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 ESPECIALIZADOS DE LOS ORGANISMOS PÚBLICOS DE INVESTIGACIÓN, CONVOCADO POR RESOLUCION DE 22 DE MAYO DE 2024 (BOE Nº 131 DE 30 DE MAYO)

Cuestionario del primer ejercicio

Área global 6. 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.
- Cumplimente 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 ejercicio, el personal del aula le indicará los pasos a seguir.
- El **CUESTIONARIO** se podrá utilizar como borrador y se podrá llevar por el opositor al finalizar el tiempo marcado para el ejercicio.

1- Señale la afirmación CORRECTA:

A. La Ciencia de Datos, a pesar del término, no tiene nada que ver con el Big Data.
B. Un analista de datos debe tener conocimientos en estadística.
C. Las actuales aplicaciones de la Inteligencia Artificial generativa han convertido la Ciencia de Datos en un campo obsoleto.
D. La Ciencia de Datos es un campo académico muy reciente que se originó en la segunda década de este siglo con el desarrollo del aprendizaje automático profundo.

2- ¿Cuál de las siguientes afirmaciones sobre el protocolo RADIUS es INCORRECTA?

A. Fue desarrollado originalmente por Livingston Enterprises para la serie PortMaster de sus Servidores de Acceso a la Red (NAS)
B. Utiliza MD5 como algoritmo criptográfico de hashing, lo que lo hace vulnerable a ataques de colisión.
C. Utiliza TCP como protocolo de transporte para las comunicaciones entre cliente y servidor.
D. Utiliza UDP como protocolo de transporte para las comunicaciones entre cliente y servidor.

3- ¿Cuál de las siguientes NO es una metodología ágil?

A. WATERFALL.
B. Extreme Programming (XP).
C. KANBAN.
D. SCRUM.

4- ¿Qué es un sistema de tiempo real?

A. Un sistema operativo multitarea.
B. Un sistema que debe responder a eventos o datos de entrada dentro de un plazo específico.
C. Un sistema de base de datos distribuido.
D. Un sistema especialmente rápido.

5- ¿Qué es un Keylogger?

A. Un software que cifra archivos para proteger de accesos no autorizados.
B. Una herramienta que bloquea el acceso a sistemas cuando se detectan intentos de entrada no autorizados.
C. Un gestor de contraseñas.
D. Una herramienta que registra las pulsaciones de teclas en dispositivos y que puede utilizarse para robar información confidencial.

6- ¿Qué empresa es propietaria actualmente de la base de datos Web of Science?

A. Elsevier.
B. Penguin Books.
C. Clarivate.
D. Google.

7- Marque la respuesta INCORRECTA:

A. Las unidades de proceso gráfico (GPU) han desplazado a las CPU como procesadores más eficientes para el aprendizaje profundo.
B. La gran ventaja de las GPU es el reducido consumo energético requerido para su funcionamiento.
C. La estructura de las GPUs permite realizar múltiples tareas del proceso en paralelo.
D. Las GPUs también se utilizan en el entrenamiento de modelos de lenguaje de gran tamaño (Large Language Models, LLMs).

8- ¿Qué es una VDI (Infraestructura de Escritorio Virtual)?

A. Una conexión de red privada entre dispositivos a través de Internet.
B. Una solución para realizar copias de seguridad de datos en la nube.
C. Una tecnología que proporciona un entorno de escritorio virtualizado que se ejecuta en un servidor remoto, accesible a través de Internet.
D. Un entorno de escritorio virtualizado que se ejecuta en el dispositivo local del usuario.

9- ¿Qué es Digital.CSIC?

A. Una plataforma de cursos online ofrecida por el CSIC.
B. Un servicio de almacenamiento en la nube para investigadores del CSIC.
C. Un repositorio que ofrece acceso a la producción científica del CSIC mediante suscripción.
D. Un repositorio institucional que ofrece acceso abierto a la producción científica del CSIC.

10- ¿Cuál de los siguientes es un ejemplo de aplicación de un sistema de tiempo real?

