Cybersecurity Foundation Professional Certificate – CSFPC

Sample Exam V022023

1. ¿Cuál de los siguientes aspectos es un elemento clave de la seguridad de la información?

a) Confidencialidad
b) Fiabilidad
c) Privacidad
d) Anonimato

2. ¿Qué aspecto de la seguridad de la información incluye leyes y regulaciones nacionales e internacionales y obligaciones de cumplimiento?

a) Desarrollo de tecnología
b) Cifrado de datos
c) Adherencia a regulaciones y leyes
d) Entrenamiento en seguridad de la información

3. ¿En la seguridad de la información qué se enfoca en la recolección, análisis y presentación de evidencia digital en casos legales y criminales?

a) La Criptografía
b) La Seguridad de la red
c) Forense Digital
d) La Gestión de identidades y acceso

4. ¿Qué proceso en la seguridad de la información se enfoca en evaluar y desarrollar opciones para hacer frente a la exposición a riesgos?

a) Monitoreo de seguridad
b) Planificación de continuidad de negocios
c) Gestión de riesgos
d) Desarrollo de políticas de seguridad

5. ¿Qué es el diseño abierto en el contexto de la seguridad de la información?

a) Es una estrategia de seguridad que no permite la revisión de los controles de seguridad
b) Es una estrategia de seguridad que permite a los expertos revisar el funcionamiento de los controles de seguridad para garantizar su corrección
c) Es una estrategia de seguridad que no permite la identificación de los fallos en los controles de seguridad
d) Es una estrategia de seguridad que permite a los expertos revisar el funcionamiento de los controles de seguridad pero socava su seguridad

6. ¿Cuáles son las estrategias de arquitectura de seguridad del NIST mencionadas en el programa de certificación de CertiProf?

a) Monitor de Referencia, Comportamiento y Defensa en profundidad
b) Aislamiento, Comportamiento y Defensa en profundidad
c) Monitor de Referencia, Aislamiento y Defensa en profundidad
d) Comportamiento, Monitor de Referencia y Aislamiento

7. ¿Cuál es el propósito del principio de precaución en el contexto de la seguridad de la información?

a) Fomentar el despliegue rápido de innovaciones tecnológicas sin considerar su potencial impacto negativo
b) Ignorar el potencial impacto negativo de las innovaciones tecnológicas en la seguridad de la información
c) Considerar el potencial impacto negativo de las innovaciones tecnológicas en la seguridad de la información antes de su despliegue a gran escala
d) Promover el despliegue masivo de innovaciones tecnológicas sin importar su potencial impacto negativo

8. ¿Cuáles son dos enfoques principales para el modelado formal en el contexto de la seguridad de la información mencionados en el CYBOK Guide?

a) Matemático y Simbólico
b) Computacional y Matemático
c) Computacional y Simbólico
d) Experimental y Simbólico

9. ¿Cuál es el tema de gran relevancia en relación a los costos de la seguridad de la información en el CYBOK Guide?

a) Investigación de la Ciberdelincuencia
b) Tecnología de la Seguridad
c) Economía de la Seguridad
d) Política de la Seguridad

10. ¿Qué elementos son considerados al calcular la probabilidad en el proceso de gestión de riesgos en seguridad de la información según el CYBOK Guide? Seleccione todas las que apliquen.

a) Frecuencia de ocurrencia de eventos
b) Presencia de vulnerabilidad desconocida
c) Naturaleza de la amenaza
d) Presencia de vulnerabilidad conocida

11. ¿Cuál es el papel del monitoreo de seguridad en la gestión de incidentes de ciberseguridad según el CYBOK Guide?

a) Identificación de vulnerabilidades en sistemas
b) Análisis de las causas de los incidentes de seguridad
c) Corrección de las vulnerabilidades identificadas
d) Detección temprana y respuesta a los incidentes de seguridad

12. ¿Cuál de las siguientes opciones es un principio que define qué controles se necesitan para identificar positivamente operaciones conformes a una política de seguridad y rechazar las demás?

a) Autenticación de doble factor
b) Valores predeterminados a prueba de fallos (Fail-safe defaults)
c) Cifrado de extremo a extremo
d) Análisis de amenazas en tiempo real

13. ¿Cuál de los siguientes elementos no forma parte de la definición de Renn para evaluación de riesgos en seguridad de la información?

a) Resultados que repercuten en lo que valora el ser humano
b) Posibilidad de ocurrencia (incertidumbre)
c) Combinación de resultados y posibilidad de ocurrencia
d) Relación entre riesgo y seguridad

14. ¿Qué enfoque es necesario considerar en situaciones en las que los riesgos son menos claros (riesgos complejos) en el análisis de seguridad de la información?

a) La transferencia del riesgo
b) Análisis de impacto de la ocurrencia
c) Análisis de coste-beneficio
d) Análisis de rentabilidad

