POF: PRUEBA OBJETIVA FINAL			
Denominación del curso	IFCT0109. Seguridad Informática	**Código curso:**	23-38/002065
Denominación del MF/ UF	MF0488_3 Gestión de incidentes de seguridad informática	**Fecha:**	27/09/2024
		Duración:	60 minutos
Nombre Docente Examinador	Benito Manuel González Rodríguez	**Firma Docente**	
Nombre y apellido del alumno/a **DNI**		**Firma Alumno**	
		Nota Obtenida	

INSTRUCCIONES:

- Lea detenidamente la prueba y conteste a los siguientes ítems.
- La prueba tiene una duración de 60 minutos.

PRUEBA OBJETIVA FINAL

Seguridad Informática.

MF0488_3 Gestión de incidentes de seguridad informática

Marca con una "x" en las casillas de "V" (verdadero) o "F" (falso) según sean las siguientes afirmaciones. Se recomienda en estos ítems que se contesten los que se sepan ya que los errores restan puntuación. El valor de cada pregunta correcta será de 1 punto.

1. Los sistemas habituales utilizados para la detección y contención de código malicioso son los IPS/IDS, Antivirus y Firewall V__ F__

2. Un incidente de seguridad es cualquier evento que puede afectar a la integridad, confidencialidad y disponibilidad de la información V__ F__

3. La CONTENCIÓN DE UN INCIDENTE es devolver los sistemas, dispositivos y equipos a su estado original antes de producirse el incidente. V__ F__

4. En el análisis forense informático, las EVIDENCIAS VOLÁTILES son las que se almacenan en el sistema de ficheros y no se pierden al apagar el equipo V__ F__

5. Dentro de los incidentes de seguridad informática, los ingresos y operaciones no autorizadas a los sistemas son incidentes de DENEGACIÓN DE SERVICIO V__ F__

6. **La colocación sistemas NIDPS delante del cortafuegos externo permite una monitorización de los ataques contra la infraestructura de una organización, principalmente los dirigidos contra el firewall de la red** V__ F__

7. **Se habla de POLÍTICA DE RESPUESTA ACTIVA cuando el sistema IDS/IPS detecta una intrusión, además de generar una alarma, modifica el entorno para evitar que la intrusión tenga éxito.** V__ F__

8. **Se habla de VERDADERO POSITIVO cuando el IDS/IPS detecta como ataque el tráfico de datos que en verdad es inofensivo** V__ F__

9. **Los ARCHIVOS DE REGISTRO O ARCHIVOS DE LOG son una fuente importante de seguridad y de solución de problemas** V__ F__

10. **Un CERT/CSIRT está formado por un grupo de expertos responsable del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información** V__ F__

A continuación, presentamos una serie de ítems de selección múltiple, para responder señala con una "X" la respuesta correcta. Recuerda que el error se penaliza. Si te equivocas, rodea con un círculo la "x" y vuelve a marcar con una "X". 1 punto.

11. **Los IDS que tienen como función principal la detección de comportamientos inusuales que sucedan en un host de una red son los IDS…**
    a) de detección de abusos o firmas
    b) basados en red (NIDS)
    c) basados en host (HIDS)
    d) de detección de anomalías

12. **Dentro de la Gestión de Incidentes, el momento en el que se aplican las medidas correctivas para restaurar el sistema a la situación inicial antes de producirse el incidente, es la fase de…**
    a) Respuesta al incidente
    b) Análisis del incidente
    c) Registro del incidente
    d) Prevención del incidente

13. **Para la ubicación de un sistema IDS/IPS, la zona de confianza, en la que cualquier tipo de acceso anómalo que haya en la red hay que considerarlo como acceso hostil, es la Zona…**
    a) Verde
    b) Amarilla
    c) Azul
    d) Roja

14. El orden en el que se realizan las fases de un Plan de Prevención de Incidentes es…

a) Preparación y prevención, erradicación y notificación
b) Preparación y prevención, detección y notificación, análisis preliminar, contención, erradicación y recuperación, investigación y actividades posteriores
c) Preparación y prevención, análisis preliminar, contención, erradicación y recuperación, investigación, detección y notificación y actividades posteriores
d) Preparación y prevención, investigación, análisis preliminar, erradicación y recuperación, contención, detección y notificación y actividades posteriores

15. Los IPS que tienen como funcionalidad principal bloquear direcciones IP que puedan ser causantes de algún tipo de ataque, son los IPS…

a) con acción de decepción
b) de bloqueo de IP
c) de filtrado de paquetes
d) de autodefinición de firmas

16. La capacidad del IDS/IPS para resistir a los ataques y a los fallos del sistema (cortes de electricidad, etc.), es …

a) La tolerancia a fallos
b) La completitud
c) La precisión
d) El tiempo de respuesta

