CONVOCATORIA 08/23

Primera prueba: ejercicio escrito – Cuestionario tipo test

1. **El objetivo de la CNMV es:**
   a) Velar por la transparencia de los mercados de valores europeos y la correcta formación de precios, así como la protección de los inversores profesionales y sujetos regulados.
   b) Velar por la transparencia de los mercados de valores españoles y la correcta formación de precios, así como la protección de los inversores profesionales y sujetos regulados.
   c) Velar por la transparencia de los mercados de valores y materias primas europeos y la correcta formación de precios, así como la protección de los inversores profesionales y demás sujetos regulados.
   d) Velar por la transparencia de los mercados de valores españoles y la correcta formación de precios, así como la protección de los inversores.

2. **¿Cuál de las siguientes Direcciones Generales NO forma parte de la CNMV?**
   a) Dirección General de Servicio Jurídico.
   b) Dirección General de Política Monetaria.
   c) Dirección General de Mercados.
   d) Dirección General de Entidades.

3. **El Reglamento Europeo de Protección de Datos (GDPR) aplica sobre los siguientes sujetos:**
   a) Personas físicas y jurídicas.
   b) Organizaciones y sector público.
   c) Personas físicas.
   d) Personas jurídicas.

4. **Una organización maneja un alto volumen de información sensible. Se requiere que se establezcan medidas para reducir el riesgo de exfiltración de datos por un usuario. ¿Cuál es la medida que MÁS beneficiaria en la reducción del riesgo?**
   a) Deshabilitar los puertos USB.
   b) Habilitar el firewall a nivel de puesto de usuario.
   c) Deshabilitar la red Wifi.
   d) Parchear los sistemas.

5. **¿En cuál de los siguientes casos se requiere que una entidad haga un informe de evaluación de impacto, según el Reglamento General de Protección de Datos?**
   a) En todos los casos donde se traten datos personales.
   b) Cuando ha ocurrido un incidente y haya indicios de haberse filtrado los datos de personas físicas.
   c) En los casos en que los que sea probable que los tratamientos conlleven un alto riesgo para los derechos y libertades de las personas físicas.
   d) Cuando se realiza tratamiento de datos altamente confidenciales de la entidad.

6. **¿Cuál de las siguientes opciones describe correctamente el ámbito de aplicación de la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)?**
   a) Solo aplica a datos personales de menores de 16 años.
   b) Se aplica únicamente a datos almacenados en servidores dentro de la Unión Europea.
   c) Es aplicable a todo tratamiento de datos personales, independientemente del sector o actividad.
   d) Solo se aplica a datos personales recopilados en entornos laborales.

7. **¿Qué tipo de medida de gestión del riesgo sería un ciberseguro?**
   a) Una aceptación del riesgo.
   b) Una mitigación del riesgo.
   c) Una transferencia del riesgo.
   d) Una anulación del riesgo.

8. **¿Qué tipo de control de seguridad se utiliza al desplegar un banner de aviso al iniciar sesión en un sistema?**
   a) Preventivo.
   b) Disuasorio.
   c) Correctivo.
   d) De detección.

9. **Eres parte del equipo de gestión de riesgos dentro de tu organización y estás inmerso en un proceso de evaluación. Estás en el proceso de cálculo del *Single Loss Expectancy* (SLE) para un ataque de denegación de servicio sobre un servidor web. ¿Cuál es la fórmula que utilizarías?**
   a) AV * EF
   b) EF * ARO
   c) ALE * ARO
   d) AV * ARO

(AV: asset value, EF: exposure factor, ARO: annual rate of occurrence, ALE: annualized loss expectancy)

10. **¿Cuál es el primer paso en la gestión del riesgo relacionado con las TIC?**
    a) Implementar controles de seguridad.
    b) Identificar los activos de información.
    c) Realizar evaluaciones de riesgos.
    d) Monitorizar y revisar continuamente los sistemas.

11. **¿Qué se representa normalmente en un mapa de riesgos en ciberseguridad?**
    a) Una matriz (o mapa de calor) que representa los riesgos identificados en función de su probabilidad e impacto.
    b) Un plano de la empresa que representa las ubicaciones afectadas en caso de materializarse los riesgos.
    c) Un esquema de los activos TIC de la empresa y sus interconexiones para tomar decisiones para cada riesgo en caso de un ciberincidente.
    d) Un mapa geográfico que indica en tiempo real el origen y el destino de los principales ataques cibernéticos en Internet.

12. **¿Qué norma ISO establece las directrices para la gestión de riesgos de la seguridad de la información?**
    a) ISO 27001
    b) ISO 27002
    c) ISO 27005
    d) ISO 31000

13. **¿Cuál es la principal tarea en el análisis de riesgos en el contexto de la gestión del riesgo TIC?**
    a) Implementar medidas de seguridad.
    b) Comunicar los riesgos al órgano de dirección.
    c) Realizar auditorías de seguridad periódicas.
    d) Determinar la probabilidad e impacto de eventos adversos.

