POF: PRUEBA OBJETIVA FINAL			
Denominación del curso	IFCT0109. Seguridad Informática	**Código curso:**	23-38/002065
Denominación del MF/ UF	MF0487_3 Auditoría de seguridad informática	**Fecha:**	03/09/2024
		Duración:	60 minutos
Nombre Docente Examinador	Benito Manuel González Rodríguez	**Firma Docente**	
Nombre y apellido del alumno/a	Jorge Escobar Viñuales	**Firma Alumno**	Jorge Escobar Viñuales
DNI	43835997K	**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.

MF0487_3 Auditoría 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. **El PRINCIPIO DE INTEGRIDAD MORAL indica que los auditores deberán desempeñar sus tareas con una actitud honesta, leal y diligente, evitando siempre participar en actividades que puedan perjudicar a terceras personas o al auditado** V__ F__

2. **El RGPD permite el consentimiento tácito del interesado o afectado del tratamiento** V__ F__

3. **El Proceso y metodología utilizados para estimar la magnitud de los riesgos a los que se expone una organización es el TRATAMIENTO DE LOS RIESGOS.** V__ F__

4. **Escribiendo PING LOCALHOST se verifica si los protocolos TCP/IP están instalados y si funcionan correctamente en el equipo.** V__ F__

5. **La garantía de la fuente de la que proceden los datos es la CONFIDENCIALIDAD** V__ F__

6. **Las aplicaciones que reenvían o bloquean las conexiones a unos servicios concretos se denominan PROXY** V__ F__

7. **Un CORTAFUEGOS puede permitir el acceso a la red interna del tráfico tanto autorizado como no autorizado** V__ F__

8. **Al finalizar la auditoría de protección de datos se realizará una exposición analítica y depurada de los principales hallazgos, observaciones y conclusiones recogidos en el INFORME FINAL** V__ F__

9. **La prueba de auditoría en la que se comprueba el historial de la información consiste en la revisión de LOGS o archivos de registro** V__ F__

10. **La auditoría de seguridad informática es la que analiza todos los procesos referentes a la seguridad informática, tanto física como lógica** 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. **De las siguientes definiciones, indique cuál se corresponde con una vulnerabilidad del tipo "error de búfer"**

a) Se produce cuando se intentan almacenar datos de forma incontrolada en su espacio.
b) Se origina cuando el programa no puede autenticar correctamente al usuario que intenta acceder a él.
c) Vulnerabilidad que se localiza en el nivel de base de datos del programa o aplicación y se produce cuando el filtrado de las variables utilizadas con código SQL no se realiza correctamente.
d) Vulnerabilidad que sucede cuando el programador realiza el diseño de la aplicación con fallos y errores

12. **Indique cuál de los siguientes conceptos no debe incluirse obligatoriamente en la planificación de la auditoría informática**

a) Áreas que serán auditadas
b) Fecha límite para la finalización de la auditoría
c) Empleados de la organización al completo
d) Composición del equipo de auditoría

13. **Los analizadores de protocolos o analizadores de red…**

a) analizan el tráfico de datos de una red solo en tiempo real.
b) buscan los puertos abiertos de una red.
c) facilitan información sobre características específicas de ciertos componentes hardware del equipo.
d) analizan el tráfico de datos de una red tanto en tiempo real como en momentos posteriores a la captura de datos.

14. **De las siguientes, ¿Cuál es la definición de ANÁLISIS DE LOS RIESGOS?**

a) Un fallo de seguridad en un programa o en un sistema de información
b) Conjunto de procesos realizados para modificar los riesgos de una organización.
c) Estimación de las probabilidades de que una amenaza se materialice sobre los activos de la organización causando efectos negativos o pérdidas.
d) Proceso y metodología utilizados para estimar la magnitud de los riesgos a los que se expone una organización.

15. **Dentro de las normas de Auditoría, la que indica que en el informe deben constar las normas y principios de auditoría utilizados en la auditoría y las excepciones de incumplimientos, es…**

a) La Consistencia
b) La Planificación
c) El Control interno
d) La Evidencia

16. **¿Cuál de las siguientes actividades no se corresponde con los conocimientos básicos del equipo de auditores informáticos?**

a) Sistemas operativos
b) Gestión de bases de datos
c) Desarrollo de proyectos financieros
d) Seguridad física y del entorno

17. **De las siguientes, ¿Cuál es la definición de INTEGRIDAD?**

a) La información debe estar disponible a los usuarios siempre que sea necesario.
b) La información debe ser correcta y completa.
c) La información debe estar disponible solo para los usuarios que estén correctamente autorizados.
d) La garantía de la fuente de la que proceden los datos.

18. **El derecho del interesado a obtener sin dilación indebida del responsable del tratamiento la rectificación de sus datos personales inexactos es el derecho de…**

a) Portabilidad de los datos
b) Rectificación
c) Limitación del tratamiento
d) Acceso

19. **De los siguientes, ¿cuáles son PRUEBAS de auditoría?**

a) No conformidades
b) Informe Final
c) Checklists
d) Amenazas

20. **Los hallazgos que se detectan cuando se encuentra algún incumplimiento de un requisito definido en la auditoría son...**

a) No conformidades
b) Observaciones
c) Oportunidades de mejora
d) Normativas técnicas

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 ……. informática consiste en una serie de técnicas y procedimientos realizados con el objetivo de evaluar y controlar un sistema de información.

22. La herramienta del sistema operativo …….. se utiliza para seguir la ruta de los paquetes en una red IP y el retardo que se produce en este tránsito.

23. El …… es la estimación de las probabilidades de que una amenaza se materialice sobre los activos de la organización, causando efectos negativos o pérdidas.

24. Un …… es el conjunto de recursos del sistema de información o relacionados con este que son necesarios para el correcto funcionamiento de la organización y para que se alcancen los objetivos definidos por esta

25. Una …… es una acción o conjunto de acciones que se realizan para minimizar o eliminar una amenaza sobre un activo de información.

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 para que se usa una matriz de riesgos:

27. Define Impacto residual, riesgo potencial y riesgo residual:

28. **Define controles disuasorios, preventivos, detectores y correctivos**

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 la función correspondiente de la derecha.

D. Envío de correos electrónicos con la identidad de otro usuario.

E. Modificación no autorizada de los datos de un archivo.

F. Incapacidad de acceder a un servicio determinado del sistema de información. por saturación de datos.

G. Envío por error de correos electrónicos con datos confidenciales de los clientes de la organización.

H. Obtención y utilización de los privilegios y permisos del administrador sin autorización.

1) DIVULGACIÓN

2) SUPLANTACIÓN

3) ELEVACIÓN DE PRIVILEGIOS

4) ALTERACIÓN

5) DENEGACIÓN DE SERVICIO

Solución: _____

1. Ordene las fases del proceso de análisis y gestión de riesgos.

1) A. IDENTIFICACIÓN DE LOS ACTIVOS.

2) B. DETERMINACIÓN DEL IMPACTO DE UNA AMENAZA.

3) C. ESTABLECIMIENTO DE SALVAGUARDAS (ATENUANTES).

4) D. REVISIÓN DEL IMPACTO Y DETERMINACIÓN DEL IMPACTO RESIDUAL.

5) E. <

6) F. VALORACIÓN DE LOS ACTIVOS.

7) G. DETERMINACIÓN DEL RIESGO.

8) H. REVISIÓN DEL RIESGO Y DETERMINACIÓN DEL RIESGO RESIDUAL.

Solución: _____

Fdo. _____

PLANTILLA DE CORRECCIÓN
IFCT0109. Seguridad Informática
MF0487_3 Auditoría 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