A. Procesamiento de textos.
B. Sistema de control de tráfico aéreo.
C. Navegación en internet.
D. Reproducción de música.

11- ¿Cuál de las siguientes afirmaciones es CORRECTA respecto al proceso de Autenticación en un sistema AAA?

A. Se asignan permisos a los usuarios para acceder a recursos específicos.
B. Se registran las operaciones de los usuarios en el sistema.
C. Se confirma la identidad de los usuarios antes de permitir el acceso al sistema.
D. Se verifica que los datos transferidos en el sistema estén cifrados.

12- ¿Cuáles de las siguientes afirmaciones es CORRECTA?

A. El uso de VPN (Red Privada Virtual) proporciona una conexión segura, pero no impide el rastreo de cookies en la navegación, ni previene la descarga o ejecución de software malicioso.
B. Utilizar la misma contraseña para varias cuentas se considera una buena práctica de seguridad.
C. Desactivar las actualizaciones automáticas en navegadores web mejora la seguridad.
D. La navegación en modo incógnito evita el rastreo de la actividad por parte de terceros en línea y protege frente al malware.

13- ¿Qué es GitHub?

A. Un software de código abierto de control de versiones.
B. Una plataforma donde se puede almacenar y compartir código.
C. Un repositorio de software licenciado bajo suscripción.
D. Un servicio de almacenamiento en la nube exclusivo para personal del CSIC.

14- Señale la aseveración INCORRECTA sobre las aplicaciones de la Ciencia de Datos en investigación:

A. Además de su creciente importancia en sectores como la educación, la salud, el e-comercio, o el financiero, la Ciencia de datos también encuentra aplicación en la investigación científica, por ejemplo, en la astroinformática o en la bioinformática.
B. Algunos de los usos destacados de la Ciencia de Datos en biología son en secuencia del ADN y en clasificación de proteínas.
C. La astroinformática, y a su través, la Ciencia de Datos, no tiene aplicación posible en la moderna cosmología.
D. La gran cantidad de datos suministrados por radiotelescopios, el telescopio Hubble, o el observatorio de rayos X Chandra convierten a la Ciencia de Datos en una herramienta imprescindible para la astronomía moderna.

15- ¿Qué es el smishing?

A. Un tipo de fraude basado en la ingeniería social y en la suplantación de identidad que se realiza a través de llamadas telefónicas.
B. Noticias falsas que circulan principalmente por Internet a través de redes sociales o apps de mensajería como WhatsApp.
C. Un tipo de ciberataque basado en el envío de mensajes de texto (SMS).
D. Un método de protección de contraseñas mediante autenticación de dos factores.

16- ¿Cuál de estos conceptos no está asociado a SCRUM?

A. SCRUM Master.
B. Product Backlog.
C. Daily Meeting.
D. Diagrama de Gantt.

17- ¿Qué es un actuador en el contexto de la robótica?

A. Un dispositivo que convierte energía en movimiento.
B. Un sensor de temperatura.
C. Un software de control.
D. Un tipo de batería.

18- ¿Qué es IEEE Xplore?

A. Una base de datos de investigación académica que proporciona artículos y trabajos sobre Ciencias de la Computación, Ingeniería Eléctrica y Electrónica.
B. Una base de datos de investigación académica que proporciona artículos y trabajos sobre Astronomía y Astrofísica.
C. Un protocolo de metadatos.
D. Un repositorio digital de artículos académicos desarrollado en el CSIC.

19- ¿Cuál de las siguientes afirmaciones sobre el protocolo TACACS+ es CORRECTA?

A. Cifra todo el contenido de la comunicación entre el cliente y el servidor.
B. Utiliza UDP para la comunicación entre cliente y servidor.
C. Se considera una evolución del protocolo RADIUS.
D. Utiliza el puerto TCP 1813 para las comunicaciones.

20- ¿Cuál es uno de los principios fundamentales de la metodología KANBAN?

