MINISTERIO
DE CIENCIA, INNOVACIÓN
Y UNIVERSIDADES

CSIC
CONSEJO SUPERIOR DE INVESTIGACIONES CIENTÍFICAS

PROCESO SELECTIVO POR EL SISTEMA DE PROMOCIÓN INTERNA PARA INGRESO EN LA ESCALA DE TÉCNICOS SUPERIORES ESPECIALIZADOS DE LOS ORGANISMOS PÚBLICOS DE INVESTIGACIÓN, CONVOCADO POR RESOLUCION DE 24 DE MAYO DE 2024 (BOE Nº 131 DE 30 DE MAYO)

Cuestionario del primer ejercicio

A6 – CIENCIA DE DATOS

Especialidad: D4 – SEGURIDAD INFORMÁTICA

- No abra el **CUESTIONARIO** ni empiece el examen hasta que se le indique.
- Solo se calificarán las respuestas marcadas en la **HOJA DE RESPUESTAS**
- El cuestionario consta de **80 preguntas**, cada una de ellas con **cuatro respuesta alternativas**, de las cuales **sólo una de ellas es correcta**.
- Una vez abierto el cuestionario, compruebe que consta de todas las páginas y preguntas y que sea legible. En caso contrario solicite uno nuevo al personal del aula.
- Las **contestaciones erróneas se PENALIZARÁN** con un 25 % de su valoración.
- Lea atentamente las **instrucciones** para contestar la **HOJA DE RESPUESTAS**, que figuran al dorso de la misma.
- Cumpllimente los datos personales y firme la **HOJA DE RESPUESTAS**.
- El tiempo para la realización de este ejercicio será de **noventa (90) minutos**.
- **NO SEPARE** ninguna de las copias de la **HOJA DE RESPUESTAS**. Una vez finalizado el ejericio, el personal del aula le indicará los pasos a seguir.
- El **CUESTIONARIO** se podrá utlizar como borrador y se podrá llevar por el opositor al finalizar el tiempo marcado para el ejercicio.

Barcelona 20 de septiembre de 2024

1. Indicar de las siguientes características cuál NO se corresponde con el modelo de computación en la nube:

A) Acceso bajo demanda.

B) Flexibilidad en la configuración de los recursos.

C) Elasticidad y rapidez en el aprovisionamiento de recursos.

D) Dependencia de recursos físicos locales.

2. La virtualización de recursos consiste en:

A) El conjunto de técnicas software que permiten abstraer las características físicas de un computador, de forma que se puedan ejecutar diferentes máquinas virtuales.

B) La utilización de máquinas virtuales hardware para proporcionar acceso al software existente en un sistema para un grupo virtual de usuarios.

C) La explotación de organizaciones virtuales para el aprovisionamiento de recursos de computación a gran escala, especialmente en colaboraciones científicas.

D) La sustitución de los recursos humanos de una organización por asistentes basados en inteligencia artificial.

3. Indicar cuál de los siguientes conceptos NO es una propiedad de seguridad de un activo de información en una organización.

A) Confidencialidad.

B) Integridad.

C) Migralidad.

D) Autenticidad.

4. Indicar cuál de los siguientes es un motor de bases de datos relacional:

A) MariaDB.

B) MongoDB.

C) Apache Cassandra.

D) Amazon DynamoDB.

5. ¿Cuál de las siguientes características es fundamental en el desarrollo de software abierto?

A) Código cerrado y restrictivo.

B) Licencias propietarias.

C) Colaboración y transparencia.

D) Propiedad exclusiva del autor.

6. ¿Cuál de las siguientes afirmaciones es correcta acerca del aprendizaje automático (machine learning)?

A) El aprendizaje automático se refiere únicamente a la capacidad de las máquinas para procesar grandes volúmenes de datos.

B) El aprendizaje automático es un enfoque que permite a las máquinas aprender y mejorar automáticamente a través de la experiencia sin ser programadas explícitamente.

C) El aprendizaje automático solo se aplica en la investigación científica y no tiene aplicaciones en otros campos.

D) El aprendizaje automático es una técnica exclusiva de la programación orientada a objetos.

7. ¿Qué es un Data Management Plan (Plan de Gestión de Datos)?

