1. ***Cuando nuestro servidor ha sido objeto de un ataque de flood, ¿ qué debemos entender que ha ocurrido ?***
   - *a) Nuestro servidor ha sido infectado con malware, provocando que enviemos masivamente correos o nuestros contactos.*
   - *b) Que la sala de servidores ha sido inundada por una manipulación en el alcantarillado.*
   - *c) Que nuestro servidor ha sufrido la saturación por la publicación de una gran cantidad de mensajes no deseados.*
2. ***Si nuestra medida de intervención telemática afecta a un tercero no investigado a priori, deberemos paralizar nuestra investigación, salvo:***
   - *a) Ninguna es correcta*
   - *b) Que los medios del tercero se están utilizando maliciosamente por el autor sin su conocimiento.*
   - *c) Que el titular de la línea no se haya percatado de la intervención.*
3. ***Su función es interceptar las pulsaciones que se teclean en el sistema y tener acceso a los datos pesonales:***
   - *a) Dropper* *b) Typosquatter* *c) Keylogger*
4. ***Práctica consistente en investigar y publicar información privada extraída de internet sobre una persona u organización:***
   - *a) Doxing* *b) Fooding* *c) Banneo*
5. ***¿ Cómo se denomina al programa informático que se instala en nuestro ordenador de manera inesperada y sin nuestro permiso, en la que el usurario lo confunde con un programa totalmente legítimo, pero al ejecutarlo, puede llegar a permitir que otro usuario se haga con el control del ordenador ?***
   - *a) Hoax* *b) Gusano* *c) Troyano*
6. ***¿ Cómo se denomina el envio de imágenes de contenido sexual producidos por el propio remitente a otras personas por medio de teléfonos móviles ?***
   - *a) Grooming* *b) Starking* *c) Sexting*
7. ***Phishing:***
   - *a) Es una estafa por medio de mansajes sms, con ofertas interesantes o la concesión de fabulosos premios.*
   - *b) Es el métido utilizado para engañar y conseguir información personal mediante el envio de correos electrónicos fraudulentos o dirigiéndose a un sitio web falso.*
   - *c) Es un término de naturaleza informática para denominar un nuevo tipo de delito.*
8. ***Una botnet se refiere a:***
   - *a) Un tipo de red segura dentro de la intranet.*
   - *b) Una red de ordenadores que han sido infectados por programas nocivos.*
   - *c) Una red de buscadores que recopila automáticamente información de internet.*
9. ***La resolución por solicitudes de instalaciones fijas de vidiocámaras corresponderá al Delegado de Gobierno. ¿ De qué plazao dispone éste para la resolución del procedimiento ?***
   - *a) En el plazo máximo de dos meses, contados a partir del día siguiente al de la presentación de la solicitud.*
   - *b) En el plazo máximo de un mes, contados a partir del día siguiente al de la presentación de la solicitud.*
   - *c) En el plazo máximo de dos meses, contados a partir del día de la presentación de la solicitud.*
10. ***El Convenio sobre Cibercriminalidad se firma en el ámbito del Consejo de Europa el 23 de noviembre de 2001. ¿ Cuándo entró en vigor de forma general ?***
    - *a) El 20 de mayo de 2010* *b) El 1 de julio de 2004* *c) El 10 de agosto de 2006*
11. ***Según el Artículo 579 del Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal, el juez podrá acordar, en resolución motivada, la observación de las comunicaciones postales y telegráficas del investigado, así como de las comunicaciones de las que se sirva para la realización de sus fines delictivos por un plazo de:***
    - *a) Hasta tres meses, prorrogable por iguales o superiores periodos hasta un máximo de dieciocho meses.*
    - *b) Hasta tres meses prorrogable por iguales periodos hasta un máximo de dieciocho meses.*
    - *c) Hasta tres meses, prorrogable por iguales o inferiores periodos hasta un máximo de dieciocho meses.*
12. ***¿ Qué es el " flaming " ?***
    - ***a**) Mensajes ofensivos a través de internet.*
    - *b) Técnica empleada por hackers para saltarte las protecciones de firewalt de protección de sus víctimas.*
    - *c) Técnica de formateo del disco duro interno del ordenador para evitar que nadie se haga con dicha información.*
13. ***Según el Real Decreto 596/1999, de 16 de abril, por el que se aprueba el Reglamento de desarrollo y ejecución de la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, ¿ a quién corresponde la presidencia de la Comisión de Garantías de Videovigilancia ?***
    - *a) Presidente del Tribunal Superior de Justicia de la CCAA.*
    - *b) Presidente del Tribunal Supremo.*
    - *c) Directora de la Agencia Española de Protección de Datos.*
14. ***El tipo de hackers que utilizan sus conocimientos para cometer actividades ilegales, extorsionar, ciberdelitos… se conoce con el nombre de:***
    - *a) Black hat hacker* *b) Grey hat hacker* *c) White hat hacker*
15. ***¿ Cómo se denomina el " bullying " en el entorno laboral ?***
    - *a) Adult grooming* *b) Moobing* *c) Child grooming*