15. ¿Qué tipo de modelo de gobernanza del riesgo se enfoca en ser claro, abierto y responsable con respecto a la toma de decisiones de seguridad de la información?

a) Tecnocracia
b) Decisionista
c) Transparente
d) Directivo

16. ¿Cuáles son los tres componentes clave de la evaluación de riesgos en la seguridad de la información?

a) Vulnerabilidad, probabilidad, e impacto
b) Amenaza, tiempo y costo
c) Protección, detección y respaldo
d) Sensibilidad, precisión y eficacia

17. ¿Qué es una consecuencia negativa de que una amenaza explote una vulnerabilidad?

a) Vulnerabilidad
b) Probabilidad
c) Impacto
d) Riesgo

18. ¿Cuál de las siguientes fases NO forma parte de los siete pasos del NIST?

a) Priorizar y Alcance
b) Orientar
c) Crear un Target Profile
d) Conducir un Risk Assessment

19. ¿Qué es el acoso cibernético?

a) El uso de medios electrónicos para seguir a una persona
b) El robo de datos
c) El uso de correos electrónicos fraudulentos
d) La difusión de información falsa en línea

20. ¿Qué es Phishing?

a) Un tipo de spam que envía correos electrónicos que parecen ser de servicios genuinos
b) Una actividad dañina facilitada por Internet que implica seguir a otra persona
c) El robo de datos
d) El acecho cibernético

21. ¿Cuál de los siguientes enunciados mejor describe la discusión sobre la aplicación de leyes y regulaciones a la ciberseguridad?

a) Los legisladores y jueces deben reexaminar todos los principios con respecto a la ciberseguridad y abandonar los precedentes establecidos
b) El Internet es una herramienta de acción humana que debe regirse por las mismas leyes que se aplicaban antes de su existencia
c) La ciberseguridad debe regirse por un conjunto de leyes y regulaciones específicas
d) La ciberseguridad es una jurisdicción legal separada y distinta del espacio real

22. ¿Qué es una patente?

a) Una forma de proteger la propiedad intelectual
b) Una forma de proteger la propiedad material
c) Una forma de proteger la seguridad de la información
d) Una forma de registrar una patente a nivel estatal

23. ¿Cuáles son las limitaciones generales de los seres humanos en términos de seguridad de la información?

a) Capacidad de procesar grandes cantidades de datos
b) Capacidad de detectar señales de seguridad
c) Solo pueden prestar atención a una tarea a la vez
d) Ninguna de las anteriores

24. ¿Qué es la Autenticación de Múltiples Factores?

a) Una forma de autenticación que usa un solo método para validar la identidad del usuario
b) Una forma de autenticación que combina varios métodos para validar la identidad del usuario
c) Una forma de autenticación que usa contraseñas únicas para validar la identidad del usuario
d) Una forma de autenticación que usa dos factores para validar la identidad del usuario

25. ¿Cuáles son los tres principales criterios utilizados para evaluar la usabilidad?

a) Precisión, velocidad y satisfacción
b) Eficiencia, exactitud y satisfacción
c) Eficiencia, exactitud y rapidez
d) Precisión, eficiencia y satisfacción

26. ¿Qué objetivo busca la confidencialidad basada en la Ofuscación de los datos?

a) Proteger la información sensible de los usuarios
b) Evitar que una persona acceda a la información sensible de los usuarios
c) Controlar el grado en que un adversario puede hacer inferencias sobre la información sensible de los usuarios
d) Garantizar la integridad de los datos

27. ¿Qué es la anonimización de datos?

a) Una técnica para encriptar la información para que sea ilegible
b) Un proceso para eliminar cualquier información personal identificable de un conjunto de datos
c) Una forma de asegurar que los datos se mantengan seguros
d) Una práctica para evitar la divulgación de información privada

28. ¿Qué es la adición de datos ficticios en la seguridad de la información?

a) Una práctica para evitar que los hackers accedan a los datos reales
b) Una técnica para mejorar la seguridad de la información
c) Una práctica para aumentar los tiempos de respuesta
d) Una técnica para aumentar la seguridad al agregar datos falsos a la información real

29. ¿Qué son los programas potencialmente no deseados (PUP)?

a) Un programa malicioso diseñado para robar información
b) Un programa que proporciona herramientas para aumentar la seguridad
c) Un programa que se instala sin el consentimiento de un usuario
d) Un programa que se descarga con la intención de mejorar la funcionalidad

30. ¿Qué es el método de Fuzzing?

a) Una técnica de prueba de seguridad que envía un conjunto de entradas inválidas a un programa para evaluar su respuesta
b) Una técnica de prueba de seguridad que se basa en el análisis de patrones de tráfico para detectar ataques
c) Una técnica de prueba de seguridad que busca vulnerabilidades en aplicaciones web
d) Una técnica de prueba de seguridad que explora la estructura interna de un programa para detectar vulnerabilidades