A) Un plan para la eliminación de datos obsoletos y sin valor.

B) Un plan para asegurar que los datos sean inaccesibles y no puedan ser utilizados.

C) Un plan que establece cómo se gestionarán, organizarán, almacenarán y compartirán los datos durante un proyecto de investigación.

D) Un plan que prioriza la recopilación de datos sin tener en cuenta su calidad o relevancia.

8. ¿Cuál de los siguientes métodos es un ejemplo de accounting en los Sistemas de Autorización, Autenticación y Accounting?

A) Control de acceso físico.

B) Registro de tiempos de sesión.

C) Cifrado de datos.

D) Detección de intrusiones.

9. ¿Qué es GitHub?

A) Una plataforma de desarrollo colaborativo.

B) Un sistema operativo .

C) Un lenguaje de programación.

D) Un motor de búsqueda.

10. En un CPD de un centro de investigación se va a adquirir un Sistema de Alimentación Ininterrumpida (SAI) y tenemos las siguientes especificaciones: 500 VA (Voltiamperios) y 300 W (watios), que indican:

A) La potencial real y la potencia aparente respectivamente del SAI.

B) La energía eléctrica y la potencia que puede suministrar el SAI.

C) La potencia aparente y la potencia real del SAI.

D) La potencia del SAI solo que dados en dos unidades diferentes de potencia.

11. En el contexto de seguridad de sistemas informáticos, la autenticación:

A) Otorga certificados digitales a los recursos que están disponibles.

B) Confirma la disponibilidad de los recursos.

C) Confirma que los usuarios son quienes dicen ser validando su identidad.

D) Proporciona permisos de acceso a los datos almacenados en los recursos.

12. ¿Cuál de estos lenguajes proporciona una plataforma unificada y un modelo de programación que permite la programación paralela de GPUs, CPUs, DSPs y FPGAs?

A) OpenCL.

B) OpenMP.

C) CUDA.

D) SYSCL.

13. ¿Cuál de las siguientes afirmaciones sobre XML es correcta?

A) XML es un modelo de metadatos utilizado para describir la presentación de una página web

B) XML es un lenguaje de programación utilizado para crear páginas web interactivas.

C) XML es un lenguaje de marcado que permite definir etiquetas personalizadas para estructurar y almacenar datos.

D) XML es un formato de imagen utilizado para gráficos y multimedia en la web

14. Indica cuál de estos sistemas operativos es de tiempo real

A) QNX

B) Fedora Linux

C) Windows RT

D) Minix

15. ¿Cuál de las siguientes afirmaciones describe mejor el concepto de escalabilidad en la computación científica en la nube?

A) Se refiere a la capacidad de almacenar grandes cantidades de datos científicos en la nube, en escalas mayores del Petabyte.

B) Implica la posibilidad de acceder a recursos de cómputo adicionales según las necesidades del usuario.

C) Significa utilizar software especializado en la nube para realizar cálculos científicos complejos.

D) Se refiere a la colaboración y el intercambio de datos científicos entre diferentes investigadores en las diferentes escalas o etapas de la investigación.

16. De entre las siguientes funcionalidades, indica cuál NO está relacionada con la gestión ágil de proyectos:

A) Diagramas de Gantt interactivos.

B) Tableros Kanban.

C) Hojas de ruta de commits automatizados.

D) Planificación de minitrabajos Sprints.

17. ¿Qué función principal tiene un sistema de control de versiones en un repositorio digital de software?

A) Almacenar y organizar los archivos de código fuente.

B) Permitir a los desarrolladores colaborar y trabajar en equipo en el mismo proyecto.

C) Gestionar y rastrear los cambios realizados en los archivos a lo largo del tiempo.

D) Compilar y ejecutar el software en diferentes entornos de desarrollo.

18. En la programación orientada a objetos, una clase es:

A) Una plantilla en la que se definen los los atributos y métodos predeterminados de un tipo de objeto.

B) Una propiedad que permite subdividir una aplicación en partes más pequeñas e independientes de la aplicación en sí.

C) Una técnica por la cual el entorno de objetos se encarga de destruir automáticamente los objetos no referenciados.

D) Una ubicación de almacenamiento abstracta asociada a un nombre simbólico, que contiene una cantidad de información conocida.