16. El <u>miedo</u> a quedarse sin dispositivo móvil se define como:

a) Movilofobia *b) Nomofobia* *c) Aporofobia*

17. Las medidas impuestas por el <u>Juez de registros remotos</u> sobre equipos informáticos tendrán una duración de:

a) La medida tendrá una duración máxima de tres meses, prorrogables por periodos sucesivos de igual o inferior duración hasta el plazo máximo de dieciocho meses.

b) La medida tendrá una duración máxima de un mes, prorrogable por iguales periodos hasta un máximo de tres meses.

c) La medida tendrá duración máxima de un mes, prorrogable por iguales o inferiores periodos hasta máximo de 3 meses.

18. Según el <u>Real Decreto 596/1999, de 16 de abril</u>, por el que se aprueba el Reglamento de desarrollo y ejecución de la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos. Las instalaciones fijas de videocámaras que realicen las Fuerzas Armadas y las Fuerzas y Cuerpos de Seguridad en sus inmuebles, ¿ <u>serán susceptibles de la aplicación de dicho Reglamento</u> ?

a) No se les aplicará en ningún caso.

b) Se les aplicará en todo caso.

c) No se aplicará siempre que éstas se dediquen exclusivamente a garantizar la seguridad y protección interior o exterior de los mismos.

19. El <u>tipo de hacker que descubre una vulnerabilidad</u> y se ofrece a arreglarla, a particulares o empresas, a cambio de una prestación económica es un:

a) Grey hat hacker *b) Black hat hacker* *c) White hat hacker*

20. Según el <u>Artículo 598 ter g</u>. del Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuciamiento Criminal, la autorización para la interceptación de las comunicaciones telefónicas y telemáticas tendrá una duración de:

a) Seis meses, prorrogables por periodos sucesivos de igual duración hasta el plazo máximo de dieciocho meses.

b) Tres meses, prorrogables por periodos sucesivos de igual o inferior duración hasta el plazo máximo de 18 meses.

c) Tres meses, prorrogables por periodos sucesivos de igual duración hasta el plazo máximo de dieciocho meses.

21. Según el <u>Convenio sobre Ciberdelincuencia</u>, hecho en Budapest el 23 de noviembre de 2002, por " pornografía infantil " entenderá todo material pornográfico que contenga la representación visual de.

a) Ambas son correctas.

b) Una persona que parezca un menor comportándose de una forma sexualmente explícita.

c) Un menor comportándose de una forma sexualmente explícita.

22. " <u>Alert Cops</u> " es una aplicación móvil official del Ministerio del Interior que permite avisar:

a) A las Fuerzas y Cuerpos de Seguridad del Estado.

b) A las Fuerzas y Cuerpos de Seguridad.

c) A las Fuerzas y Cuerpos de Seguridad del Estado, además de las policías localesy y autonómicas.

