**BLOQUE I: FUNDAMENTOS DE SEGURIDAD DE LA INFORMACIÓN**

1. Una definición muy aceptada de la Garantía de la información desde la Ingeniería de Sistemas hace un énfasis especial en el que sostiene que:

*Security Engineering is about building systems to remain \_\_\_\_\_\_ in the face of malice, error or mischance.*

Indica el término correspondiente:

1. Dependable
2. Practical
3. Available
4. Usable
5. Observa la siguiente definición de Garantía de la Información e indica el término más apropiado para completarla.

*Information Assurance is the practice of assuring information and managing \_\_\_\_ related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposses.*

Indica el término correspondiente:

1. Profits
2. Risks
3. Things
4. Goals
5. Desde una perspectiva generalista, agrupamos las medidas de seguridad en tres grandes bloques:
6. Defensa, confidencialidad e integridad
7. Defensa, disponibilidad y dependibilidad
8. Dependibilidad, seguridad y robustez
9. Defensa, disuasión y detección
10. La funciones de un sistema seguro trata con los riesgos del sistema mediante variadas funciones de seguridad que comprenden la evitación de riesgos, la disuasión, \_\_\_\_\_, \_\_\_\_, y la recuperación. Indica los dos términos que faltan por detallar.
11. Evaluación y preservación
12. Detección y evaluación
13. Análisis e información
14. Prevención y detección
15. Podemos traducir asset en español como: objeto valioso, objeto de valor y bien; en definitiva algo que debe ser protegido. Suponga que hablamos de una base de datos sobre pacientes. En este caso hablamos de personas cuyos perfiles están en un sistema de cómputo. ¿Es un asset del sistema el paciente en sí?
16. No, pues un sistema informático no puede tener como finalidad la de protección de personas
17. No, pues lo que forma parte del sistema es el historia, que si es un asset
18. No, el asset es la privacidad del historial del paciente, que es lo que queremos proteger
19. Si, pues en definitiva es el objeto que queremos proteger
20. Un programa que forma parte de la aplicación informática de un sistema…
21. También puede ser un asset, y ser necesaria su protección
22. No puede ser un asset, pues es e sistema en si mismo
23. Nunca es un asset pero puede que este esté hecho para proteger assets
24. Es un asset solo si no es necesario para llevar a cabo una misión del sistema
25. Una característica esencial que nos permite distinguir lo que es un asset del sistema de lo que no, es precisamente...
26. Que existe en cuanto es información o software, no hardware
27. Que su utilización requiere un intercambio de datos en red
28. Que cualquier alteración indebida sobre él induce un comportamiento erroneo en el sistema
29. Que su valor no es volátil, y perdura en el tiempo
30. Las amenazas son posibles sucesos que pueden hacer que nuestro sistema funcione mal, y existen a muchos niveles y en diversos modos que dependen de las malas intenciones de personas o colectivos, pero tambien de hechos completamente externos, por eso…
31. No podemos protegernos de absolutamente todas las amenazas posibles
32. Es preciso prever absolutamente todas las amenazas posibles y poner contramedidas
33. Es preciso calcular la probabilidad de absolutamente todas las amenazas posibles
34. Es preciso calcular el riesgo de todas las amenazas posibles
35. Las vulnerabilidades del sistema son, informalmente hablando, los puntos flacos del sistema que pueden ser atacado o vulnerados por la realización de alguna de las amenazas posibles en nuestro sistema. Por ello las vulnerabilidades en un programa...
36. No tienen por qué provenir necesariamente de errores en el diseño, programación…
37. Provienen necesariamente de amenazas imprevistas
38. Deben de ser siempre eliminadas
39. Provienen necesariamente de errores en el diseño, programación, etc
40. Imagine un sencillo sistema informático-ciclista, donde pueden pasar cosas tan inesperadas como (a) "caerse de la bici" o (b) "ser embestido por un peatón". Todos sabemos que nuestra noción de riesgo es formalmente la probabilidad de un suceso perjudicial para nuestro sistema (expresado porcentualmente, por ejemplo). En este caso, ¿qué le parece que es cada uno de estos dos sucesos?
41. (a) es un posible riesgo, y (b) una amenaza
42. (a) es una vulnerabilidad, y (b) un posible riesgo
43. (a) es una amenaza, y (b) una vulnerabilidad
44. Tanto (a) como (b) son posibles riesgos medibles
45. El principio llamado "of Easiest Penetration" no es, en el fondo, más que una extensión de la Ley de Murphy (Ley de la Tostada con Mantequilla) para el caso de un atacante malintencionado. Lo que está claro es que un sistema informático presenta siempre un punto más débil...
46. Que se convierte finalmente en el que representa el mayor riesgo
47. En comparación con el resto del sistema, aunque no tiene necesariamente que ser débil en términos absolutos
48. Que conviene debilitar especialmente para que no ataquen otros puntos más fuertes
49. Por eso hay que protegerlo para que deje de ser un punto débil
50. El concepto de ataque, siempre conlleva la característica de intencionalidad. En los términos más generales, su finalidad es...
51. Hacerse con información confidencial
52. Violar la política de seguridad del sistema
53. Hacerse con el control del sistema
54. Hacer entrar el sistema en un modo de error
55. Existen cuatro tipos de amenazas a los assets del sistema que provienen de vulnerabilidades del sistema, tal y como se han enunciado en el aula. Son fabricación, interceptación...
56. Interrupción y degradación
57. Modificación e interrupción
58. Denegación e interrupción
59. Integridad y confidencialidad
60. Los objetivos canónicos de la seguridad informática son (cuidado porque admitimos sinónimos)...
61. Confidencialidad, autenticación y dependencia
62. Continuidad, imparcialidad y disponibilidad
63. Disponibilidad, privacidad e integridad
64. Confidencialidad, autenticación y no repudio
65. La definición de integridad de la información es una cualidad que admite muchos sinónimos en función del contexto en que se aplique. Aun así, en general, entendemos que la información preserva su integridad...
66. Cuando puede modificarse, pero sólo a través de copias autorizadas por la política de seguridad
67. Cuando solo se modifica conforme a la política de seguridad del sistema
68. Cuando no se modifica
69. Cuando preserva la semántica original de la información contenida en el mensaje
70. Una pérdida de datos, se cataloga entre las amenazas posibles de un sistema como un ataque...
71. Por fabricación, de datos
72. Por modificación, de datos
73. Por interceptación, de software
74. Por interrupción, de datos
75. ¿Recuerdas el "Principio de Adecuación de la Protección"? Se enunció en dos partes; la primera reza así:

*Computer items must be protected only until they lose their value.*

y la segunda...

1. *They must be protected upto the maximum of their value.*
2. *They must be protected to a degree consistent with their value.*
3. *They must be available to consistently with their value.*
4. *They must be protected to a certain degree.*
5. Los errores de los sistemas producen efectos no deseados en el comportamiento del sistema que se pueden manifestar externamente como...
6. Faltas del sistema
7. Vulnerabilidades que conllevan fallos
8. Fallos en el servicio
9. Faltas activas
10. Todos los errores en los sistemas...
11. Pueden producir fallos en el servicio, pero también pueden no producirlos
12. Producen necesariamente faltas en el servicio
13. Producen necesariamente fallos en el servicio
14. Pueden producir faltas en el servicio, pero también pueden no producirlas
15. Decimos que un sistema está funcionando en modo degradado...
16. Como consecuencia de un fallo parcial
17. A raíz de una transición de falta durmiente a falta activa
18. A consecuencia de un error durmiente
19. Como consecuencia de una falta activa
20. A la medida de cómo es afectada la dependibilidad ( ) de A por la dependibilidad de B la denominamos...
21. Dependibilidad de A de B
22. Dependencia de A de B
23. Confianza del sistema A en el B
24. Confiabilidad de A de B
25. Los cinco atributos de la dependibilidad (*dependability*) más aceptados por los expertos son disponibilidad, confiabilidad...
26. Seguridad, manejabilidad e integridad
27. Continuidad, disponibilidad y confidencialidad
28. Confidencialidad, integridad y seguridad
29. Seguridad, mantenibilidad e integridad
30. A la propiedad de la dependibilidad (*dependability*) que consiste en la continuidad en el servicio correcto le atribuimos el nombre de...
31. Confiabilidad (reliability)
32. Infalibilidad (infalibility)
33. Continuidad (continuity)
34. Disponibilidad (availability)
35. Los tres atributos que caracterizan la "seguridad" de un sistema (en paralelo con la dependibilidad -dependability) son...
36. Confidencialidad, integridad y disponibilidad
37. Confidencialidad, fiabilidad y mantenibilidad
38. Confidencialidad, confiabilidad y mantenibilidad
39. Seguridad, confidencialidad y mantenibilidad
40. Las técnicas que nos permiten conseguir la dependibilidad (dependability), frente a fallos pueden agruparse en cuatro categorías principales. De las siguientes respuestas, una de ellas no pertenece a esta lista de categorías:
41. Predicción
42. Tolerancia
43. Diagnosis
44. Eliminación
45. Uno de los celebrados principios de seguridad enunciados en 1975 por Saltzer y Schoeder, es el de la mínima exposición (*minimum exposure*). Ya se ha comentado más de una vez, que estos principios presentan abundantes dependencias que convierten su consecución en un ejercicio de ingeniería complejo y no exento de decisiones críticas. Del resto de los principios mencionados, uno de ellos parece entrar en conflicto casi directo con el indicado, al menos en apariencia...
46. El de intermediar complemente los objetos
47. El de dar el menor privilegio posible
48. El de evitar los puntos de fallo únicos
49. El de apertura del diseño
50. El principio de Kerchoff reza...

*Un criptosistema basa toda su seguridad en la posesión de claves secretas.*

Al diseñar un sistema que obedece a este principio nos encuadramos en el fundamento de seguridad de...

1. Abrir el diseño
2. Exposición mínima
3. *Complete mediation*
4. Simplificación
5. Al aplicar el principio de diseño de sistemas seguros enunciado por Saltzer y Schoeder denominado "del menor privilegio posible", ayudamos a minimizar las consecuencias negativas de los errores, pero además...
6. minimizamos la ventana de oportunidad del adversario
7. reducimos las interfaces externas a la mínima expresión
8. reducimos los efectos negativos de los ataques desde el interior
9. podemos concentrar las medidas de seguridad en compartimentos específicos