19. ¿En qué consiste el aprendizaje no supervisado?

A) Un tipo de aprendizaje en el que no se utilizan etiquetas para entrenar el modelo.

B) Un tipo de aprendizaje que solo se aplica a problemas de regresión.

C) Un tipo de aprendizaje que utiliza redes neuronales recurrentes (RNN).

D) Un tipo de aprendizaje que utiliza regresión logística.

20. ¿Cuál de las siguientes opciones describe qué es Big Data?

A) Una cantidad de datos que es demasiado grande para ser procesada por sistemas tradicionales.

B) Un conjunto de herramientas utilizadas para el procesamiento de datos en tiempo real.

C) Una base de datos de gran tamaño.

D) Una técnica para el análisis de datos utilizando algoritmos de inteligencia artificial.

21. ¿Qué es una TPU?

A) Es una unidad de procesamiento gráfico.

B) Es una unidad de procesamiento central.

C) Es una unidad de procesamiento tensorial.

D) Es una unidad de procesamiento vectorial.

22. El aprendizaje automático se ha visto revolucionado en los últimos años por la evolución de distintas formas de computación basada en redes neuronales. El factor clave para el uso extendido de estos nuevos algoritmos ha sido

A) El rápido acceso a disco.

B) La eficiente implementación en Unidades Centrales de Procesamiento.

C) La eficiente implementación en Unidades Graficas de Procesamiento.

D) La reducción de la latencia en la transmisión de información.

23. La principal característica de un sistema de tiempo real es:

A) Disponer de un planificador basado en prioridades.

B) Respuesta a interrupciones con niveles de prioridad.

C) Respuesta a los eventos dentro de un plazo determinado.

D) Ausencia de gestor de memoria virtual.

24. El soporte y coordinación para el tratamiento de vulnerabilidades y la resolución de incidentes de seguridad que tengan las Administraciones de las Comunidades Autónomas corresponde a:

A) INCIBE-CERT.

B) CCN-CERT.

C) Al CERT correspondiente de la Comunidad Autónoma.

D) Al CERT del Ministerio de Defensa.

25. ¿Cuál es el protocolo más común para iniciar una sesión remota segura mediante línea de comandos a una máquina Linux?

A) SSH.

B) Telnet.

C) RDP.

D) VPN.

26. ¿Cuál de las siguientes técnicas se utiliza para reducir la dimensionalidad de los datos en aprendizaje profundo?

A) Data augmentation (aumento de datos).

B) Reducción de ruido.

C) Redes neuronales convolucionales (CNN).

D) Análisis de componentes principales (PCA).

27. ¿Cuál de las siguientes bibliotecas NO es ampliamente utilizada para implementar deep learning en Python?

A) TensorFlow.

B) Scikit-learn.

C) PyTorch.

D) Wamba.

28. Respecto a la metodología MAGERIT y la gestión de riesgos, el riesgo calculado, tomando en consideración el valor propio de un activo y el valor de los activos que dependen de él, se denomina:

A) Riesgo inherente.

B) Riesgo repercutido

C) Riesgo acumulado.

D) Riesgo total.

29. ¿Qué objetivo principal tienen las normativas STIC?

A) Establecer requisitos técnicos específicos para la infraestructura de telecomunicaciones.

B) Proporcionar directrices para la seguridad y protección de la información en sistemas y redes.

C) Regular el uso de dispositivos de almacenamiento portátiles.

D) Controlar el acceso a las redes sociales en el ámbito laboral.

30. ¿Cuál es una de las recomendaciones generales de las normativas STIC para la protección de datos?

A) Desactivar todos los sistemas de seguridad para mejorar el rendimiento.

B) Realizar auditorías periódicas y revisiones de seguridad.

C) Usar contraseñas predeterminadas para todos los sistemas.

D) Permitir el acceso sin restricciones a todos los datos.

31. La guía de auditoria de cumplimiento del Esquema Nacional de Interopoperabilidad (ENI) establece una lista de controles que se estructuran en las tres categorías siguientes:

A) Marco organizativo, marco funcional y medidas técnicas.

B) Marco funcional, marco técnico y marco operacional.

C) Marco organizativo, marco funcional y marco técnico.

D) Marco organizativo, marco operacional y medidas técnicas.