14. **Para la gestión del riesgo de TIC, ¿cuál de los siguientes factores NO sería determinante en el análisis de impacto en el negocio de cara a su análisis de continuidad?**
    a) La criticidad de las funciones de negocio.

b) Los ratios financieros de las áreas de negocio.
c) Las interdependencias entre los activos de información identificados y clasificados.
d) Los procesos de apoyo.

15. ¿Qué línea de actuación NO debería formar parte del plan de auditoría de riesgos de TIC de una organización?

a) Definición del alcance de los sistemas de TIC a auditar.
b) Auditorías focalizadas en sistemas de TIC.
c) Externalización de la auditoría.
d) Recurrir a personal del área de sistemas de información en caso de escasez de recursos.

16. ¿Qué es la matriz RACI utilizada para la gestión del riesgo?

a) Es la matriz que relaciona el riesgo, los activos, el control y la información.
b) Es la matriz de asignación de responsabilidades en la gestión de proyectos.
c) Es la matriz que asigna los riesgos y su impacto.
d) Ninguna de las anteriores.

17. Un atacante malicioso llama al servicio de help desk de una organización y se hace pasar por el director del departamento de operaciones. El atacante, afirma que ha olvidado la contraseña y necesita que se la restauren rápidamente ya que necesita acudir a una reunión, ¿Qué tipo de ataque describiría MEJOR este tipo de llamada telefónica?

a) Vishing.
b) Tailgating.
c) Watering Hole.
d) On-path.

18. ¿Cuál es el tipo de ataque caracterizado por la inyección de cadenas maliciosas que interactúan con la base de datos aprovechando una ausencia de validación de entrada en una aplicación?

a) Ataque de replay.
b) XML injection.
c) LDAP injection.
d) SQL injection.

19. Una organización destruye todos los documentos en una trituradora previamente a depositarlos en un contenedor. ¿Qué tipo de técnica de obtención de información está intentando prevenir la organización?

a) Shoulder surfing.
b) Pharming.
c) Dumpster diving.
d) Tailgating.

20. Observa la siguiente salida de una terminal de comandos. ¿Qué tipo de ataque está siendo ejecutado?

```
root@kali:`# attack.py 10.0.0.100 443
    [+] Attempting username: admin password: 8846F7EAEE8FB117AD06BDD830B7586C
    [-] Failed.
    [+] Attempting username: admin password: 92937945B518814341DE3F726500D4FF
    [-] Failed.
    [+] Attempting username: admin password: AFC44EE7351D61D00698796DA06B1EBF
    [-] Failed.
    [+] Attempting username: admin password: 209C6174DA490CAEB422F3FA5A7AE634
    [-] Success!  Username: admin and password: 209C6174DA490CAEB422F3FA5A7AE634 is valid!
```

a) Credential harvesting.
b) Denegación de servicio.
c) Pass the hash.
d) Phishing.

21. ¿Cuál es el tipo de malware que dispone de características únicas en cuanto a capacidad de autoreplicación sin necesidad de activación?

a) Gusano.
b) Virus.
c) Troyano.
d) Spyware.

22. ¿Cuál de los siguientes es un framework que recoge las técnicas, tácticas y procedimientos que seguiría un atacante en todo el ciclo de vida de una explotación?

a) COOP.
b) CURL.
c) MDM.
d) MITRE ATT&CK.

23. ¿En cuál de las siguientes acciones se está usando OSINT?

a) Descifrar una contraseña conociendo el hash de la misma.
b) Intentar acceder al correo web de un usuario de la misma organización probando las contraseñas más típicas.

c) Obtener información de un usuario en una red social para luego enviarle un enlace en un phishing.
d) Dejar varios dispositivos USB infectados con virus en un aparcamiento público.

24. ¿Cuál de los siguientes tipos de malware está diseñado para activarse tras una cantidad de tiempo definido, evento específico o fecha concreta?

a) Rootkit.
b) Troyano.
c) Adware.
d) Bomba lógica.

25. ¿Cuál de las siguientes definiciones se correspondería con una Amenaza Avanzada Persistente (APT)?

a) Un ataque en el que se configura un servidor con el mismo aspecto que el de una organización para que los empleados introduzcan sus credenciales al abrir un enlace.
b) Un ataque contra un sitio web en el que se modifica la apariencia visual de una o varias páginas web.
c) Una actividad maliciosa en la que un ciberatacante trata de obtener el control de un servidor de nombres de dominio de Internet.
d) Un ataque dirigido contra una organización, que trata de robar o filtrar información sin ser detectado.

26. ¿Qué estándar se emplea comúnmente para identificar las vulnerabilidades de seguridad conocidas?

a) CVE.
b) CVSS.
c) MITRE ATT&CK.
d) OWASP.

27. ¿Cuál de los siguientes mecanismos ayuda a preservar la integridad de los datos frente a un ataque de cifrado de ransomware?

a) Tener copias de seguridad fuera de línea.
b) Usar un almacenamiento RAID 5 en los servidores de datos.
c) Usar almacenamiento SAN con replicación síncrona de discos en otro centro de datos.
d) Usar una red de fibra con dobles caminos.

