¡Felicitaciones! ¡Aprobaste!

Calificación recibida 100 % **Calificación del último envío** 100 % **Para Aprobar** 80 % o más

Ir al siguiente elemento

1. ¿Cuál de los siguientes es un ejemplo de incidente de seguridad? **1 / 1 punto**

- ○ Un fenómeno meteorológico extremo provoca una interrupción de la red.
- ◉ Se realizan diversas transferencias no autorizadas de documentos confidenciales a un sistema externo.
- ○ Una empresa experimenta un aumento del volumen de tráfico en su sitio web debido al lanzamiento de un nuevo producto.
- ○ Un usuario autorizado envía un archivo por correo electrónico a un cliente.

✓ **Correcto**

2. ¿Qué proceso se utiliza para proporcionar un plan de respuesta efectiva a incidentes? **1 / 1 punto**

- ◉ El ciclo de vida de respuesta a incidentes del Instituto Nacional de Estándares y Tecnología (NIST).
- ○ Las 5 W de un incidente.
- ○ El marco de ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST).
- ○ El diario de gestión de incidentes.

✓ **Correcto**

3. ¿Con qué paso comienza el ciclo de vida de respuesta a incidentes del Instituto Nacional de Estándares y Tecnología (NIST)? **1 / 1 punto**

- ○ Detección y análisis
- ◉ Preparación
- ○ Contención, erradicación y recuperación
- ○ Actividad posterior a un incidente

✓ **Correcto**

4. ¿Cuáles son algunas de las funciones que desempeña un equipo de respuesta a incidentes de seguridad informática (CSIRT)? Selecciona tres respuestas. **1 / 1 punto**

- ☑ Analista de seguridad

✓ **Correcto**

- ☑ Coordinador de incidentes

✓ **Correcto**

- ☐ Gerente de incidentes
- ☑ Responsable técnico

✓ **Correcto**

5. ¿Qué elementos comunes contienen los planes de respuesta a incidentes? Selecciona dos respuestas. **1 / 1 punto**

- ☑ Procedimientos de respuesta a incidentes

✓ **Correcto**

- ☑ Información del sistema

✓ **Correcto**

- [ ] Simulaciones
- [ ] Información financiera

6. Un analista de ciberseguridad recibe una alerta sobre un posible incidente de seguridad. ¿Qué tipo de herramienta debería usar para examinar la evidencia de la alerta con mayor detalle? **1 / 1 punto**

- ○ Una herramienta de documentación
- ○ Una herramienta de recuperación
- ○ Una herramienta de detección
- ◉ Una herramienta de investigación

✓ **Correcto**

7. ¿Cuáles de los siguientes métodos puede utilizar un analista de seguridad para generar una documentación efectiva? Selecciona dos respuestas. **1 / 1 punto**

- [x] Redactar la documentación de forma que minimice la confusión.

✓ **Correcto**

- [x] Proporcionar explicaciones claras y concisas de conceptos y procesos.

✓ **Correcto**

- [ ] Redactar la documentación utilizando lenguaje técnico.
- [ ] Proporcionar documentación en formato impreso.

8. ¿Cuál es la diferencia entre un sistema de detección de intrusiones (IDS) y un sistema de prevención de intrusiones (IPS)? **1 / 1 punto**

- ○ Un IDS detiene la actividad intrusiva, mientras que un IPS monitorea la actividad del sistema y alerta sobre la actividad intrusiva.
- ○ Un IDS y un IPS tienen las mismas capacidades.
- ○ Un IDS automatiza la respuesta y un IPS genera alertas.
- ◉ Un IDS monitorea la actividad del sistema y alerta de las actividades intrusivas, mientras que un IPS detiene dichas actividades.

✓ **Correcto**

9. ¿Cuál es la diferencia entre una herramienta de gestión de eventos e información de seguridad (SIEM) y una herramienta de orquestación, automatización y respuesta de seguridad (SOAR)? **1 / 1 punto**

- ○ Las herramientas SIEM se utilizan para la gestión de casos, mientras que las herramientas SOAR recopilan, analizan e informan sobre los datos de registro.
- ○ Las herramientas SIEM utilizan la automatización para responder a los incidentes de seguridad. Las herramientas SOAR recopilan y analizan datos de registro, que luego son revisados por analistas de seguridad.
- ◉ Las herramientas SIEM recopilan y analizan datos de registro, que luego son revisados por analistas de seguridad. Las herramientas SOAR, en cambio, utilizan la automatización para responder a los incidentes de seguridad.
- ○ Las herramientas SIEM y las herramientas SOAR tienen las mismas capacidades.

✓ **Correcto**

10. Completa el espacio en blanco: Durante el paso de _____ del proceso SIEM, los datos sin procesar recopilados se transforman para crear consistencia en los registros. **1 / 1 punto**

- ○ agregación de datos
- ○ recopilación de datos
- ○ análisis de datos
- ◉ normalización de datos

✓ **Correcto**