A. Roles claramente definidos para cada miembro del equipo.
B. Trabajo dividido en sprints.
C. Priorización de historias de usuario.
D. Limitar el trabajo en proceso (WIP).

21- ¿Cuál de los siguientes repositorios ofrece TODO su contenido en acceso abierto?

A. JSTOR.
B. ScienceDirect.
C. PubMed Central.
D. Wiley Online Library.

22- Señale la respuesta CORRECTA sobre las cámaras de tiempo de vuelo:

A. Las cámaras de tiempo de vuelo no se pueden utilizar en aplicaciones de robótica.
B. Las cámaras de tiempo de vuelo miden el tiempo que un UAV (dron) está en el aire.
C. La base del funcionamiento de las cámaras de tiempo de vuelo es la medida de distancias recorridas por un haz de luz infrarroja.
D. Las cámaras de tiempo de vuelo se basan en medir el cambio de fase de una señal de ultrasonidos.

23- ¿Cuál de las siguientes herramientas de software proporciona un espacio de trabajo digital unificado, que permite a los usuarios acceder a sus aplicaciones y escritorios virtuales desde cualquier dispositivo y ubicación?

A. Nagios.
B. Zabbix.
C. EndNote.
D. Citrix Workspace.

24- ¿Cuál es una de las características de SCOPUS?

A. Proporciona acceso a citas, resúmenes y métricas de impacto de artículos en revistas académicas mediante suscripción.
B. Proporciona guías de publicación de revistas electrónicas.
C. Es una base de datos temática sobre ciencias de la vida.
D. Proporciona acceso abierto a todo su contenido.

25- Marque la respuesta CORRECTA sobre el sesgo en el aprendizaje automático:

A. El uso de una fuente de datos tan extensa como internet garantiza la ausencia de sesgo en los datos extraídos.
B. Si los datos utilizados en el aprendizaje son imágenes, es imposible que se produzca un aprendizaje sesgado.
C. El proceso de anotación de imágenes es crítico y se ha de prestar especial atención durante el mismo para evitar o reducir el sesgo en el aprendizaje basado en imágenes.
D. El sesgo que puede aparecer durante el aprendizaje automático se debe más a los algoritmos de aprendizaje que a los datos suministrados para el aprendizaje.

26- ¿Qué es la integración de instrumentación en robótica?

A. El uso de instrumentos musicales en robots.
B. La incorporación de sensores y actuadores en sistemas robóticos.
C. La creación de software para robots.
D. El diseño de hardware para robots.

27- ¿Cuál de los siguientes es un ejemplo de software de código abierto?

A. Microsoft Office.
B. Adobe Photoshop.
C. Linux.
D. AutoCad.

28- ¿Qué estándar IEEE define las especificaciones de seguridad para redes WiMAX?

A. IEEE 802.11.
B. IEEE 802.15.
C. IEEE 802.16.
D. IEEE 802.3.

29- La Cualificación del Delegado de Protección de Datos:

A. Es requisito disponer de titulación universitaria.
B. Es requisito disponer de titulación universitaria en derecho.
C. Es requisito disponer de titulación universitaria con conocimientos en derecho y la práctica en materia de protección de datos.
D. Ninguna de las anteriores es cierta.

30- ¿Se puede filtrar el tráfico, mediante un firewall de nivel 3, entre dos máquinas situadas en la misma LAN?

A. Si.
B. No.
C. Depende de la configuración del FW.
D. Depende de la configuración de la LAN.

31- ¿Cuál de los siguientes protocolos de comunicación envía la información cifrada?

A. HTTPS.
B. ICMP.
C. SNMP.
D. SMTP.

32- En una organización quieren otorgar a los usuarios permiso de acceso a un recurso en función de su rol ¿qué tipo de control de acceso deben aplicar?

A. Control de acceso MAC.
B. Control de acceso RBAC.
C. Control de acceso ABAC.
D. Control de acceso DAC.

33- Una organización quiere evitar ataques por fuerza bruta a sus servidores linux por ssh, ¿qué medida le recomendarías?