23. En el ámbito de los delitos informáticos, ¿ qué es un " <u>ransomware</u> " ?

a) Un virus que bloquea el contenido de un ordenador y solicita un rescate a cambio de desencriptarlo.

b) Un programa que desfigura visualmente la página web para publicar en ella un mensaje.

c) Un programa que se instala en el ordenador y realiza llamadas a numerous de tarificación adicional sin que el usuario sepa (también conocido como NTA).

24. Según el <u>Artículo 282 bis del Real Decreto</u> de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuciamiento Criminal, la identidad supuesta será otorgada por el Ministerio del Interior por el plazo de:

a) Seis meses prorrogables por periodos de igual duración.

b) Seis meses prorrogables por periodos de igual duración hasta un máximo de 18 meses.

c) Seis meses prorrogables por periodos de igual o inferior duración.

25. ¿ En qué se basa el conocido como " <u>Pump and Dump</u> " ?

a) Delincuentes que acceden a las cuentas de varios clients de la bolsa y las utilizan para alzar el precio de las acciones y luego venderlas.

b) Se basa en la especulación de criptodivisas, donde se pretende minar información encriptada para luego venderla en forma de Bitcoin.

c) Se basa en abrir operaciones con activos tanto en compra como en venta para compensar las ganancias de unos activos con las pérdidas de los otros.

26. Corresponde la <u>investigación de actividades delictivas</u> que afecten a la seguridad lógica y a los fraudes dentro del CNP:

a) Brigada Central de Investigación Tecnológica.

b) Brigada Central de Seguridad Informática.

c) Grupo de Delitos Telemáticos.

27. La <u>diferencia básica</u> entre delito informático y la criminalidad informática es:

a) No hay ningún tipo de diferencia, ambas se castigan conforme al Código Penal.

b) Una se comete mediante la informática y otra la utiliza como medio.

c) Además de la anterior, se diferencia en su punibilidad.

28. <u>De entre los delitos que se pueden cometer a través de internet</u>, ¿ cuál de los siguientes necesita de la interposición de una querella para poder ser perseguido ?

a) Hurtos y fraudes *b) Calumnia e injurias.* *c) a y b, son correctas.*

29. La Ley Orgánica de Protección de datos de character personal, define a los " <u>datos de carácter personal</u> " como:

a) Cualquier información concerniente a personas físicas identificadas o identificables.

b) Cualquier información concerniente a personas físicas identificables.

c) Cualquier información concerniente a personas físicas y/o jurídicas identificadas o indentificables.

30. Asociación en red de máquinas autónomas que forman un grupo de equipos que ejecutan una aplicación controlada y manipulada, que controla todos los ordenadores/servidores infectados de forma remota y que pueden emplearse para robar datos o apagar un sistema.

a) Crackers *b) Net Bots* *c) Botnets*

31. Delitos de estafa a través de la manipulación de datos o programas para la obtención de un lucro ilícito, son considerados como:

a) Fraudes informáticos *b) Sabotajes informáticos* *c) Rodos informáticos*

32. El " Vishing " es:

a) Fraude que persigue el mismo fin que el " Phishing ", es decir, la obtención de datos confidenciales de usuarios pero a través de la IP.

b) Acceso a las cuentas de muchos clients para alzar el precio de acciones modestas.

c) Fraude conocido como microespías.

33. Se entiende como sistema informático según el Convenio Sobre la Ciberdelincuencia:

a) Cualquier representación de hechos, información o conceptos de una forma que permita el tratamiento informático, incluido un programa diseñado para que un sistema informático ejecute una función.

b) Todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa.

c) Ambas son correctas.

