Promedio de calificaciones: 9,00 / 10,00.

Pregunta 1

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

¿A qué se debe principalmente la repetición de ataques anteriores?:

- a. A no actualizar las medidas antimalware.
- b. A no documentar adecuadamente la causa y el coste del incidente.
- c. A no aplicar medidas preventivas.

Quitar mi elección

Siguiente página

Pregunta 3

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

¿Cuál de las siguientes cuestiones no es un criterio para la toma de decisión en relación con la contención de un incidente?:

- a. Premisas para preservar las evidencias, de cara a una investigación posterior.
- b. Daño potencial a la organización.
- c. Tiempo de espera online.
- d. Hurto de activos y detalle de su valor.

Quitar mi elección

Página anterior

Siguiente página

Pregunta 4

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

La Ciberresiliencia es:

- a. La resistencia frente a la repetición de incidentes conocidos.
- b. La resistencia a los incidentes recursivos.
- c. La capacidad para resistir, proteger y defender el uso del ciberespacio frente a los atacantes.
- d. La resistencia informática extrema.

Quitar mi elección

Página anterior

Siguiente página

Pregunta **5**

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

La distribución Linux más popular en el área del Hacking Ético es:

- a. Fedora.
- b. Ninguna de las anteriores.
- c. Red Hat.
- d. SUSE.

Quitar mi elección

Página anterior

Siguiente página

Pregunta **6**

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

¿En caso de ausencia de procedimientos de actuación, qué suele ocurrir en los momentos iniciales de afectación por un incidente?:

- a. Se cortan súbitamente las comunicaciones LAN/WAN.
- b. Se levantan inmediatamente todos los escudos antimalware.
- c. Por lo general hay un cierto desconcierto en lo relativo a las medidas que se deben tomar.

Quitar mi elección

Página anterior

Siguiente página

Pregunta **7**

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

La identificación de la Causa Raíz suele suponer:

- a. El 75% del trabajo de análisis.
- b. El 10% del trabajo de análisis.
- c. El 80% del trabajo de análisis.
- d. El 50% del trabajo de análisis.

Quitar mi elección

Página anterior

Siguiente página

Pregunta **8**

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

La clave de las Lecciones Aprendidas es:

- a. La precisión del análisis del incidente.
- b. La calidad de las evidencias recopiladas.
- c. La documentación del incidente.
- d. La Ciber-Resiliencia de la organización.

Quitar mi elección

Página anterior

Siguiente página

Pregunta **9**

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

¿Cuál es la orientación principal de la política de combate de los incidentes en la actualidad?:

- a. Reactiva.
- b. De análisis forense y lecciones aprendidas.
- c. Proactiva y Preventiva.

Quitar mi elección

Página anterior

Siguiente página

Pregunta **10**

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

¿Cuáles son las principales ventajas de disponer de un SOC?:

- a. El análisis de los datos con posterioridad a una incidencia.
- b. El almacenamiento de datos relevantes en relación con los incidentes.
- c. Todas las anteriores.
- d. La centralización de la actividad de ciberseguridad de la empresa.

Quitar mi elección

Página anterior

Terminar intento...