A. Impedir los accesos fuera del horario laboral.
B. Configurar una regla en iptables.
C. Utilizar fail2ban.
D. Segmentar la red.

34- ¿Cuál es la sanción por una falta grave según el RGPD?

A. Multa administrativa de hasta 10.000.000€ o, en el caso de empresas, de cuantía equivalente al 2% como máximo del volumen de negocio total anual, lo que resulte mayor en cuantía.
B. Multa administrativa de hasta 20.000.000€ o, en el caso de empresas, de cuantía equivalente al 4% como máximo del volumen de negocio total anual, lo que resulte mayor en cuantía.
C. Dependiendo de factores, como la reincidencia en la infracción podrá ser entre 40.001€ y 300.000€.
D. El RGPD no especifica cuantía para las sanciones.

35- ¿Qué técnica se utiliza para permitir que múltiples VLANs compartan una única conexión física entre switches?

A. Trunking.
B. Mirroring.
C. Spanning Tree.
D. Port Aggregation.

36- ¿Cuál de las siguientes NO es una técnica criptográfica?

A. XOR.
B. Crypto9.
C. ROT13.
D. Sistema Enigma.

37- En referencia a Bluetooth Secure Simple Pairing (SSP), ¿cuál es la función del método "Numeric Comparison" y cómo contribuye a la mitigación de ataques "man-in-the-middle"?

A. Proporciona una clave pública estática que los dispositivos comparten, eliminando la necesidad de una verificación manual del usuario.
B. Genera y muestra un código numérico en ambos dispositivos, que el usuario debe confirmar si coinciden, lo que dificulta la intercepción de la conexión por un atacante.
C. Utiliza un canal secundario de comunicación cifrada para autenticar la conexión sin intervención del usuario, lo que previene ataques pasivos.
D. Establece una clave secreta compartida entre los dispositivos mediante el intercambio de un código QR, asegurando la autenticidad de los dispositivos emparejados.

38- Quieres restringir el acceso a un servidor web seguro de tu institución en función del origen del cliente, ¿qué utilizarías?

A. Un antivirus.
B. Un IDS.
C. Un cortafuegos.
D. Un DNS.

39- ¿Cuál de los siguientes ataques afecta a WPA2 pero no a WPA3?

A. Ataque de fuerza bruta.
B. Ataque de intermediario (MITM).
C. Ataque KRACK.
D. Ataque de denegación de servicio (DoS)

40- Según la Política de Seguridad de las TIC (Política STIC) y la normativa derivada, ¿qué información clasificada es considerada de mayor importancia?

A. Confidencial.
B. Difusión limitada.
C. Secreto.
D. Reservado.

41- ¿Qué tipo de ataque puede ser mitigado mediante el uso de un firewall en una red LAN?

A. Ataques de fuerza bruta.
B. Ataques de denegación de servicio (DoS).
C. Ataques de phishing.
D. Ataques de ingeniería social.

42- ¿PGP e IKE son ejemplos de qué tipo de criptografía?

A. Algoritmos de hash.
B. Criptografía homomórfica.
C. Clave privada.
D. Clave pública.

43- Señale cuál de las siguientes características de seguridad está incluida tanto en el estándar WPA2 como en el estándar WEP:

A. Intercambio dinámico de claves.
B. Autenticación 802.1x.
C. Preshared Keys (PSK).
D. Encriptación AES

44- ¿Qué medida puede ayudar a prevenir el ARP spoofing en una red LAN?

A. Usar direcciones IP estáticas.
B. Implementar autenticación de dos factores.
C. Utilizar un protocolo de seguridad como ARP Guard.
D. Desactivar el firewall.

45- ¿Qué es la criptografía?

A. Proceso de convertir un texto cifrado en texto sin formato.
B. Proceso de convertir texto ininteligible en texto sin formato.
C. Proceso de convertir texto sin formato en texto ininteligible y viceversa.
D. Proceso de convertir texto sin formato en texto cifrado.

46- ¿Cuál de las siguientes afirmaciones es la CORRECTA?