34. Los dispositivos electrónicos pueden ser ocupados o aprehendidos en tres supuesto, que serían:

a) Como pieza de convección. *b) Como cuerpo o instrument del delito.* *c) Ambas son correctas.*

35. Aquellos foros de cotilleos, chismes, diramaciones etc., sobre algunos compañeros que causan situaciones muy gravosas tanto para las personas objetos de los rumores como para los que los propagan, son llamados:

a) Gossping *b) Blogs* *c) Ambas son correctas*

36. Entre las herramientas delictivas digitales más destacadas, existen unos programas que registran cada tecla del ordenador que pulsa el usuario y que se utilizan para intentar descubrir contraseñas, por tanto, hablamos de:

a) Keyloggers *b) Keyransom* *b) Ransomioggers*

37. El colectivo que conoce el funcionamiento de los sistemas telefónicos y se dedica a alterar el comportamiento de los mismos, es conocido como:

a) Phoneaker *b) Phrealker* *c) Wannaber*

38. Cuando un programa se instala en una computadora y proporciona al intruso un control absolute sobre el equipo, aludimos a los programas:

a) Zombi

b) Inertes

c) Inactivos o adormecidos, pues el intruso tiene pleno control sobre el ordenador sin que el propietario se percate de la situación.

39. Los dispositivos que constituyan prueba digital, se incorporan al proceso bajo la responsabilidad de:

a) Del Secretario Judicial. *b) Del Juez de Instrucción.* *c) Del Letrado de Oficio.*

40. ¿ Qué tribunal reconoció como derecho fundamental el " Habeas Data " ?

a) El Tribunal Constitucional.

b) El Tribunal Europeo de Derechos Humanos.

c) El Tribuinal Supremo.

41. Según el Convenio sobre la Ciberdelincuencia:

a) Cada parte designa un punto de contacto disponible 24 horas del día, 7 días a la semana conocida como RED 24/7.

b) Cada parte debe adoptar medidas legislativas para tipificar como delito en su derecho interno, conoductas como falsificación informática, fraude informático, delitos relacionados con la pornografía infantil, etc.

c) Ambas son correctas.

42. Imágenes transparentes dentro de una página web o denetro de un correo electrónico con un tamaña de 1 x 1 pixeles utilizadas para obtener información del usuario:

a) Web bug. *b) Spoofing.* *c) Googlebug.*

43. Nos mandan un mensaje a través de Facebook, prometiéndonos que rellenando unos formularios, vamos a ganar mucho dinero en poco tiempo, esta práctica se conoce como:

a) Estafa *b) Malware* *c) Hoax*

44. Viola la seguridad de un sistema informático de forma similar a como lo hace un hacker, con la diferencia que lo hace con fines de aprovechamiento personal o para hacer daño:

a) Cracker *b) Es la definición propia de hacker.* *c) Pracker*

45. Se encarga de llevar a cabo una serie de " alerta tecnológica " para mantener informado a los ciudadanos a través de las redes sociales o desde su propia web, de los timos, SPAM, hoax, etc:

a) Brigada Central de Seguridad Informática.

b) Brigada Central de Investigación Informática.

c) Brigada Central de Investigación Tecnológica.

46. ¿ Se considera el " Troyano " un virus informático ?

a) Si, y afecta al software.

b) No, ya que no cumple con todas las características de los mismos.

c) Si, y afecta al hadware.

47. ¿ De qué Comisaría depende la Unidad que asume la investigación y persecución de las actividades delictivas que impliquen la utilizaicón de las tecnologías de la información y las comunicaciones y el ciberdelito de ámbito nacional y transnacional, relacionadas con el patrimonio, consumo, protección al menor, pornografía infantil, etc ?

a) Comisaría General de Seguridad Ciudadana.
b) Comisaría General de Información.
c) Comisaría General de Policía Judicial.