32. Según el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, ¿cuál de las siguientes NO es una de las funciones que desempeñarán, como mínimo los CSIRT?

A) Supervisar incidentes a escala internacional.

B) Difundir alertas tempranas, alertas, avisos e información sobre riesgos e incidentes entre los interesados.

C) Efectuar un análisis dinámico de riesgos e incidentes y de conocimiento de la situación.

D) Responder a incidentes.

33. Sobre los ataques CSRF (Cross-Site Request Forgery), ¿cuál de las siguientes afirmaciones NO es cierta?

A) Este ataque se puede realizar mediante XSS (Cross-Site Scripting) usando un objeto Image.

B) Permite al atacante generar peticiones a sitios web de terceros empleando los datos de autenticación del usuario víctima.

C) Este ataque se puede realizar mediante XSS (Cross-Site Scripting) usando un objeto XMLHttpRequest.

D) Este tipo de ataque es fácilmente identificable por el usuario y el navegador, existiendo mecanismos para mitigarlo.

34. Un ataque Port Stealing es

A) Un tipo de ataque DoS (Denial of Service).

B) Un tipo de ataque DDoS (Distributed Denial of Service).

C) Un tipo de ataque MitM (Man in the Middle).

D) Un tipo de ataque XSS (Cross Site Scripting).

35. ¿Cuál de los siguientes mecanismos NO está relacionado con la autentificación/autorización de los servidores de correo para el envío de mensajes de un dominio?

A) DKIM.

B) SPF.

C) MKY.

D) DMARK.

36. Con respecto a la seguridad en dispositivos y en el backend, indica cuál es la afirmación correcta

A) Tanto Oauth como OpenID Connect son soluciones para autenticación.

B) Tanto Oauth como OpenID Connect son soluciones para autorización.

C) Oauth es una solución para autenticación y OpenID Connect es una solución para autorización.

D) Oauth es una solución para autorización y OpenID Connect es una solución para autenticación.

37. ¿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.

38. ¿Cuál es una ventaja de la criptografía simétrica?

A) Menor complejidad y mayor velocidad en comparación con la criptografía de clave pública.

B) Mayor dificultad para la implementación.

C) Necesidad de intercambio frecuente de claves públicas.

D) Complejidad en la gestión de claves.

39. ¿ Qué es el algoritmo conocido como Rijndael ?

A) Un algoritmo de criptografía simétrica

B) Un algoritmo de critografía de clave pública

C) Un algoritmo de hash

D) Un algoritmo de generación de números aleatorios.

40. ¿Cuál de los siguientes algoritmos es un ejemplo de criptografía simétrica?

A) AES (Advanced Encryption Standard)

B) RSA (Rivest-Shamir-Adleman)

C) DSA (Digital Signature Algorithm)

D) ECC (Elliptic Curve Cryptography)

41. ¿Qué caracteriza a la criptografía de clave pública?

A) Utiliza un par de claves, una pública y una privada, para cifrar y descifrar datos.

B) Usa una sola clave compartida para cifrar y descifrar datos.

C) Se basa en el cifrado de bloques fijos de datos.

D) La generación de una clave aleatoria no compatida.

42. ¿Cuál de los siguientes algoritmos es un ejemplo de criptografía de clave pública?

A) RSA (Rivest-Shamir-Adleman)

B) DES (Data Encryption Standard)

C) Blowfish

D) Twofish

43. ¿Qué ventaja tiene la criptografía de clave pública sobre la criptografía simétrica?

A) Facilita la distribución de claves sin necesidad de compartir una clave secreta.

B) Es más rápida en el procesamiento de grandes volúmenes de datos.

C) Requiere menos recursos computacionales para cifrar y descifrar datos.

D) Utiliza una sola clave para cifrar y descifrar datos.

44. ¿Qué función principal desempeñan las autoridades de certificación (CA) ?

A) Emiten y gestionan certificados digitales que autentican la identidad en comunicaciones en línea.

B) Desarrollan software para análisis de datos científicos.

C) Administran los derechos de autor para publicaciones científicas.

D) Proveen hardware para almacenamiento de datos.

45. Qué diferencia a la autorización de la autenticación?

A) La autorización otorga permisos para acceder a recursos específicos, mientras que la autenticación verifica identidad.