A. Para acceder a un recurso solo es necesario un proceso de autenticación.
B. Para acceder a un recurso solo es necesario un proceso de autorización.
C. Para acceder a un recurso es necesario un proceso de autenticación y uno de autorización.
D. Para acceder a un recurso es necesario un proceso de autenticación y uno de accounting.

47- ¿Cuál de las siguientes medidas NO es deseable por seguridad en los sistemas personales de los usuarios?

A. Configurar actualizaciones de software.
B. Trabajar desde una cuenta con mínimos privilegios.
C. Instalar un antimalware.
D. Activar la opción de recuerdo de contraseña en las aplicaciones.

48- Los proveedores de plataforma como servicio (SaaS) se encargan de la seguridad de:

A. la capa de infraestructura.
B. la capa de software.
C. La capa de plataforma.
D. La capa física.

49- Una autoridad de certificación (CA) realiza las siguientes funciones.

A. Se limita a verificar la identidad del solicitante.
B. Verifica la identidad del solicitante y emite certificados digitales.
C. Emite certificados digitales y mantiene la lista de revocación de certificados, así como demuestra la validez de los certificados.
D. Verifica la identidad del solicitante, emite certificados digitales y mantiene la lista de revocación de certificados, así como demuestra la validez de los certificados.

50- ¿Qué tipo de sistema es un IDS?

A. Sistema preventivo.
B. Sistema reactivo.
C. Sistema de encriptación.
D. Sistema de gestión de eventos.

51- El servicio de filtrado antispam proporcionado por RedIRIS se llama:

A. Lavadora.
B. Centrifugadora.
C. MicroClaudia.
D. EMMA.

52- Se quiere evitar el envío de correo electrónico sin encriptar desde dentro de la red local de una empresa hacia Internet, ¿que se debería hacer?

A. Cerrar el puerto 587 en el cortafuegos en salida.
B. Cerrar el puerto 25 en el cortafuegos en entrada.
C. Cerrar el puerto 465 en el cortafuegos.
D. Cerrar el puerto 25 en el cortafuegos en salida.

53- ¿Qué es IAM en Cloud?

A. Vigila que se cumplan las políticas de seguridad.
B. Gestiona identidades y accesos para controlar la autenticación y las credenciales de los usuarios.
C. Detecta amenazas mediante la recolección y análisis de incidentes de seguridad históricos y en tiempo real.
D. Identifica y subsana posibles riesgos en la configuración de la nube.

54- ¿Cuál de las siguientes NO es una medida de seguridad física de un servidor?

A. Ubicación segura.
B. Control de acceso.
C. Respaldo y recuperación.
D. Certificado digital.

55- Si accedemos a un sitio HTTPS y recibimos un aviso de que la autoridad de certificación que ha emitido el certificado de servidor no es reconocida por nosotros, y aun así aceptamos establecer comunicación con ese servidor, ¿la comunicación entre cliente y servidor será cifrada?

A. No, puesto que el certificado no es válido.
B. Sí, puesto que el certificado permite cifrar esa comunicación aunque haya sido emitido por una autoridad en la que no confiamos.
C. No, puesto que aunque hayamos aceptado ese certificado no podemos utilizarlo para hacer el cifrado de información.
D. Sí, porque al aceptar el cifrado se va a realizar con un certificado de cliente.

56- ¿Cuál de los siguientes NO es un protocolo de autenticación?

A. EAP-MD5.
B. DES.
C. Kerberos.
D. PAP.

57- Un emisor A mandó un mensaje cifrado a receptor B usando criptografía de clave pública. ¿Qué clave debe usar el receptor B para descifrar el mensaje?

A. Su clave pública.
B. La clave pública del emisor A.
C. Su clave privada.
D. La clave privada del emisor A.

58- Según la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos y garantía de derechos digitales, la edad mínima a efectos del consentimiento necesario para el tratamiento de datos en relación con la oferta directa de servicios de la sociedad de la información es de:

A. 18 años.
B. 16 años.
C. 13 años.
D. 14 años.

59- ¿Qué medida de seguridad recomendarías a los usuarios para evitar ser víctima de phishing?

