

[Página Principal](#)[Mis cursos](#)[Cursos Personales](#)[rubenvalentin.caravaca_SAD](#)[UT1](#)[UT1_Autoevaluación.Cuestionario Parte I](#)

Comenzado el	jueves, 10 de octubre de 2024, 19:44
Estado	Finalizado
Finalizado en	jueves, 10 de octubre de 2024, 20:18
Tiempo empleado	33 minutos 58 segundos
Puntos	59,00/64,00
Calificación	9,22 de 10,00 (92%)

Pregunta 1

Parcialmente correcta

Se puntúa 9,00 sobre 10,00

1. ¿Cuáles son las dos grandes categorías en las que se pueden dividir las amenazas a un sistema informático?

Amenazas internas y amenazas externas. ❌

2. ¿Qué tipo de amenaza incluye el sobrecalentamiento de los componentes del sistema?

Amenazas físicas. ✔

3. ¿Cuál de las siguientes es una amenaza lógica?

Software malicioso. ✔

4. ¿Qué efectos pueden tener las amenazas lógicas en una empresa?

Pérdida de clientes y deterioro de la reputación. ✔

5. ¿Qué es lo que nunca puede ser completamente seguro según la unidad de trabajo?

Un sistema informático. ✔

6. ¿Qué implica el "Internet de las Cosas" (IoT) según la unidad de trabajo?

Conexión a internet de dispositivos como automóviles y frigoríficos. ✔

7. ¿Cuál es el papel del administrador de sistemas mencionado en la unidad de trabajo?

Supervisar y proteger continuamente el sistema informático. ✔

8. ¿Qué es necesario para proteger un sistema informático de amenazas físicas y lógicas?

Medidas de protección diseñadas para enfrentar distintos tipos de amenazas. ✔

9. Según la unidad de trabajo, ¿cuál de estos ejemplos NO es mencionado como una amenaza física?

Violación de la privacidad de los datos. ✔

10. ¿Qué desafío enfrenta el administrador del sistema informático según la unidad de trabajo?

Debe estar inmerso en un ciclo continuo de supervisión y protección. ✔

Pregunta 2

Correcta

Se puntúa 14,00 sobre 14,00

¿Qué método utilizan las auditorías de seguridad para identificar vulnerabilidades?

Técnicas de pentesting. ✓

¿Cuál es el propósito de contratar hackers éticos en el contexto de una auditoría de seguridad?

Para simular ataques que podrían realizar hackers maliciosos. ✓

¿Qué validez pueden tener los análisis forenses de sistemas informáticos?

Como prueba en un proceso judicial. ✓

¿Qué se debe incluir en el contenido mínimo de un informe de auditoría de seguridad según la norma ISO 19011?

Objetivo, alcance, equipo auditor, fechas, lugares y criterios de la auditoría. ✓

¿Qué se utiliza para garantizar la integridad de las pruebas en un análisis forense?

Una rigurosa cadena de custodia. ✓

¿Qué información se suele recopilar en la fase de adquisición de datos durante un análisis forense?

Ficheros log del sistema, correos electrónicos, historial del navegador. ✓

¿Qué herramienta forense es conocida por su capacidad para analizar la memoria volátil?

Volatility. ✓

¿Para qué es utilizada principalmente la herramienta Magnet AXIOM?

Para recuperar y analizar evidencias de múltiples plataformas. ✓

¿Qué característica especial ofrece ProDiscover Forensic?

Adquisición de imágenes de discos y análisis de datos. ✓

¿Cuál es una función clave de los SAI más avanzados respecto a la gestión de la energía?

Segmentación de carga entre tomas críticas y no críticas. ✓

¿Qué permite hacer un sistema de monitoreo en red de los SAI?

Controlar todos los SAI del sistema de manera centralizada. ✓

¿Qué debe hacerse cuando el SAI entra en modo batería debido a un corte de suministro?

Actuar rápidamente para apagar los equipos antes de que la batería se agote. ✓

¿Cuál es una recomendación importante si un SAI debe ser trasladado?

Manipularlo con cuidado y asegurarse de que está apagado. ✓

¿Qué herramienta no está diseñada para realizar análisis forense?

Lynis.



Pregunta 3

Parcialmente correcta

Se puntúa 7,00 sobre 10,00

1. ¿Qué entiendes por seguridad informática?

Protección de sistemas contra el acceso no autorizado



2. ¿Qué técnica se suele utilizar en informática para asegurar el "no repudio"?

Uso de firmas digitales



3. ¿Qué significa la "integridad" de la información?

La información está completa, exacta y protegida contra modificaciones no autorizadas



4. ¿Qué entendemos en Seguridad por "amenaza"?

Cualquier circunstancia o evento con el potencial de causar daño a un sistema informático



5. ¿Qué diferencia a un hacker de un cracker?

Un hacker accede a sistemas por curiosidad, un cracker por beneficio ilícito



6. ¿Qué es la encriptación?

Un proceso de convertir información o datos en un código secreto para prevenir accesos no autorizados



7. ¿Qué tipos de malware conoces?

Todos los anteriores



8. ¿Qué es una DMZ en términos de redes de computadoras?

Una subred física o lógica que separa una red interna de una externa



9. ¿En qué orden protegerías los siguientes elementos y por qué?

