemas informáticos.
b) Delitos en los que las TIC ayudan a su ejecución.
c) Delitos en los que las TIC dificultan su investigación.

46. ¿En qué caso, de los siguientes, la <u>recogida de datos</u> no necesita autorización de su titular?:

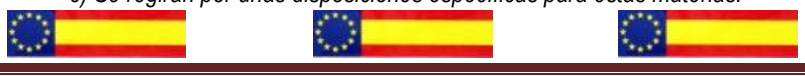
a) Cuando una ley así lo permita.
b) Si los datos sean de acceso público y su tratamiento sea necesario para el interés legítimo del responsable del sistema.
c) En ambos casos.

47. Las <u>cesiones de datos</u> que resulten de consultas, transferencias, etc., tienen la consideración de:

a) Ficheros de datos. *b) Tratamiento de datos.* *c) Administración y gestión de datos.*

48. Los <u>ficheros</u> establecidos para la investigación del terrorismo y otras formas graves de delincuencia organizada:

a) Se les aplica la LOPD.
b) Quedan totalmente excluidos de la aplicación de esta ley.
c) Se regirán por unas disposiciones específicas para estas materias.



49. A los ficheros procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las fuerzas y cuerpos de seguridad les serán de aplicación :

a) La LOPD. *b) La Ley de FCS.* *c) Una ley específica para esta materia.*

50. El derecho de oposición en la LOPD significa que:

a) Una persona puede oponerse a que sus datos puedan ser tratados con fines publicitarios u otro motivo legítimo.
b) Una persona puede solicitar la cancelación de sus datos de un fichero, al considerar que son inexactos.
c) Una persona puede solicitar ver los datos suyos existentes en un fichero.

51. ¿Qué tipo de ficheros administrados por la Policía Nacional se regula por una normativa específica para esa materia, aunque la LOPD se la aplica con carácter general?:

a) Los ficheros correspondientes al DNI.
b) Los datos sobre el ADN recogidos a algunos reseñados.
c) Los ficheros generados como consecuencia de investigaciones policiales.

52. De las siguientes, ¿qué normativa afecta y protege al derecho al honor, a la intimidad individual y familiar y a la propia imagen?:

a) La ley Orgánica 1/1982 de Protección Civil, del derecho a la intimidad.
b) La ley Orgánica 4/1997 de utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.
c) Ambas respuestas son correctas.

53. El consentimiento del titular requerido en la entrada en un domicilio se obtiene en base a:

a) El consentimiento de todos los titulares que pueda tener ese domicilio.
b) Solo se necesita el consentimiento de uno de sus titulares.
c) Basta con el consentimiento de un titular y la no oposición del resto.

54. La interceptación de comunicaciones está tipificada en el Código Penal en su artículo:

a) 264 y siguiente. *b) 197 y siguiente.* *c) 196.*

55. ¿Qué otro derecho fundamental interfiere especialmente en el derecho a la intimidad personal y familiar?:

a) El derecho al honor. *b) El derecho de información.* *c) El derecho a la propia imagen.*

56. Los operadores de telecomunicaciones tienen la obligación de guardar:

a) El contenido de las comunicaciones realizadas en sus medios.
b) Los datos generados en sus comunicaciones, pero no su contenido.
c) Tienen obligación de guardar tanto los datos generados en sus comunicaciones, como el contenido de las mismas.

57. Señala la respuesta que contenga datos que no deban guardarse referentes a comunicaciones telemáticas:

a) Los necesarios para identificar la localización del equipo de comunicación móvil
b) Datos para la identificación del contenido íntegro de la comunicación realizada.
c) Datos necesarios para rastrear e identificar el origen de una comunicación.

58. ¿Qué requisitos son imprescindibles que se cumplan en la denominada cadena de custodia?:

a) Autenticidad, inalterabilidad e indemnidad.
b) Al derecho de las comunicaciones.
c) A ambos derechos.

59. La intervención de un correo electrónico aun no leído por el destinatario, ¿a qué derecho fundamental afecta?:

a) Al derecho de la intimidad.
b) Al derecho al secreto de las comunicaciones.
c) A ambos derechos.

60. La calumnia o la injuria, ¿a qué derecho fundamental atentan particularmente?:

a) Al derecho a la intimidad personal.
b) Al secreto de las comunicaciones.
c) Al derecho al honor y la propia imagen.