A. No pulsar en los enlaces incluidos en correos electrónicos sin verificar antes a qué sitio web te dirigen.
B. Abrir todos los correos electrónicos que reciban sin importar su procedencia.
C. Contestar con información personal cuando te lo soliciten por correo electrónico.
D. Descargar todos los ficheros adjuntos recibidos por correo electrónico para su posterior uso.

60- ¿Para qué suele utilizarse una llave pública?

A. Es un algoritmo matemático que transforma una clave en una nueva serie de caracteres ilegibles.
B. Es un método criptográfico que asocia la identidad de una persona a un mensaje.
C. Es la clave que se utiliza para descifrar la información enviada.
D. Es la clave que se utiliza para cifrar la información enviada.

61- ¿Qué tipo de algoritmo no utiliza ninguna clave en la criptografía?

A. Funciones hash.
B. Algoritmos de clave pública.
C. Algoritmos de cifrado y descifrado.
D. Algoritmos de clave simétrica.

62- ¿Qué tipo de software utilizarías para ver el tráfico de entrada a una red local proveniente de Internet?

A. TCPView.
B. Telnet.
C. Sniffer.
D. Rdp.

63- En los modos de cifrado de bloque:

A. En todos los modos de cifrado de bloque cada bloque se cifra separadamente de los demás sin dependencia de otros bloques.
B. En el modo ECB cada bloque cifrado depende del bloque cifrado anteriormente.
C. En el modo CBC tanto el cifrado como el descifrado dependen del bloque cifrado anteriormente.
D. En el modo CFB un error en un bit del criptograma afectará sólo a un bloque del texto en claro recuperado.

64- Al crear un certificado digital, ¿qué clave se utiliza para crear la firma digital del certificado?

A. La clave pública de la autoridad de certificación (CA).
B. La clave privada del sujeto.
C. La clave pública del sujeto.
D. La clave privada de la autoridad de certificación (CA).

65- ¿Qué protocolo de red subyacente utiliza SFTP para transferir archivos?

A. TCP.
B. UDP.
C. ICMP.
D. HTTP.

66- ¿Qué técnica utilizan los antivirus para identificar sitios web de phishing?

A. Análisis de comportamiento del usuario.
B. Comparación con una base de datos de URLs maliciosas
C. Monitoreo de la actividad de la red en tiempo real.
D. Análisis heurístico.

67- ¿Cuáles son los contenidos mínimos de la política de seguridad, de acuerdo con el Esquema Nacional de Seguridad?

A. Los objetivos o misión de la organización y el marco legal y regulatorio en el que se desarrollarán las actividades.
B. Los objetivos o misión de la organización, el marco legal y regulatorio en el que se desarrollarán las actividades y los roles o funciones de seguridad.
C. Los objetivos o misión de la organización, el marco legal y regulatorio en el que se desarrollarán las actividades, los roles o funciones de seguridad, la estructura del comité o comités para la gestión y coordinación de la seguridad y las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.
D. Los objetivos o misión de la organización, el marco legal y regulatorio en el que se desarrollarán las actividades, los roles o funciones de seguridad y la estructura del comité o comités para la gestión y coordinación de la seguridad.

68- ¿Cuál de los siguientes NO se considera un tipo de seguridad en función de la naturaleza de los activos según la Política de Seguridad de las TIC (CCN-STIC-001)?

A. Seguridad de las actividades.
B. Seguridad de las transacciones.
C. Seguridad de la información.
D. Seguridad de las personas.

69- ¿Qué se entiende por IP Spoofing?

A. Es un ataque que se basa en la ejecución de código "Script" arbitrario en un navegador.
B. Es un ataque que pretende provocar un direccionamiento erróneo en los equipos afectados, mediante la traducción errónea de los nombres de dominio a direcciones IP.
C. Es un ataque que consiste en modificar la cabecera de los paquetes enviados a un determinado sistema informático para simular que proceden de un equipo distinto al que verdaderamente los originó.
D. Es un ataque que se compone de un conjunto de actuaciones que persiguen colapsar determinados equipos o redes informáticas, para impedir que puedan ofrecer sus servicios a sus clientes y usuarios.