17. Dentro de los códigos maliciosos, las aplicaciones diseñadas con el fin de registrar el comportamiento de un usuario en un ordenador de modo remoto se denominan…

a) Gusanos
b) Cookies
c) Keyloggers
d) troyanos

18. En el ANÁLISIS FORENSE INFORMÁTICO, la fase en la que se realiza un análisis exhaustivo para reconstruir el timeline del ataque y llegar a su inicio para detectar al atacante, es la fase de…

a) Confirmación de las pruebas realizadas y realización del informe
b) Estudio preliminar
c) Análisis e investigación de las evidencias
d) Adquisición de datos y recopilación de evidencias

19. Cuando el IDS/IPS detecta como ataque el tráfico de datos que en verdad es inofensivo, se habla de...

a) Ataque detectado correctamente
b) Falso positivo
c) Falso negativo
d) Verdadero positivo

20. **En el análisis forense informático, el criterio de admisibilidad de evidencias electrónicas de COMPLETITUD o SUFICIENCIA es…**

a) La evidencia debe estar completa, tiene que hacerse manteniendo su integridad

b) Las técnicas de recolección y tratamiento de la evidencia deben cumplir las normativas legales vigentes en el ordenamiento jurídico

c) La evidencia debe haber sido generada y registrada en la escena del crimen y debe mostrar que los medios utilizados no se han modificado

d) El sistema no fue vulnerado y funcionaba correctamente cuando se recibió, almacenó o generó la prueba

A continuación, presentamos una serie de ítems de completar. Para responder rellena la línea de puntos con la respuesta correcta. Puntuación: 1 punto.

21. La ……. es devolver los sistemas, dispositivos y equipos a su estado original antes de producirse el incidente.

22. los **…….** Son centros de respuesta a incidentes de seguridad en tecnologías de información formados por expertos encargados de diseñar medidas preventivas y reactivas ante incidentes de seguridad.

23. Cuando los intrusos en este caso falsifican la información del sistema atacando a su autenticidad, se habla de un ataque de **…….**

24. El objetivo principal del ……. es recoger las evidencias digitales presentes en cualquier tipo de incidencia y delito informático

25. Un …… es un sistema para detectar accesos no autorizados a un equipo o una red que ante cualquier actividad sospechosa emiten una alerta, pero no tratan de mitigar la intrusión.

A continuación, presentamos una serie de ítems de respuesta breve. Para responder rellena la línea de puntos con la respuesta correcta. Puntuación: 1 punto.

26. **Define y explica las diferencias entre IDS, IPS y SIEM:**

_____

_____

_____

_____

_____

27. **Indica las diferencias entre HIDS y NIDS:**

28. **Nombra y describe las fases de un Plan de Gestión de Incidentes:**

A continuación, presentamos una serie de ítems de respuesta de correspondencia. Deber relacionar las premisas a la derecha con las respuestas a la derecha. Para responder traza una flecha de cada premisa a su respuesta o respuestas, Si te equivocas, marca la flecha con una x. También puedes poner la correspondencia entre las letras y números. Por ejemplo: B2, C6… Puntuación: 2 puntos.

29. Relaciona los conceptos de la izquierda con los nombres de la derecha.

A. SISTEMAS DE DETECCIÓN Y ELIMACIÓN DE VIRUS

B. SISTEMAS DE DETECCIÓN Y CONTENCIÓN DE CÓDIGO MALICIOSO.

C. EQUIPOS DE RESPUESTA DE INCIDENTES DE SEGURIDAD INFORMÁTICA

1) NORTON 360 DELUXE

2) INCIBE-CERT

3) MCAFEE TOTAL PROTECTION

4) FIREWALL

5) CCN-CERT

6) IDS/IPS

Solución: _____

30. Ordene las fases del análisis forense informático.

1) FASE 1	A. ADQUISICIÓN DE DATOS Y RECOPILACIÓN DE EVIDENCIAS
2) FASE 2	B. CONFIRMACIÓN DE LAS PRUEBAS REALIZADAS Y REALIZACIÓN DEL INFORME
3) FASE 3	C. ANÁLISIS E INVESTIGACIÓN DE LAS EVIDENCIAS
4) FASE 4	D. ESTUDIO PRELIMINAR

Solución: _____

Fdo. _____

PLANTILLA DE CORRECCIÓN
IFCT0109. Seguridad Informática
MF0488_3 Gestión de incidentes de seguridad informática

Puntuación:

Ítems de verdadero/Falso
Puntuación=1 Punto
Fórmula P=A-E

Ítems de selección múltiple
Puntuación=1 Punto
Fórmula P=A-(E/3)

Ítems de texto incompleto
Puntuación=1 Punto
Fórmula P=A

Ítems de respuesta breve
Puntuación=1 Punto
Fórmula P=A

De correspondencia
Puntuación
2 puntos = 0 errores
1 punto =1 error
0 puntos > 1 errores