61. ¿Cómo se denomina la figura creada por la institución 2/2011 del Fiscal General de Estado, en relación con la especialización fiscal sobre el ciberdelito?:

a) Fiscal de sala coordinador en materia de criminalidad informática
b) Fiscal especialista en ciberdelincuencia.
c) Fiscal de sala especialista en delincuencia informática.

62. ¿Qué especialidad de delincuencia informática fue pionera en el ciberdelito?:

a) Ciberterrorismo.
b) La cibercriminalidad en las redes sociales.
c) La delincuencia informática intrusiva.

63. Señala la respuesta que no corresponde con la idea que sobre el delito informático mantiene la Fiscalía General de Estado y, en general, todo el sistema penal español:

a) Cuando la utilización de las nuevas tecnologías resulte determinante en el desarrollo de la actividad delictiva.
b) Cuando la utilización de un sistema informático implique una mayor dificultad en la investigación del hecho e identificación de sus responsables.
c) Cuando en un delito se utilice un ordenador, sistema informático o cualquier otra tecnología de las conocidas TIC.

65. Una característica común de los delitos informáticos es:

a) La percepción, por la gran mayoría de personas, de que, dados los avances de las TIC, su intimidad no está amenazada.
b) Los sistemas de lucha contra el delito informático van por delante de la cibercriminalidad.
c) Una vez establecido un sistema de crimen informático, se perpetua de forma fácil por la automatización del proceso.

66. Para el Convenio de Budapest, interferencia de datos:

a) Son los actos deliberados que dañen, borren, deterioren, alteren o supriman datos informáticos.
b) Es la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático.
c) Es el acceso deliberado e ilegítimo a la totalidad o a una parte de un sistema informático.

67. El concepto "delitos relacionados con el contenido" de la Convención de Budapest se refiere exclusivamente a:

a) La intromisión en la intimidad.
b) La comisión de delitos con beneficio económico.
c) La pornografía infantil.

68. El Convenio de Budapest señala como delitos de pornografía infantil:

a) Su producción, oferta o puesta a disposición y su difusión a través de un sistema informático.
b) Su adquisición para uno mismo o para otros o su posesión en un dispositivo de almacenamiento de datos informáticos.
c) Ambas conductas.

69. ¿Qué acciones castiga el artículo 264 y concordantes del Código Penal español vigente?

a) Delitos de amenazas y coacciones.
b) Delitos de daños, sabotajes y denegación de servicios informáticos.
c) Falsedades documentales.

70. La obstaculización o interrupción ilícita del funcionamiento de un sistema informático lo contempla nuestro Código Penal en su artículo:

a) 264bis. *b) 264.* *c) 197.*

71. No está penada en nuestro Código Penal actual la siguiente acción:

a) Amenazas que no constituyan delito.
b) La adquisición sin autorización de una clave de acceso informático, sin llegar a utilizarla.
c) Las injurias que, por su naturaleza o efectos no sean consideradas en el concepto público como graves.

72. ¿Qué término reciben los ciberactivistas que rompen la protección de programas informáticos para obtener sus claves, compitiendo entre sí en ser los más activos en estas acciones?

a) Spoofingers. *b) Pishing.* *c) Warez.*

73. ¿Qué tiempo dura el mandato del director de la Agencia de Protección de Datos?:

a) 4 años.
b) 5 años.
c) Es un cargo funcionarial, por lo tanto, hasta su cese o jubilación.

74. ¿En qué tipo de especialidad delictiva informática se avisa a las víctimas, por medio de un correo electrónico o medio similar, para que entre en una web falsa que imita otra conocida por ellas?

a) Phishing. *b) Pharming.* *c) Spoofing.*

75. La difusión de noticias impactantes, tendenciosas y falsas, propagadas por Internet sobre nuevos virus o hecatombes informáticas, se conocen con el término:

a) Crimeware. *b) Hoax.* *c) Buggins.*

76. Los delitos de falsificación documental utilizando sistemas informáticos se encuadran en la clasificación de la Fiscalía General del Estado rn rl siguiente epígrafe:

a) Delitos en los que se atentan a los propios sistemas informáticos.
b) Delitos en los que las TIC ayudan a su ejecución.
c) Delitos en los que las TIC dificultan su investigación.

77. En caso de tratamiento de datos que se utiliza para cumplir las funciones de las administraciones públicas:

a) La recogida de datos debe ser autorizada por su titular.
b) La recogida y tratamiento de sus datos debe conocerla explícitamente su titular.
c) No es necesaria la autorización de su titular.

