Promedio de calificaciones: 9,00 / 10,00

Pregunta 1

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

El estándar para la recopilación de información de incidentes de Ciberseguridad es:

- a. La Norma ISO/IEC 27032.
- b. La Norma RFC3227.
- c. La Norma ISO 27001.
- d. La Norma ISO 9001.

Quitar mi elección

Siguiente página

Pregunta 2

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

¿Qué se debe hacer con la información recopilada una vez concluido el análisis del incidente?:

- a. Respaldar cuidadosamente todos los datos, de cara a las auditorías.
- b. Una vez constatada la necesidad de guardar la información, descartar los datos inútiles.
- c. Respaldar la información personal durante 7 años, por imperativo legal.

Quitar mi elección

Página anterior

Siguiente página

Pregunta **3**

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

Los Pilares Fundamentales para la Recopilación de Evidencias son:

- a. Todos los anteriores.
- b. Las Personas.
- c. Los Procedimientos.
- d. La Tecnología.

Quitar mi elección

Página anterior

Siguiente página

Pregunta **4**

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

¿Qué características deben tener los procesos que recopilan información con valor legal?:

- a. Deben estar previamente validados por los auditores de calidad.
- b. Deben ser conocidos, replicables y no deben alterar la información al recogerla.
- c. Deben estar previamente validados por los analistas legales.

Quitar mi elección

Página anterior

Siguiente página

Pregunta **5**

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

La labor del Equipo Morado se efectúa:

- a. Durante la manifestación del incidente.
- b. Tras la finalización del incidente.
- c. Antes de la aparición del incidente en el entorno.

Quitar mi elección

Página anterior

Siguiente página

Pregunta **6**

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

Un Sistema de Almacenamiento en red:

- a. Tiene por defecto un cifrado de tres niveles.
- b. Tiene por defecto un cifrado simple.
- c. Por defecto no tiene ningún tipo de cifrado.
- d. Tiene por defecto un cifrado de dos niveles.

Quitar mi elección

Página anterior

Siguiente página

Pregunta **7**

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

Señalar el tipo de información que tiene mayor volatilidad:

- a. Logs del sistema.
- b. Registros y contenido de la caché.
- c. Información temporal del sistema.
- d. Configuración física y topología de la red.

Quitar mi elección

Página anterior

Siguiente página

Pregunta **8**

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

La mejor ventaja posible en la contención de incidentes es:

- a. Los metadatos contenidos en la información.
- b. Ninguna de las anteriores.
- c. La precisión de la información recopilada.
- d. El factor tiempo.

Quitar mi elección

Pregunta **9**

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

¿Qué es lo más importante cuando una evidencia cambia de condiciones de custodia?:

- a. Indicar cuándo y cómo se realizó el intercambio.
- b. Indicar quién ha custodiado la evidencia, cuánto tiempo y cómo la ha almacenado.
- c. Indicar dónde, cuándo y quién manejó la evidencia.
- d. Indicar dónde, cuándo y quién descubrió y recolectó la evidencia.

Quitar mi elección

Página anterior

Siguiente página

Pregunta **10**

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

¿Cuáles son las claves del procedimiento de almacenamiento de evidencias?:

- a. El almacén lógico/físico de la información.
- b. La Cadena de Custodia de la información.
- c. Ambas cosas son claves en este proceso.

Quitar mi elección

Página anterior

Terminar intento...