CertiProf Lead Cybersecurity Professional Certificate (LCSPC)

Preguntas de apoyo (V092020)

1. ¿Cuál no es un objetivo del CSF del NIST?

a) Ayudar a los responsables y operadores de infraestructuras críticas a identificar, inventariar y gestionar riesgos informáticos.
b) Establecer un lenguaje distinto para gestionar riesgos de ciberseguridad.
c) Establecer criterios para la definición de métricas para el control del desempeño en la implementación.
d) Ninguna de las anteriores.

2. ¿Qué son los Perfiles del marco del CSF del NIST?

a) Presenta los estándares, directrices y prácticas de la industria de una manera que permita la comunicación de actividades y resultados de ciberseguridad.
b) Proporcionan un contexto sobre cómo una organización ve el riesgo de la ciberseguridad.
c) Representa los resultados basados en las necesidades empresariales que una organización ha seleccionado de las Categorías y Subcategorías.
d) Ninguna de las anteriores.

3. ¿Cuál no es una función del Framework Core del CSF del NIST?

a) Detectar (DE).
b) Analizar (AN).
c) Identificar (ID).
d) Ninguna de las anteriores.

4. ¿Qué permite la función Recuperar?

a) Desarrollar e implementar las actividades apropiadas para mantener los planes de resiliencia.
b) Desarrollar e implementar las actividades apropiadas para identificar la ocurrencia de un evento de ciberseguridad.
c) Desarrollar e implementar las salvaguardias apropiadas para asegurar la provisión de servicios de Infraestructura crítica.
d) Ninguna de las anteriores.

5. ¿Cuáles son las subcategorías?

a) Extensión de las funciones de Ciberseguridad.
b) Controles de Ciberseguridad.
c) Secciones específicas de normas.
d) Ninguna de las anteriores.

6. ¿El Framework NIST consta de 5 funciones simultáneas y continuas?

a) Falso.
b) Verdadero.

7. En el proceso de gestión de riesgo ¿con qué debe cumplir el nivel de implementación de RIESGO INFORMADO?

a) Las prácticas de gestión de riesgos son aprobadas por la administración, pero no pueden establecerse como políticas de toda la organización.
b) Las prácticas de gestión de riesgos de la organización son formalmente aprobadas y expresadas como políticas.
c) La organización adapta sus prácticas de ciberseguridad basadas en las lecciones aprendidas y los indicadores predictivos.
d) Ninguna de las anteriores.

8. ¿Las 5 funciones continuas del CSF del NIST dan pie al ciclo de vida de la Ciberseguridad?

a) Verdadero.
b) Falso.
c) Depende de las partes interesadas.
d) Ninguna de las anteriores.

9. ¿Qué indica la actividad “crear un perfil actual del CSF”?

a) La organización crea un perfil objetivo que se centra en la evaluación de las categorías y subcategorías del marco que describen los resultados deseados de ciberseguridad de la organización.
b) La organización desarrolla un perfil actual indicando los resultados de categoría y subcategoría del núcleo del Marco que se están alcanzando actualmente.
c) Esta evaluación podría guiarse por el proceso general de gestión de riesgos de la organización o por actividades anteriores de evaluación de riesgo.

10. ¿Qué permite la función Identificar?

a) Desarrollar e implementar las actividades apropiadas para mantener los planes de resiliencia.
b) Desarrollar el entendimiento organizacional para manejar el riesgo de ciberseguridad a los sistemas, activos, datos y capacidades.
c) Desarrollar e implementar las salvaguardias apropiadas para asegurar la provisión de servicios de Infraestructura crítica.
d) Ninguna de las anteriores.

11. "El Marco proporciona un lenguaje común para comunicar los requisitos entre las partes interesadas interdependientes responsables de la prestación de servicios esenciales de infraestructura crítica". El anterior enunciado es:

a) Verdadero.
b) Falso.
c) Depende de las partes interesadas.
d) Ninguna de las anteriores.

12. ¿Cuál es el objeto y campo de aplicación del ISO/IEC 27032?

a) Proporcionar una guía para mejorar el estado de la Ciberseguridad, destacando aspectos únicos de dicha actividad y su dependencia de otros ámbitos de seguridad.
b) Aplicar como marco de referencia para la seguridad de la información en los países miembros de América latina.
c) Desarrollar e implementar las actividades apropiadas para mantener los planes de resiliencia cibernética.
d) Ninguna de las anteriores.

13. Según el ISO/IEC 27032, ¿cuál de los siguientes ámbitos no se encuentra relacionado con la Ciberseguridad?

a) Seguridad de la Información.
b) Seguridad de Internet.
c) Seguridad en RRHH.
d) Ninguna de las anteriores.

14. ¿Cuál de los proveedores se incluyen dentro de las partes interesadas del ciberespacio?

a) Proveedores de servidores.
b) Proveedores de aplicaciones.
c) Proveedores de accesos remotos.
d) Ninguna de las anteriores.

15. ¿Qué incluye la categoría de Activos personales del ciberespacio?

a) Laptop de la entidad.
b) La propiedad intelectual.
c) Moneda virtual.
d) Ninguna de las anteriores.