78. ¿Qué es el proceso de disociación respecto al tratamiento de datos?:

a) La operación de ceder los datos administrados a otra entidad distinta a la que cedieron por su titular.
b) Aquel tratamiento de datos personales que dé lugar a otro fichero cuyos datos no puedan identificarse o asociarse a personas en concreto.
c) La difusión de un fichero de datos a varias entidades solicitantes.

79. Señala un tipo de ficheros regulados por una normativa específica para esa materia:

a) Los ficheros de datos especialmente protegidos.
b) Los ficheros correspondientes a materias clasificadas.
c) Los ficheros derivados por el Registro Civil y Registro Central de Penales y Rebeldes.

80. ¿Qué significa exactamente el derecho de consulta al Registro General de Protección de Datos?:

a) Que el titular de datos almacenados en un fichero tiene derecho a saber de la existencia de ese fichero.
b) Que el titular de datos almacenados en un fichero tiene derecho a conocer qué datos suyos existen en ese fichero.
c) Que el titular de los datos almacenados en un fichero tiene derecho a impugnar los datos jurídicos derivados valorados en orden a un tratamiento de sus datos.

81. Ante la solicitud de datos sobre la ideología, religión o creencias solicitados a una persona:

a) El solicitante debe advertir al interesado acerca de su derecho a no prestarlos.
b) El solicitante deberá advertir al interesado que debe firmar un consentimiento escrito.
c) Las dos respuestas anteriores son correctas.

82. La reseña de detenidos que se otorga a toda persona acusada de delito y que pasa a disposición de la autoridad judicial está considerada como:

a) Fichero específico regulado por la LOPD.
b) Fichero de datos de carácter general.
c) Fichero regulado por una normativa específica.

83. La Ley Orgánica 4/1997, que regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, en cuanto a la garantía de la intimidad de las personas, impone la obligación de:

a) Avisar de la existencia de videocámaras en una determinada zona.
b) Indicar el lugar de donde se encuentra cada una de las videocámaras instaladas.
c) Avisar de que un determinado lugar puede contener o no videocámaras de control.

84. ¿En qué casos el artículo 55 de la Constitución Española suspende el derecho a la inviolabilidad del domicilio?:

a) En los estados de alarma, excepción y sitio.
b) En los estados de excepción y sitio.
c) Solo en estado de sitio.

85. En el delito de descubrimiento y revelación de secretos:

a) El perdón del ofendido anula la acción penal.
b) Es un delito público.
c) Se persigue a instancia de parte.

86. La vulneración del derecho al secreto de las comunicaciones se plasma en el Código Penal como delito de:

a) Calumnias e injurias.
b) Daños y sabotajes.
c) Descubrimiento y revelación de secretos.

87. El acceso a los datos almacenados en los soportes de información de los operadores de telecomunicaciones, por parte de los agentes de la policía judicial:

a) Debe estar amparado por una autorización judicial.
b) No necesitan autorización judicial para acceder a esos datos, pero sí al contenido del mensaje.
c) Solo pueden acceder a esta información los jueces o el Ministerio Fiscal directamente.

88. ¿Cómo se denomina el servicio de la Policía Nacional encargado de dirigirse a las operadoras de telecomunicaciones para solicitar datos generados por sus comunicaciones?:

a) SATEL. *b) RDSI.* *c) SITEL.*

89. ¿Qué procedimiento asegura que los datos obtenidos en un backup de un soporte de datos original se corresponden íntegramente con el original, a efectos judiciales?:

a) La certificación efectuada por el secretario judicial que presenció el volcado.
b) El acta de los funcionarios actuantes dando fe de la correspondencia en el contenido de ambos soportes.
c) El número hash de que se provee la copia.

90. La intervención telefónica vulnera el derecho al secreto de las comunicaciones garantizando en el artículo 18.3 de la CE pero, ¿en qué casos se concreta esta vulneración?:

a) Con el conocimiento del contenido de la comunicación.
b) Con el conocimiento del número con el que se comunica o la duración de la conferencia.
c) En ambos casos.

91. Además de la propia Constitución, ¿qué normativa protege civilmente el derecho a la intimidad y la propia imagen?:

a) La Ley Orgánica 1/1982.
b) La Ley Orgánica 15/1999.
c) La Ley Orgánica 4/2015.