B) La autorización y autenticación son procesos idénticos.

C) La autorización es el proceso de cifrar datos, mientras que la autenticación verifica la velocidad de transferencia.

D) La autorización verifica la identidad, mientras que la autenticación otorga permisos.

46. ¿Qué es una vulnerabilidad en el contexto de seguridad informática?

A) Una debilidad en un sistema que puede ser explotada por una amenaza.

B) Un tipo de ataque que cifra datos.

C) Un método para aumentar el rendimiento del sistema.

D) Un software antivirus que protege contra amenazas.

47. Indique la respuesta correcta de acuerdo con lo establecido en el artículo 9 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

A) El solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología.

B) El solo consentimiento del afectado bastará para levantar la prohibición del tratamiento de datos relativos a sus creencias u origen racial o étnico.

C) El consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos personales relativos a condenas e infracciones penales o administrativas.

D) El consentimiento del afectado bastará para levantar la prohibición del tratamiento de datos cuya finalidad sea identificar su religión u orientación sexual.

48. Según el ENI, la publicación de servicios a través de la Red de comunicaciones de las AAPP (Red SARA) se encuentra contemplada dentro de la dimensión de la interoperabilidad:

A) Técnica.

B) Semántica.

C) Comunicativa.

D) Organizativa.

49. De acuerdo con el Esquema Nacional de Seguridad, ¿cada cuánto tiempo es necesario realizar una auditoría ordinaria en los sistemas de información de la Administración Autonómica?

A) Todos los años.

B) Al menos cada 2 años.

C) Al menos cada 5 años.

D) Solo es necesario realizar auditorías cuando se produzcan modificaciones sustanciales en los sistemas de información.

50. ¿Cuál de los siguientes no se incluye en la Estructura Orgánica definida en la Estrategia de Ciberseguridad Nacional?

A) El Consejo de Seguridad Nacional.

B) El Consejo Nacional de Ciberseguridad.

C) El Foro Nacional de Ciberseguridad.

D) El Consejo Ejecutivo de Ciberseguridad.

51. ¿Qué Guía CCN-STIC de seguridad versa acerca de la Gestión y uso de dispositivos móviles?

A) CCN-STIC 820.

B) CCN-STIC 822.

C) CCN-STIC 823.

D) CCN-STIC 827.

52. ¿Cuál es una medida de seguridad recomendada para redes inalámbricas?

A) Usar cifrado WPA3 para proteger la transmisión de datos.

B) Dejar la red abierta para facilitar el acceso a los usuarios.

C) Desactivar la autenticación en el punto de acceso.

D) Compartir la clave de red públicamente.

53. ¿Qué acción ayuda a proteger una red Wi-Fi contra ataques?

A) Cambiar el nombre de la red (SSID) y las contraseñas regularmente.

B) Usar el nombre de red predeterminado.

C) Permitir el acceso de cualquier dispositivo sin autenticación.

D) Desactivar el cifrado de la red Wi-Fi.

54. ¿Qué es el cifrado WPA2 en redes inalámbricas?

A) Un estándar de seguridad que cifra los datos transmitidos para proteger la red.

B) Un protocolo para compartir archivos en la red local.

C) Un método para aumentar la velocidad de la conexión inalámbricd.

D) Un sistema para crear redes virtuales privadas.

55. ¿Cuál es una medida de seguridad recomendada para aplicaciones en la nube?

A) Implementar controles de acceso basados en roles y cifrar datos en tránsito y reposo.

B) Permitir el acceso a todos los datos sin restricciones.

C) Usar contraseñas predeterminadas para todas las cuentas.

D) Desactivar las funciones de seguridad integradas.

56. ¿Qué es el cifrado de datos en reposo en la nube?

A) Proteger datos almacenados en servidores de la nube mediante cifrado.

B) Cifrar datos únicamente durante la transmisión.

C) Desactivar el cifrado para mejorar el rendimiento.

D) Utilizar contraseñas simples para acceder a datos almacenados.

57. ¿Cuál es una práctica para garantizar la seguridad en aplicaciones en la nube?

A) Realizar auditorías de seguridad y revisar los permisos de acceso periódicamente.

B) Compartir todas las credenciales de acceso con usuarios no autorizados.