31. Basado en CyBOK. ¿Cuál es el primer paso en el Ciclo de Gestión de Incidentes?

a) Establecer los controles de seguridad
b) Identificar el incidente
c) Establecer los procesos y capacidades adecuadas
d) Resolver el incidente

32. Basado en CyBOK. ¿Cuáles son los tres niveles principales para comunicar un mensaje de alerta?

a) Estructura, Codificación y Mensaje
b) Diseño, Protocolo e Integridad
c) Esquema, Codificación y Protocolo de transporte
d) Diseño, Criptografía y Mensaje

33. ¿Qué es el análisis de malware?

a) El proceso de aprender acerca de los comportamientos maliciosos
b) El proceso de escribir y desarrollar malware
c) El proceso de destrucción de malware
d) El proceso de prevenir la propagación de malware

34. ¿Qué es Syslog en seguridad de la información?

a) Una técnica de encriptación de datos
b) Una herramienta de administración de usuarios
c) Un protocolo de seguridad para la transmisión de datos
d) Un sistema de registro de eventos y notificaciones

35. ¿Qué es la Teoría de los Patrones del Crimen?

a) Una teoría que describe cómo los ciberdelincuentes se comportan en la red
b) Una teoría que describe cómo los hackers se conectan a la red
c) Una teoría que describe cómo los ciberdelincuentes usan la tecnología para cometer crímenes
d) Una teoría que describe cómo los ciberdelincuentes pueden evitar la detección

36. ¿Cuál de los siguientes mejor describe la Teoría de la Actividad Rutinaria según el CYBOK Guide?

a) Un enfoque para el diseño de sistemas de seguridad básicos
b) Un proceso para determinar los requisitos de seguridad
c) Una estrategia para mejorar los procedimientos de seguridad
d) establece que la ocurrencia de un crimen está influenciada principalmente por una oportunidad inmediata para que se cometa un crimen

37. ¿Qué es la ofuscación?

a) Una técnica para procesar datos sin riesgo para las personas
b) Una herramienta para cifrar los datos
c) Una técnica para ocultar los datos
d) Una práctica para desvincular la identidad de la información

38. ¿Qué es la técnica de generalización en seguridad de la información?

a) Una técnica para mejorar la seguridad de la información almacenada
b) Un enfoque para limitar los accesos a la información
c) Una metodología para simplificar la seguridad de la información
d) Una técnica para reducir la precisión con la que se comparten los datos, con el objetivo de reducir la precisión de las inferencias del adversario

39. ¿Qué es el servicio en el que los ciberdelincuentes pueden subcontratar la instalación de malware en ordenadores infectados en su nombre?

a) Una prueba de seguridad de la información
b) Una herramienta de cifrado
c) Una plataforma de análisis de seguridad
d) Servicios de pago por instalación (PPI)

40. ¿Qué es el Web defacement?

a) Una forma de vulnerabilidad en un sitio web
b) Una forma de ofensa personal en línea
c) Una forma de pirateo en un sitio web
d) Una forma de vandalismo digital en un sitio web

41. ¿Qué es el ciberbullying?

a) Una forma de expresión de emociones en línea
b) El uso de Internet para amenazar a alguien
c) Una forma de intimidación en línea
d) Una forma de conectar con personas en línea

42. ¿Qué es el cryptojacking?

a) Una forma de piratear criptomonedas
b) Una forma de piratear contraseñas
c) Una forma de minar criptomonedas utilizando scripts de páginas web
d) Una forma de instalar malware en los ordenadores de las víctimas

43. ¿Qué es el fraude de tarifa adelantada?

a) Una forma de estafa por internet que implica el pago de tarifas por adelantado para obtener un producto o servicio
b) Una forma de estafa por internet que implica el envío de correos electrónicos para robar información personal
c) Una forma de estafa por internet que implica la manipulación de tarifas en línea
d) Una forma de estafa por internet que implica el envío de archivos maliciosos para robar información

44. ¿Cuáles de los siguientes son las cinco funciones incluidas en el marco de seguridad de información NIST?

a) Identificar, Proteger, Detectar, Reaccionar, Recuperar
b) Identificar, Proteger, Monitorear, Reaccionar, Recuperar
c) Identificar, Proteger, Detectar, Reaccionar, Reorganizar
d) Identificar, Proteger, Detectar, Responder, Recuperar

45. ¿Qué se incluye en una evaluación de riesgo de seguridad de la información?

a) Análisis de amenazas
b) Clasificación de vulnerabilidades
c) Inventario de activos
d) Respaldo de datos

Respuestas

1. b
2. c
3. c
4. c
5. b
6. c
7. c
8. c
9. c
10. b,c,d
11. d
12. b
13. d
14. c
15. c
16. a
17. c
18. c
19. a
20. a
21. b
22. a
23. c
24. b
25. d
26. c
27. b
28. d
29. c
30. a
31. c
32. c
33. a
34. d
35. c
36. d
37. d
38. d
39. d
40. d
41. c
42. c
43. a
44. d
45. a