70- ¿Qué se entiende por autenticación?

A. Proceso para verificar la identidad de alguien o algo.
B. Procedimiento que utilizan las empresas de software para verificar el uso legal de sus productos.
C. Método que se usa para comprobar que la información de una organización es auténtica y no ha sido modificada.
D. Procedimiento empleado para verificar que un mensaje de correo electrónico no fue modificado durante su envío.

71- Los cifrados de bloque pueden utilizarse en una variedad de modos de operación. ¿Cuál de los siguientes no es uno de ellos?

A. ECB.
B. OFB.
C. CFB.
D. CTE.

72- Un grupo de investigadores quiere acceder desde casa a los equipos ubicados en su centro de trabajo de la forma más segura posible, ¿qué solución le darías?

A. Conectarse mediante VPN a la red del centro usando 2FA.
B. Utilizar soluciones tipo TeamViewer o AnyDesk.
C. Abrir los puertos necesarios en el cortafuegos del centro hacia sus equipos.
D. Crear una VLAN separada del resto y permitirles el acceso desde sus domicilios.

73- Diferencia entre un virus y un “Caballo de Troya”:

A. El virus suele utilizar canales encubiertos.
B. El virus presenta un mecanismo de replicación.
C. El “Caballo de Troya” advierte de su presencia.
D. El “Caballo de Troya” no esconde funciones potencialmente maliciosas.

74- ¿Qué tipo de ataques puede intentar un adversario en una red?

A. Ataques pasivos y activos.
B. Ataques pasivos y defensivos.
C. Ataques activos y defensivos.
D. Ataques defensivos y reactivos.

75- ¿Cuál de los siguientes aspectos NO es considerado como un objetivo de seguridad según la STIC?

A. Disponibilidad de la información.
B. Confidencialidad de la información.
C. Integridad de la información.
D. Neutralidad de la información.

76- ¿Qué tipo de criptografía utiliza una única clave compartida entre el remitente y el receptor?

A. Criptografía de clave privada.
B. Criptografía de clave simétrica.
C. Funciones hash.
D. Criptografía de clave pública.

77- ¿Qué se entiende por política STIC?

A. Conjunto de elementos estratégicos, directivas, procedimientos, códigos de conducta, normas organizativas y técnicas que tiene por objetivo la protección de los sistemas de información del Organismo.
B. Conjunto de normas que regulan la interacción entre el departamento TIC y el resto de departamentos de una organización.
C. Conjunto de guías de configuración de los sistemas operativos de los sistemas de información de la organización.
D. Conjunto de pasos a seguir ante un incidente de seguridad en una organización.

78- Según se indica en el artículo 33 del RGPD, en caso de violación de la seguridad de los datos personales que constituya un riesgo para los derechos y las libertades de las personas físicas, en qué plazo el responsable del tratamiento la notificará a la autoridad de control competente:

A. A más tardar 24 horas después de que haya tenido constancia de ella.
B. A más tardar 72 horas después de que haya tenido constancia de ella.
C. A más tardar 30 días después de que haya tenido constancia de ella.
D. No es necesario realizar ninguna notificación.

79- ¿Qué componente de SNMPv3 se encarga de definir los niveles de seguridad?

A. MIB.
B. VACM.
C. USM.
D. PDU.

80- Los usuarios de tu institución se quejan de la dificultad de tener que utilizar múltiples contraseñas para acceder a los diferentes servicios y sistemas. Desde el punto de vista de la seguridad ¿qué les recomendarías a tus usuarios?

A. Utilizar la misma contraseña en todos los sistemas.
B. Usar un gestor de contraseñas.
C. Dejar las contraseñas en blanco.
D. Escribir las contraseñas en un documento en la nube.