Prepara tu examen de IDC

Introducción

Cada centro, cada año y cada docente, puede plantear al alumnado un modelo de examen concreto que, a su criterio, pueda servir como una correcta evaluación del módulo.

Para ayudar a preparar las evaluaciones, he pensado que podría ser de ayuda crear un archivo único para cada módulo, que pueda crecer cada año con el feedback y apoyo de la comunidad, con cuestionarios de todo tipo, con solucionario o solo los enunciados, pues la intención primera es poder ofrecer una idea de lo que podemos encontrarnos a la hora de una evaluación, poder aprender con ello, y no algo que una persona acabe memorizando, y esperando, sin comprender ni ahondar en la materia, que aparezca mágicamente en el examen.

Este documento, por tanto, no pretende ser una guía única y veraz de exámenes pasados o futuros, pero si una fuente de información sobre la que basar vuestros estudios.

Posibles modelos.

Modelo 1.

Ejemplo para preparación.

PREGUNTAS DEL TEST DE CONOCIMIENTOS:

1. (Puntuación: 0,25). ¿Cuál es la tercera regla pragmática de la ciberseguridad según Agile Corporation?

A) Privacidad.
B) Resiliencia.
C) Respuesta.
D) Protegerse de lo desconocido.

2. (Puntuación: 0,25). ¿Qué es OSINT?

A) Una técnica de hackeo.
B) Un proceso de análisis de datos recopilados de fuentes de acceso público.
C) Un protocolo de seguridad informática.
D) Un tipo de malware.

3. (Puntuación: 0,25). ¿Qué es una tubería de Logstash?

A) Una herramienta para filtrar información antes de insertarla en la base de datos.
B) Una definición de entrada, filtrado y salida hacia Elasticsearch.
C) Un punto de acceso a un protocolo de comunicaciones.
D) Un formato de archivo utilizado por Logstash.

4. (Puntuación: 0,25). ¿Qué es un SOC en la estrategia integral de ciberseguridad?

A) Un software antivirus.
B) Un cortafuegos personal.
C) Un entorno de detección y análisis.
D) Un sistema de copias de seguridad.

PREGUNTAS TEÓRICO-PRÁCTICAS:

PTP1. (2 puntos). Decálogo de seguridad.

El CCN publica y actualiza periódicamente un informe en el que se detallan tanto los Principios Generales en Materia de Ciberseguridad, como recomendaciones, medidas fundamentales y buenas prácticas para concienciar y facilitar el uso seguro de las Tecnologías de la Información y la Comunicación. Dicho informe incluye un Decálogo Básico de Ciberseguridad.

Este decálogo recoge en su principio número 5 que "***Cifrar la información sensible*** y revisar con frecuencia el mecanismo de cifrado para usar el que sea más fuerte en cada momento".

Para cumplir con este principio los trabajadores de una empresa usan un cifrado simétrico de los mensajes, para lo que usan una única clave secreta que solamente la conocen los empleados de la empresa. La clave usada es "TopS3cr3t".

Responde a las siguientes preguntas:

1. ¿Cuál es el proceso de comunicación encriptada entre trabajadores usando la clave indicada? (0,4)

2. ¿Qué principales problemas detectas con el uso de esta clave? Justifica dos problemas. (0,6)

3. Si deciden cambiar este tipo de cifrado por un cifrado de clave asimétrica, ¿Cuál es el proceso para que dos personas puedan comunicarse de forma Segura usando este cifrado asimétrico? (0,6)

4. ¿Qué riesgo corre el uso de este tipo de claves asimétricas? (0,4)

PTP2. (1 punto). Plan de respuesta ante incidentes.

Cuando se sospecha que se está produciendo un posible incidente se deben realizar una serie de actuaciones recogidas en el plan de respuesta ante incidentes.

En el caso en el que se ha conseguido eliminar un incidente real o se ha descartado como un falso positivo, el proceso de respuesta ante incidentes no ha terminado.

Responde a las siguientes preguntas relativas a la fase de cierre de incidentes:

1. ¿Qué son las lecciones aprendidas? ¿Se debe recoger alguna información referente al incidente? (0,5)

2. ¿cómo se relaciona esta actuación con el proceso de mejora continua de la empresa? Justifica la respuesta. (0,5)

Modelo 2.

Ejemplo pasado por alumnado.

Test

1. ¿Qué se debe hacer para protegerse frente a posibles amenazas según el decálogo básico de Ciberseguridad?
2. ¿Qué objetivo persiguen las auditorías internas de cumplimiento en materia de prevención?
3. ¿Qué es el contenido abusivo en términos de ciberseguridad?
4. ¿Cuál es el objetivo de las recomendaciones en el ámbito de la seguridad física y del entorno según la norma ISO/IEC 27001?
5. ¿Qué herramienta permite comprobar si un nombre de usuario está disponible en más de 550 servicios online? (NameCheck, Tineye, Spokeo, Knowem)
6. ¿Quiénes pueden notificar un ciberincidente al CSIRT de referencia?
7. ¿Qué consecuencias puede tener un fallo en la cadena de custodia?
8. ¿Qué se debe hacer con la información sobrante o confusa durante el análisis preliminar de evidencias?
9. ¿Cuál es una recomendación importante durante la fase de mitigación de un ciberincidente?
10. ¿Cuál es el criterio principal para la notificación de incidentes de ciberseguridad?
11. ¿En qué estado se encuentra un ciberincidente que ha sido resuelto, pero no se ha recibido respuesta por parte del organismo afectado?
12. ¿Cómo se puede controlar el arranque y detención del servicio de Snort?
13. ¿Qué es el SSH?
14. ¿Cuál de las siguientes secciones del menú de la página web de Kibana se utiliza para diseñar Tableros o cuadros de Mando?
15. ¿Qué se determina evaluando el impacto de un ciberincidente?
16. ¿A qué niveles de impacto de peligrosidad se deben notificar los incidentes según la Guía Oficial?
17. ¿Qué incorpora la capa de Sesión?
18. ¿De qué se compone la Capa de Aplicación?
19. ¿Qué es una tubería de Logstash?
20. ¿Cuál es el objetivo de la fase de análisis preliminar de evidencias?

PTP1.Decálogo de seguridad

1. Principal riesgo (ataque al que se expone) del uso de contraseña con “significado”.
2. Principal riesgo (ataque al que se expone) del uso de contraseña con una longitud menor de 8 caracteres.
3. Indica 4 requisitos para establecer una política de contraseñas seguras.
4. ¿Qué métodos de autenticación adicionales se podrían implementar para mejorar la seguridad en el acceso a equipos? Explique un par de ellos.

PTP2. PILAR (Datos gráfica)

BBDD --- PC --- Web Server --- Person

Current --- Target PILAR

1. Identifica los activos y determina los dominios de seguridad a los que podrían pertenecer.
2. Indica la bajada esperada en el riesgo tras la implementación de las salvaguardas.
3. ¿Estos activos llegarán a alcanzar un nivel de amenaza recomendado por PILAR tras la implementación de estas posibles salvaguardas?
4. Describe ligeramente el proceso, es decir, los pasos a realizar para conseguir una gráfica con el análisis de riesgos.

PTP3. Plan de Respuesta ante Incidentes

1. Indica un par de medidas que se pueden implementar para una correcta detección de incidentes.
2. Si tras los primeros indicios se prevé que puede tratarse de un incidente real, ¿cuáles deben ser los primeros pasos a realizar antes de poder hacer frente al incidente. Explicar al menos dos actuaciones.