Base de datos, servidor, sistema operativo, aplicación, tóner de impresora



10. ¿Qué medidas de seguridad informática implementarías?

Todas las anteriores



Pregunta 4



Correcta

Se puntúa 9,00 sobre 9,00

11. ¿Cuál es la principal función de un firewall en una red de computadoras?

Controlar y filtrar el tráfico que entra y sale de la red  

12. ¿Qué herramienta se utiliza comúnmente para realizar auditorías de seguridad en redes?

Nessus  

13. ¿Qué representa el término "alta disponibilidad" en un sistema informático?

Capacidad del sistema para operar continuamente sin fallos  

14. ¿Qué es un RAID y para qué se utiliza?

Una tecnología de almacenamiento que utiliza múltiples discos para aumentar la velocidad de acceso y/o 



15. ¿Qué es un cluster de servidores?

Un grupo de servidores que trabajan juntos para realizar tareas comunes  

16. ¿Cuál de las siguientes opciones describe mejor un "servidor proxy"?

Un servidor que actúa como intermediario entre un usuario de internet y el internet  

17. ¿Para qué se utilizan principalmente las SAN y las NAS en un entorno empresarial?

Para el almacenamiento de datos en red  

18. ¿Qué es el balanceo de carga en el contexto de una red de servidores?

Una técnica para distribuir el tráfico de red o carga de trabajo entre varios servidores  

19. ¿Qué técnica se utiliza para asegurar la privacidad y seguridad de las comunicaciones en internet?

Encriptación  

Pregunta 5

Parcialmente correcta

Se puntúa 9,00 sobre 10,00

¿Qué similitud existe entre las herramientas de protección de un albañil y un piloto de carreras?

Ambos utilizan guantes de protección. ❌

¿Cuál de las siguientes áreas NO está generalmente asociada con la seguridad informática?

Refrigeración de sistemas. ✔

¿Cuál es una característica fundamental de un sistema informático seguro?

Confidencialidad. ✔

¿Qué significa la confidencialidad en el contexto de la seguridad informática?

Los datos solo deben ser accesibles por usuarios autorizados. ✔

¿Qué debe garantizar la integridad en un sistema informático seguro?

Que los datos permanezcan completos y sin alteraciones no deseadas. ✔

Según la unidad de trabajo, ¿qué propiedad NO es fundamental para un sistema informático seguro?

Portabilidad. ✔

¿Qué es la paradoja de la seguridad en los sistemas informáticos?

A mayor seguridad, menor funcionalidad y usabilidad. ✔

¿Qué se busca equilibrar al administrar un sistema informático en un entorno corporativo?

Funcionalidad, usabilidad y seguridad. ✔

¿Quién debe decidir el equilibrio entre seguridad, funcionalidad y usabilidad de un sistema informático?

El administrador del sistema, en consenso con la dirección de la empresa. ✔

¿Cuál es un efecto común al incrementar la seguridad en un sistema informático según la paradoja de la seguridad?

Disminuye la funcionalidad y usabilidad. ✔

Pregunta 6

Correcta

Se puntúa 6,00 sobre 6,00

1. ¿Qué son las medidas pasivas de seguridad según la unidad de trabajo?

Son medidas implementadas generalmente desde la instalación del sistema para minimizar los efectos de



2. ¿Cuál es un ejemplo de medida de seguridad activa mencionado en la unidad de trabajo según la unidad de trabajo?

Instalación y supervisión de un firewall.



3. ¿Cuál es la principal diferencia entre las medidas de seguridad activas y pasivas según la unidad de trabajo?

Las medidas activas requieren supervisión constante, mientras que las pasivas no.



4. ¿Qué tipo de medidas de seguridad se conocen también como proactivas?

Medidas preventivas.



5. Según el texto, ¿las medidas paliativas se aplican en qué circunstancia?

Para mitigar los efectos de un problema una vez que ya ha ocurrido.



6. ¿Es correcto decir que las medidas preventivas solo se encuentran en la seguridad activa según la unidad de trabajo?

No, tanto las medidas preventivas como las paliativas pueden encontrarse tanto en la seguridad activa como



Pregunta 7

Correcta

Se puntúa 5,00 sobre 5,00

1. ¿Cuál es el propósito principal de restringir el acceso físico al CPD?

Para prevenir accesos no autorizados y robos. ✓

2. ¿Qué tipo de sistema de seguridad permite registrar los accesos al CPD?

Sistemas de control de acceso con registro de actividad. ✓

3. Según el RGPD, ¿qué es obligatorio cuando se instalan cámaras de videovigilancia?

Colocar carteles informativos sobre la videovigilancia. ✓

4. ¿Qué función tiene un candado Kensington?

Prevenir el robo de equipos informáticos. ✓

5. ¿Qué ventaja ofrecen los dispositivos NAS con software de grabación de videovigilancia?

Alternativa viable a los sistemas DVR/NVR. ✓

Actividad previa

◀ T2 - Práctica-(Tarea) AUDITORÍA DEL SISTEMA

Ir a...

Siguiente actividad

UT1_Autoevaluación.Cuestionario Parte II ▶

Mantente en contacto

Consejería de Educación. Región de Murcia

🌐 <https://aulavirtual.murciaeduca.es>

✉ soporte.cau@murciaeduca.es

📄 Resumen de retención de datos

📲 Descargar la app para dispositivos móviles