¡Felicitaciones! ¡Aprobaste!

Calificación recibida 90 % **Calificación del último envío** 90 % **Para Aprobar** 80 % o más

Ir al siguiente elemento

1. ¿Qué paso del ciclo de vida de respuesta a incidentes del NIST implica la investigación y validación de alertas? **1 / 1 punto**

- ○ Recuperación
- ◉ Análisis
- ○ Descubrimiento
- ○ Detección

✓ **Correcto**

2. En la respuesta a incidentes, la documentación proporciona un conjunto establecido de directrices que los miembros de una organización pueden seguir para completar una tarea. ¿Qué beneficio aporta? **0 / 1 punto**

- ○ Estandarización
- ○ Integridad
- ○ Confiabilidad
- ◉ Transparencia

✗ **Incorrecto**
Revisa el video sobre documentación.

3. Una organización está trabajando en la implementación de una nueva herramienta de seguridad. Se ha encargado a un analista de seguridad que elabore documentación sobre el flujo de trabajo que describa el proceso de uso de la herramienta. ¿Qué beneficio de la documentación presenta este escenario? **1 / 1 punto**

- ◉ Estandarización
- ○ Transparencia
- ○ Claridad
- ○ Calidad

✓ **Correcto**

4. ¿De cuáles de las siguientes opciones establecen la prueba los documentos de la cadena de custodia? Selecciona dos respuestas. **1 / 1 punto**

- ☐ Calidad
- ☐ Validación
- ☑ Fiabilidad

✓ **Correcto**

- ☑ Integridad

✓ **Correcto**

5. ¿Qué afirmación describe mejor la funcionalidad de los manuales de estrategias automatizados? **1 / 1 punto**

- ○ Utilizan una combinación de diagramas de flujo y entradas manuales para ejecutar tareas y acciones de respuesta.
- ○ Requieren el uso de la intervención humana para ejecutar tareas.
- ◉ Utilizan la automatización para ejecutar tareas y acciones de respuesta.
- ○ Requieren la combinación de intervención humana y automatización para ejecutar tareas.

✓ **Correcto**

Correcto

6. Utilizando el triaje, ¿qué alerta se consideraría prioritaria y requeriría una respuesta inmediata? 1 / 1 punto

- Un correo electrónico de phishing
- Múltiples inicios de sesión fallidos desde varias ubicaciones
- (•) Detección de ransomware
- Inicios de sesión fallidos con cuentas deshabilitadas

Correcto

7. Completa el espacio en blanco: La contención es el acto de limitar y _____ daños adicionales causados por un incidente. 1 / 1 punto

- (•) prevenir
- eliminar
- erradicar
- detectar

Correcto

8. Completa el espacio en blanco: La erradicación es _____ de todos los elementos del incidente de los sistemas afectados. 1 / 1 punto

- (•) la eliminación completa
- la prevención completa
- la desconexión completa
- el aislamiento completo

Correcto

9. ¿Qué preguntas pueden plantearse en una reunión sobre lecciones aprendidas? Selecciona tres respuestas. 1 / 1 punto

- [x] ¿Qué pudo haberse hecho de otra manera?

Correcto

- [ ] ¿Qué empleado tuvo la culpa?
- [x] ¿A qué hora ocurrió el incidente?

Correcto

- [x] ¿Cuáles fueron las medidas que se tomaron para la recuperación?

Correcto

10. Durante una reunión sobre lecciones aprendidas tras un incidente, un participante de la reunión desea identificar acciones que la organización puede emprender para evitar que se produzcan incidentes similares en el futuro. ¿A qué sección del informe final debería referirse para obtener esta información? 1 / 1 punto

- (•) Recomendaciones
- Línea de tiempo
- Detección
- Resumen ejecutivo

Correcto