CISSP-Esp: Curso de Preparación

1 - Seguridad y gestión de riesgos – preguntas – parte 1

Conteste las siguientes Preguntas para discutir en clase.

1. ¿En qué consiste la triada de la CIA? De ejemplos de cada uno de sus componentes y como protegerlos.
2. Explique la relación entre la auditoria y la rendición de cuentas.
3. ¿Qué es el no repudio?
4. Explique en que consiste el concepto de “Postura de seguridad predeterminada”.
5. Explique el concepto de “Defensa en profundidad” mostrado en La figura 1-1.
6. Explique la triada de la CIA con respecto a los siguientes términos:
    a. Abstracción
    b. Ocultación de datos
    c. Cifrado
7. Enumere por lo menos 3 responsabilidades con respecto a los “Principios de gobernanza de la seguridad”.
8. Explique en que consiste la “Alineación de funciones de seguridad”.
9. ¿Qué es un caso de negocio y cuando debe usarse?
10. ¿Cuál es la diferencia entre el custodio y el propietario de datos?
11. ¿Cuál es la diferencia entre el propietario y el administrador de un sistema?
12. ¿Qué es un Marco de control de seguridad?
13. Explique en que consisten estos marcos de seguridad:
    a. Serie ISO / IEC 27000
    b. Marco de Zachman
    c. SABSA
    d. COBIT
    e. NIST 800
    f. Controles de seguridad críticos de CIS
    g. COSO
    h. CMMI
14. Explique la diferencia entre un enfoque de arriba hacia abajo y viceversa.
15. ¿Qué es el ciclo de vida de un programa de seguridad?
16. ¿Qué marco de referencia elegiría usted para su compañía y por qué?
17. ¿Por qué es importante la “Debida diligencia y el debido cuidado?
18. ¿Qué es el Cumplimiento y por qué es importante?
19. Explique los siguientes **Conceptos de delitos informáticos**.

- Crimen asistido por computadora
- Crimen dirigido por computadora
- Delito informático incidental
- Delito de prevalencia informática
- Hackers versus crackers

20. De algunos ejemplos de delitos informáticos.
21. ¿Por es importante que los profesionales de seguridad deben comprender los diferentes sistemas legales y los elementos que los componen?

Estos sistemas incluyen lo siguiente:

- Ley del código civil
- Ley común
- Derecho penal
- Derecho civil / extracontractual
- Derecho administrativo / regulatorio
- Derecho consuetudinario
- Ley religiosa
- Ley mixta

22. Haga una lista de por lo menos 6 componentes relacionado con la propiedad intelectual.
23. ¿En qué consiste el Flujo de datos transfronterizo?
24. ¿Qué es la privacidad en el contexto de ciberseguridad?
25. ¿En qué consiste el PII?
26. Haga una lista de categorías de PII basado en la Figura 1-10.
27. Explique en que consisten las siguientes leyes:
    a. HIPAA
    b. SOX
    c. GLBA
    d. CFAA de 1986
    e. FISMA
    f. Ley USA PATRIOT de 2001
    g. GDPR
28. ¿Cuáles son los 4 cánones obligatorios del código de ética del (ISC)2?
29. Haga una lista de los 6 principales documentos de seguridad y explique en que consiste cada uno.
30. Explique la diferencia entre BIA, BCP and DRP.
31. Las causas de los desastres se clasifican en tres áreas principales según su origen. ¿Cuáles son estas? Dé ejemplos.
32. ¿Qué es un plan de contingencia?

33. ¿Cuáles son los principales pasos de SP-800-34 Rev.1?
34. Dé ejemplos de los tipos de planes que dejen incluirse durante la planificación de contingencias según el NIST 800-34 Rev. 1
35. ¿Cuáles son los 4 pasos principales del BIA?
36. Haga una lista de los procesos críticos de su empresa.
37. Como parte de la determinación de la importancia de un activo, debe comprender los siguientes términos: MTD, MTTR, MTBF, RTO, WRT, y RPO
38. Explique los siguientes conceptos:
    a. Rotación de trabajo
    b. Separación de tareas
39. Cree una política de uso aceptable para su empresa usando las estampillas en el siguiente enlace. envíeme su política por email.

https://protegermipc.net/2020/02/05/plantillas-politicas-seguridad-de-la-informacion/

40. Revise los 18 controles recomendados por el CIS y compárelos con los de su empresa. Haga una lista de los puntos en que su empresa debe mejorar la postura de seguridad.

https://www.cisecurity.org/controls/cis-controls-list/

41. Solo me envía por email la #39 y 40. Las demás preguntas son para discutir y participar en clase.