92. ¿Qué países participaron como estados observadores en el Convenio de Budapest sobre ciberdelincuencia?:

a) Japón, China y Estados Unidos.
b) Estados Unidos, China y Rusia.
c) Canadá, Japón y China.

93. Al apoderamiento ilícito de secretos e información personal y que afecta, por tanto, a la intimidad de las personas, se le denomina genéricamente:

a) Ciberdelincuencia social. *b) Ciberdelincuencia intrusiva.* *c) Cibersabotaje.*

94. Todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de algunos de sus elementos , sea el tratamiento automatizado de datos en ejecución de un programa, es, para la Convención de Budapest:

a) Un sistema informático.
b) Un sistema proveedor de servicios.
c) Todo elemento correspondiente a un sistema informático.

95. El servicio disponible en los teléfonos móviles que permite el envío de mensajes cortos entre ellos se conoce por siglas:

a) MMS. *b) GPRS.* *c) SMS.*

96. Una de las intenciones del Convenio de Budapest sobre cibercriminalidad es:

a) Unificar las penas de cada uno de estos delitos por parte de todos los países firmantes.
b) Unificar conceptos relativos a estas acciones para que se incluyan en los textos penales como delitos, por los países firmantes.
c) Implantar un sistema penal común respecto a los delitos informáticos.

97. Para la <u>Convención de Budapest</u>, la producción, venta u obtención de cualquier dispositivo o programa para atacar de alguna forma un sistema informático, es:

a) Interferencia en el sistema. *b) El fraude informático.* *c) Acceso ilícito.*

98. Señala <u>una acción catalogada en la Convención de Budapest</u> como cibercrimen en la que el autor deba obtener, para su consideración como tal, un beneficio económico o la victima un perjuicio patrimonial:

a) La falsificación informática.
b) El fraude informático.
c) La pornografía infantil.

99. Señala <u>una clasificación que no se corresponda</u> con ningún grupo clasificatorio establecido por la Fiscalía General del Estado respecto a los delitos informáticos:

a) Delitos en los que el objeto de la actividad delictiva son los propios sistemas informáticos o las TIC.
b) Delitos en los que la actividad criminal se sirve para su ejecución de las ventajas que ofrecen las TIC.
c) Delitos relacionados con infracciones al derecho a la propiedad intelectual y a los derechos afines.

100. Para <u>mayor garantía y para mantener la inalterabilidad</u> del contenido de un ordenador intervenido se debe precintar sellar:

a) El ordenador en si mismo.
b) Cada una de las ranuras de entrada de datos en el ordenador.
c) No se realiza ninguna operación específica a este respecto, pues la presencia del secretario judicial en el registro es suficiente garantía.

<u>PREGUNTAS DE RESERVA</u>

1. ¿Es <u>necesaria la presencia de asistencia</u> letrada en la entrada y registro autorizada por el mandamiento judicial?:

a) Si, además es irrenunciable.
b) No, aunque se recoge esta posibilidad a petición del interesado.
c) No; la única presencia permitida es la de los funcionarios actuantes y el titular inmueble.

2. Un <u>flood o flooder</u> se define como:

a) Programa que se utiliza para enviar mensajes repetidamente, y de forma masiva, mediante correo electrónico, sistemas de mensajería instantánea, chat, foros, etc. El objetivo de este comportamiento es provocar la saturación o colapso de los sistemas a través de los que se envía el mensaje.
b) Programa que aprovecha los fallos de seguridad, defectos o vulnerabilidades de otros programas o sistemas informáticos con el fin de obtener algún tipo de beneficio o llevar a cabo una acción concreta, como acceder a recursos protegidos, controlar sistemas sin autorización, etc.
c) Programa que se instala en un equipo con el fin de modificar los datos de acceso a Internet para que, al realizar la conexión a través de un módem, se utilice un número de traficación adicional.

3. ¿ Cuales son los <u>sistemas de protección</u> de cortafuegos ?

a) Antivirus correo electrónico.
b) Antispam, Antitroyanos y Antivirus.
c) Antispam yTodas son verdaderas.

4. El uso de redes " <u>P2P</u> " están pensadas para el intercambio de.. ?

a) Archivos *b) Datos.* *c) Ingernet*

5. ¿ Qué es un " <u>antivirus</u> " ?

a) Programas que se instalan inadvertidos
b) Redes sociales que se descargan
c) Un sistema de seguridad vial y de conexión interna en el ordenador

6. Método de protección contra la publicidad.

a) Antispam *b) Antitroyanos* *c) Antimosquitos*