48. Cuando se nos " cuela " un troyano en nuestro ordenador, debido a que iba en un programa con la misión de obtener un beneficio, causando un perjuicio en el sistema informático, hablamos de:

a) Malware *b) Software* *c) Hoax*

49. Situación en que una persona o grupo de personas ejercen una violencia psicológica extrema, de forma sistemática, durante un tiempo prolongado sobre otra persona en el lugar de trabajo:

a) Booling. *b) Pooting.* *c) Moobing.*

50. Será el encargado de promover las acciones pertinentes con objeto de privar de la patria potestad, tutela, guarda o acogimiento familiar, en su caso, a la persona que incurra en alguna de las conductas descritas en referencia a la omisión de ayuda a menores o discapacitdos para impedir que siga ejerciendo la prostitución:

a) El Juez de Menores *b) El Ministerio Fiscal* *c) El Juzgado de Instrucción*

51. ¿ Qué nombre recibe el software que despliega publicidad de distintos productos o servicios ?

a) Botnets *b) Adware* *c) Backdoors*

52. Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias:

a) Tratamiento de datos *b) Fuentes de datos* *c) Procesamiento y cesión de datos*

53. ¿ Están permitidos, según la LECr, como medios de prueba la palabra, el sonido y la imagen ?

a) Si, salvo la palabra
b) Si, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas.
c) No, por ello no permite las grabaciones como medio de prueba en un juicio.

54. Se considera delito adquirir, producir, importar o proporcionar a terceros una contraseña de ordenador que permita acceder a la totalidad o a una parte de un sistema de información:

a) Si. *b) No se considera delito.* *c) Solo si son códigos de acceso.*

55. Aquella técnica que desvia el tráfico de internet de un sitio Web hacia otro de apariencia similar para que los usuarios que se registren en la base de datos del sitio falso depositen datos y demás, es llamada:

a) Scareware. *b) Ransomware* *c) Pharming*

56. La finalidad del " Phishing " es:

a) Demostrar la habilidad del hacker.
b) Usar la información conseguida para realizar compras por internet, transferencias bancarias o retiros de dinero en efectivo a nombre de la víctima del fraude o estafa.
c) Vulnerar los sistemas de seguridad de las grandes entidades bancarias.

57. ¿ Qué acción realizan los programas denominados secuestradores ?

a) Cifran archivos importantes para el usuario y piden un rescate para poder recibir la contraseña que permite recuperaralos.
b) Son conocidos como programas " phishing ".
c) Este tipo de programas no existen.

58. El término " ingeniería social " dentro de la seguridad informática, es:

a) La práctica para obtener información confidencial a través de la manipulación de usuarios legítimos.
b) No existe dicho término a nivel de seguridad informática, si el de " ingeniería rastreadora ".
c) La práctica para facilitar la información confidencial a través de la manipulación de usuarios legítimos.

59. Con el fin de criminalizar los actos de racismo y xenofobia cometidos mediante sistemas informáticos se promulgo una norma conocida como:

a) Primera enmienda para la erradicación del racismo y xenofobia.
b) Convenio de Budapest.
c) Protocolo Adicionoal al Convenio de Ciberdelincuencia del Consejo de Europa.

60. La fuente de la prueba digital radica en:

a) La forma a través de la cual esa información entra en el proceso.
b) La información contenida o transmitida por medios electrónicos.
c) Ambas son correctas.

61. ¿ Qué buscaba el " Convenio de Budapest ", con respecto a los delitos informáticos y a los delitos en Internet ?

a) Hacer frente a los delitos descritos mediante la amortización de leyes nacionales, la mejora de las técnicas de investigación y el aumento de la cooperación entre las naciones.
b) Hacer frente a los delitos descritos mediante la modalidad y coordinación de toda la materia de criminalidad informática.
c) Realizar y generalizar las acciones criminales en la interconexión de las redes sociales para hacer frente a los delitos.

62. Si hablamos de: " La información con valor probatorio en todo proceso abierto – para cualquier infracción penal y no solo para delitos informáticos- que esté contenida en un medio electrónico o transmitida por dicho medio ", nos referimos:

a) Redes públicas *b) Prueba digital o prueba electrónica.* *c) Correo electrónico procesal.*