C) Usar aplicaciones sin verificar su origen o seguridaD)

D) Ignorar las actualizaciones de seguridad recomendadas por el proveedor de la nube.

58. ¿Qué es la acreditación de sistemas?

A) El proceso de evaluar y certificar que un sistema cumple con los requisitos de seguridad establecidos.

B) La actualización de software para mejorar su funcionalidad.

C) La creación de nuevas aplicaciones para el sistemsa.

D) La instalación de hardware adicional en el sistema.

59. ¿Qué debe incluir un plan de contingencia?

A) Estrategias para recuperar la operación normal tras un incidente o desastre.

B) Un calendario de actividades de mantenimiento regular.

C) Un análisis del mercado para nuevos productos.

D) Un plan de capacitación para el personal de ventas.

60. ¿Qué es la recuperación tras un ataque informático?

A) La creación de un nuevo software para prevenir futuros ataques.

B) El proceso de restaurar los sistemas y datos a su estado normal tras un ataque.

C) La mejora de la interfaz de usuario de los sistemas afectados.

D) La optimización del rendimiento del hardware del servidor.

61. ¿Qué es la esteganografía?

A) Es equivalente al cifrado, especialmente en imágenes digitales, audio, ficheros y video digital.

B) Es un tipo de troyano.

C) Actualmente no se utiliza para el envío de información.

D) Es el envío de un mensaje oculto, especialmente en imágenes digitales, audio, ficheros y video digital.

62. ¿Qué implica el análisis forense digital?

A) La recolección, preservación y análisis de datos para entender y documentar un incidente de seguridad.

B) La creación de un nuevo diseño para la interfaz gráfica de usuario.

C) La instalación de nuevas aplicaciones para mejorar el rendimiento del sistema.

D) La configuración de redes sociales para la empresa.

63. ¿Cuál es una técnica común utilizada en el análisis forense digital?

A) Modificación del diseño de la base de datos.

B) Actualización de la apariencia visual del software.

C) Análisis de archivos de registro y reconstrucción de eventos.

D) Reducción del tamaño de los archivos de datos.

64. ¿Cuál es una medida clave para asegurar el despliegue de servicios web?

A) Dejar la configuración de seguridad en los valores predeterminados.

B) Permitir el acceso a todos los usuarios sin autenticación.

C) Ignorar las actualizaciones de seguridad para el servidor web.

D) Implementar HTTPS para cifrar las comunicaciones entre el cliente y el servidor.

65. ¿Qué significa OWASP?

A) Online Web Application Security Program.

B) Open Web Application Security Project.

C) Open Web Application Security Protocol.

D) Organization for Web Application Security Practices.

66. ¿Qué práctica ayuda a proteger los servicios web contra ataques de inyección SQL?

A) Usar consultas preparadas y parametrizadas.

B) Permitir entradas de usuario sin validar.

C) Usar contraseñas predeterminadas para todas las bases de datos.

D) Ignorar las revisiones de seguridad del código.

67. ¿Cuál de las siguientes opciones es una función hash actualmente segura?

A) MD5

B) RSA

C) SHA-3

D) 3DES

68. ¿Cómo se diferencia principalmente el NAC de un firewall?

A) El NAC se centra en el filtrado de tráfico, mientras que el firewall gestiona el acceso físico.

B) El NAC controla el acceso a la red de dispositivos basándose en su seguridad y cumplimiento, mientras que el firewall filtra el tráfico de red.

C) El NAC proporciona análisis de rendimiento, mientras que el firewall detecta intrusiones.

D) El NAC y el firewall tienen la misma funcionalidad, solo que con diferentes interfaces.

69. Como todo criptosistema de clave pública, el protocolo del criptosistema RSA

A) Tiene dos partes: Cifrado de Mensajes, Descifrado de Mensajes.

B) Se basa en la dificultad que supone resolver el <Problema de la Factorización Externa>.

C) Tiene tres partes: Generación de claves, Cifrado de mensajes, Descifrado de mensajes.

D) Se basa en la dificultad que supone resolver el <Problema de Socrates- Arquimedes>.

70. Indique cuál de las siguientes afirmaciones es correcta:

A) En un sistema de cifrado de clave asimétrica la seguridad radica en la transmisión de la clave, mediante canal seguro, entre el emisor y el receptor del mensaje.