16. ¿Cuál opción no pertenece a las Amenazas para los activos personales?

a) Acceso y exploit indebidos.
b) Robo del dinero de la persona y fraude.
c) Fuga o robo de información personal.
d) Ninguna de las anteriores.

17. ¿Cuál opción no pertenece a los Roles de las partes interesadas en la Ciberseguridad?

a) Roles de las organizaciones.
b) Roles de los consumidores.
c) Roles de los socios.
d) Ninguna de las anteriores.

18. ¿Qué indican las Directrices para las organizaciones y proveedores de servicios?

a) Gestionar el riesgo de seguridad de la información en el negocio, entre otras.
b) Deberían orientar a los consumidores sobre cómo mantenerse seguros en línea, entre otras.
c) Cómo ellos podrían influir positivamente en el estado de la Ciberseguridad, entre otras.
d) Ninguna de las anteriores.

19. Según el ISO/IEC 27032, ¿cuáles son las categorías de los controles de Ciberseguridad?

a) Controles a nivel de software, protección del servicio, controles del usuario final y controles contra ataques de ingeniería social.
b) Controles a nivel de aplicación, protección del servicio, controles del usuario final y controles contra ataques de ingeniería inversa.
c) Controles a nivel de aplicación, protección del servidor, controles del usuario final y controles contra ataques de ingeniería social.
d) Ninguna de las anteriores.

20. ¿Qué incluyen el Marco de intercambio y coordinación de la información?

a) Los socios estratégicos.
b) Las Personas y Organizaciones.
c) Las técnicas de aprendizaje.
d) Ninguna de las anteriores.

21. ¿En dónde los controles del ISO/IEC 27032 se pueden incluir, complementariamente con el ISO 27001?

a) La política del SGSI.
b) El alcance del SGSI.
c) La declaración de aplicabilidad (Statement of Applicability- SoA).
d) Ninguna de las anteriores.

22. Dentro del Framework del NIST, ¿cuáles estándares se incluyen como controles de referencia normativos?

a) ISO/IEC 27001, NIST SP 800-82, ISA 62443.
b) CIS CSC 7.1, COBIT 2019, ISO 31000.
c) ISO/IEC 27032, ISO/IEC 27002, ISO 38500.
d) Todas las anteriores.
e) Ninguna de las anteriores.

23. ¿Cuáles son las 5 funciones simultáneas y continuas del Framework NIST?

a) Intensificar, Proteger, Detectar, Responder y Recuperar.
b) Identificar, Proteger, Detectar, Atacar y Recuperar.
c) Implementar, Proteger, Defender, Resistir y Resiliencia.
d) Identificar, Proteger, Detectar, Responder y Recuperar.
e) Ninguna de las anteriores.

24. ¿La diferencia entre Ciberseguridad y Seguridad de la Información es que la Seguridad de la Información trata información independiente de su formato y la Ciberseguridad se refiere a la protección de los activos digitales?

a) Falso.
b) Verdadero.

25. ¿Para la gestión de riesgos de Ciberseguridad qué metodología puedes usar como referencia?

a) ISO 31000.
b) ISO/IEC 27005.
c) Cobit for Risk.
d) Todas las anteriores.
e) Ninguna de las anteriores.

26. ¿Cuál se define como un tipo de programa malicioso que secuestra la información, restringiendo el acceso a la misma y solicitando el pago de un rescate a cambio de quitar esta restricción?

a) Cryptojacking.
b) Botnet.
c) Ransomware.
d) Shadow IT.
e) Spear Phishing.

27. ¿Cuál es el proceso que identifica las amenazas y peligros que existen para una organización?

a) Recuperación de desastres.
b) Continuidad del negocio.
c) Gestión de Riesgos de Ciberseguridad.
d) Seguridad de la información.
e) Ninguna de las anteriores.

28. ¿Cuál/es de las siguientes maneras es más efectiva para ayudar a mitigar la amenaza de la ingeniería social?

a) Comprar tecnologías de seguridad informática de última generación.
b) Hacer una campaña sobre Ingeniería social como parte de la Seguridad de la información.
c) Implementar un programa permanente de educación y concienciación sobre la Ciberseguridad.
d) Son válidas B y C.
e) Ninguna de las anteriores.

29. ¿La comprensión de sus roles y responsabilidades por parte del personal y los socios de la organización dentro del CSF del NIST se consideran en la categoría conciencia y capacitación?

a) Verdadero.
b) Falso.

30. ¿Qué se debería hacer para medir la eficacia del Programa de Ciberseguridad?

a) Definir indicadores usando la metodología SMART.
b) Comprar una herramienta automatizada.
c) Ninguna de las anteriores.
d) Todas las anteriores.

Respuestas

1.	B
2.	C
3.	B
4.	A
5.	B
6.	B
7.	A
8.	A
9.	B
10.	B
11.	A
12.	A
13.	C
14.	B
15.	C
16.	A
17.	C
18.	A
19.	C
20.	B
21.	C
22.	A
23.	D
24.	B
25.	D
26.	C
27.	C
28.	D
29.	A
30.	A