28. **¿Cuál de los siguientes elementos es un ejemplo de "*Host-Based*" firewall?**
    a) Un firewall configurado en el perímetro de una organización interactuando entre la red interna e Internet.
    b) Un firewall protegiendo una aplicación web sobre un servidor web.
    c) Dos firewalls creando una DMZ.
    d) Windows Firewall.

29. **Como profesional de la ciberseguridad, ¿Qué elemento incluirías en la infraestructura de una organización para atraer y analizar la actividad de un atacante?**
    a) IDS.
    b) Honeypot.
    c) IPS.
    d) Escáner de vulnerabilidades.

30. **¿Cuál de los siguientes términos es utilizado para describir la tecnología software o hardware que previene que los usuarios no envíen información delicada o crítica fuera de la red corporativa?**
    a) Firewall.
    b) Data Loss Prevention (DLP).
    c) Cifrado.
    d) Intrusion Prevention System (IPS).

31. **Una organización requiere que sus empleados realicen sus tareas diarias accediendo a Internet de forma habitual. ¿Qué tecnología deberían implementar para enmascarar las direcciones IP internas y permitir el acceso a Internet compartiendo una dirección IP pública?**
    a) DMZ.
    b) Router.
    c) NAT.
    d) DNS.

32. **Como administrador de seguridad, estás diseñando un sistema de accesos a una serie de servicios que requieren la identificación del usuario. Uno de los requisitos es que el usuario solo tenga que introducir sus credenciales una única vez con**

independencia del software y tecnología de autenticación desplegada. ¿Cuál es la solución que deberías implementar?

a) Contenedor de contraseñas.
b) Single Sign-On (SSO).
c) Remote Authentication Dial-In User Service (RADIUS).
d) Security Assertion Markup Language (SAML).

33. La organización dispone de un servidor web expuesto a Internet. Has descubierto que alguien está utilizando tu servidor como un relay de correo. ¿Cuál servicio y puerto deberías deshabilitar para detener este tipo de ataque?

a) HTTP, puerto 80.
b) SMTP, puerto 110.
c) HTTP, puerto 443.
d) SMTP, puerto 25.

34. ¿Cuál de los siguientes es un sitio alternativo de procesamiento de datos instantáneamente disponible en caso necesidad de recuperación de desastres?

a) Sitio recíproco.
b) Sitio frío.
c) Sitio templado.
d) Sitio caliente.

35. ¿Qué modelo de seguridad evita mejor que los atacantes se aprovechen de las debilidades del perímetro para acceder a los datos y aplicaciones confidenciales de la entidad?

a) NAC.
b) Zero Trust.
c) MDM.
d) MFA.

36. ¿Para qué se utilizan los registros de DNS: SPF, DMARC y DKIM?

a) Para consultar la configuración del proxy de salida a Internet de la organización.
b) Para configurar los dispositivos móviles mediante MDM.
c) Para evitar ataques de Man in de Middle.
d) Para prevenir la suplantación de dominio en el correo electrónico.

37. **¿Con qué tecnología separarías a nivel lógico el tráfico de dos redes (por ejemplo, la de usuarios de oficina y la de administración de sistemas) utilizando los mismos conmutadores (o switches) a nivel físico?**
    a) VLAN.
    b) SNMP.
    c) LACP.
    d) RMON.

38. **¿Qué dispositivo hardware se incluye por defecto en los nuevos equipos de sobremesa y portátiles para realizar tareas criptográficas?**
    a) Memoria DDR5.
    b) Un HSM.
    c) Un SSD.
    d) Un TPM.

39. **Alfredo está redactando un mensaje para Antonia y le gustaría firmar digitalmente previo envío, ¿Qué clave debería utilizar para crear la firma digital?**
    a) La clave privada de Alfredo.
    b) La clave pública de Alfredo.
    c) La clave privada de Antonia.
    d) La clave pública de Antonia.

40. **¿Qué método permite firmar y cifrar correos electrónicos entre dos usuarios mediante sus certificados individuales?**
    a) IMAPS
    b) S/MIME
    c) SMTPS
    d) STARTTLS

PREGUNTAS DE RESERVA:

41. **Se está revisando el tráfico de red de un servicio FTP y se observa que el usuario root ha estado intentando acceder con contraseñas como contraseña1, contraseña2,…., contraseñaN. ¿Qué tipo de ataque acaba de descubrir el usuario?**
    a) Un ataque de fuerza bruta.
    b) Un ataque de rainbow table.
    c) Un ataque pass the hash.
    d) Un ataque de spraying password.

42. Un sistema de ficheros realiza una copia de seguridad completa cada lunes a la 1 AM. Las copias de seguridad incrementales son realizadas cada martes, miércoles, jueves y viernes también a la 1 AM. El administrador del sistema necesita realizar una recuperación completa el jueves por la tarde. ¿Cuántas copias de seguridad son necesarias para completar la recuperación?

a) 1.
b) 2.
c) 3.
d) 4.