B) Las huellas digitales devueltas por una misma función hash tienen idéntica longitud.

C) Para ofrecer un nivel de seguridad equivalente, los sistemas de clave pública requieren menores longitudes de clave que los sistemas simétricos.

D) Se denomina criptograma al procedimiento empleado para cifrar un mensaje.

71. Señale la afirmación CORRECTA respecto a los sistemas IDS (Intrusion Detection System) e IPS (Intrusion Prevention System):

A) Un IDS es una aplicación usada para detectar accesos no autorizados a un ordenador o a una red.

B) Un IPS cuenta con una actuación reactiva, ya que no trata de mitigar una intrusión.

C) Un IDS es un software que se utiliza para proteger a los sistemas de ataques e intrusiones. Su actuación es preventiva.

D) Un IDS no es vulnerable a los ataques DDoS.

72. El estándar de sintaxis de intercambio de información personal es:

A) PKCS#7

B) PKCS#9

C) PKCS#12

D) PKCS#14

73. ¿Cual es la función principal del conjunto de herramientas 'PILAR' desarrollado por el CCN-CERT?

A) Gestión de Ciberincidentes en las entidades del ámbito de aplicación del Esquema Nacional de Seguridad.

B) Almacenamiento virtual de información (archivos, muestras, aplicaciones, etc.).

C) Análisis y gestión de riesgos de un sistema de información.

D) Auditoría de cumplimiento con el Esquema Nacional de Interoperabilidad.

74. En criptografía simétrica, ¿cómo afecta el tamaño de la clave a la seguridad del criptosistema?

A) Claves más cortas son recomendables para asegurar la compatibilidad con sistemas más antiguos.

B) El tamaño de la clave no tiene impacto en la seguridad.

C) Claves de mayor tamaño aumentan la seguridad al dificultar los ataques por fuerza bruta.

D) Las claves de mayor tamaño disminuyen la seguridad porque son más fáciles de interceptar.

75. Cuando un usuario recibe un virus hoax o bulo informático a su cuenta de correo electrónico corporativo lo mejor es:

A) Reenviar el correo a toda su lista de contactos para ponerlos en preaviso.

B) Instalar un nuevo antivirus.

C) Ignorar los avisos y recomendaciones que se indican en el mismo y eliminar el correo electrónico.

D) Hacer clic en los enlaces del mensaje para obtener más información.

76. ¿Cuál es la función principal de un firewall de estado?

A) Verificar la integridad física del hardware de red.

B) Filtrar el tráfico de red basado en el estado de las conexiones y no solo en las reglas estáticas.

C) Monitorizar el uso de ancho de banda en tiempo real.

D) Proveer acceso remoto a través de VPN.

77. ¿Cuál de las siguientes tecnologías no garantiza la seguridad de una red?

A) Firewall

B) IDS/IPS

C) VPN

D) VLAN

78. La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, establece que el tratamiento de los datos personales de un menor de edad:

A) Únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años.

B) Únicamente podrá fundarse en su consentimiento cuando sea mayor de dieciocho años.

C) Únicamente podrá fundarse en su consentimiento cuando supere un test de madurez.

D) Nunca podrá fundarse en su consentimiento.

79. ¿Qué tipo de ataques es particularmente efectivo en mitigar un WAF?

A) Ataques de denegación de servicio (DoS) a nivel de red.

B) Ataques de phishing en correos electrónicos.

C) Ataques de inyección SQL y Cross-Site Scripting (XSS).

D) Amenazas internas de malware en el servidor.

80. Según la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, el Responsable de Seguridad y Enlace:

A) Es designado por el Ministerio del Interior y los operadores críticos deben facilitar a este el acceso a sus infraestructuras.

B) Es designado por los operadores críticos y debe contar con la habilitación del Director de Seguridad.

C) Es una figura independiente tanto de los operadores críticos como del Ministerio de Interior y su designación se lleva a cabo a través de selección competitiva.

D) Es personal al servicio de la Administración General del Estado, salvo en los casos de País Vasco y Navarra donde ser un funcionario de la administración autonómica de esas comunidades, si bien en todo caso deberá contar con la habilitación expresa del Director de Seguridad.