Cuestionario Examen Final Seguridad

1. Cuál es el objetivo de la seguridad y el programa de seguridad
   Proteger a la organización y sus activos

2. Cuál es la Base de la Gestión de Seguridad
   - Identificar y Evaluar los activos de la empresa
   - Implementar políticas, procedimientos, estándares, directrices de integridad, confidencialidad y disponibilidad de los activos

3. Qué se debe determinar en el enfoque top-down a la seguridad
   Se debe determinar la funcionalidad y analizar el resultado final esperado.

4. Cuál es el rol de la oficina de seguridad
   Supervisar la mayoría de las facetas de un programa de seguridad

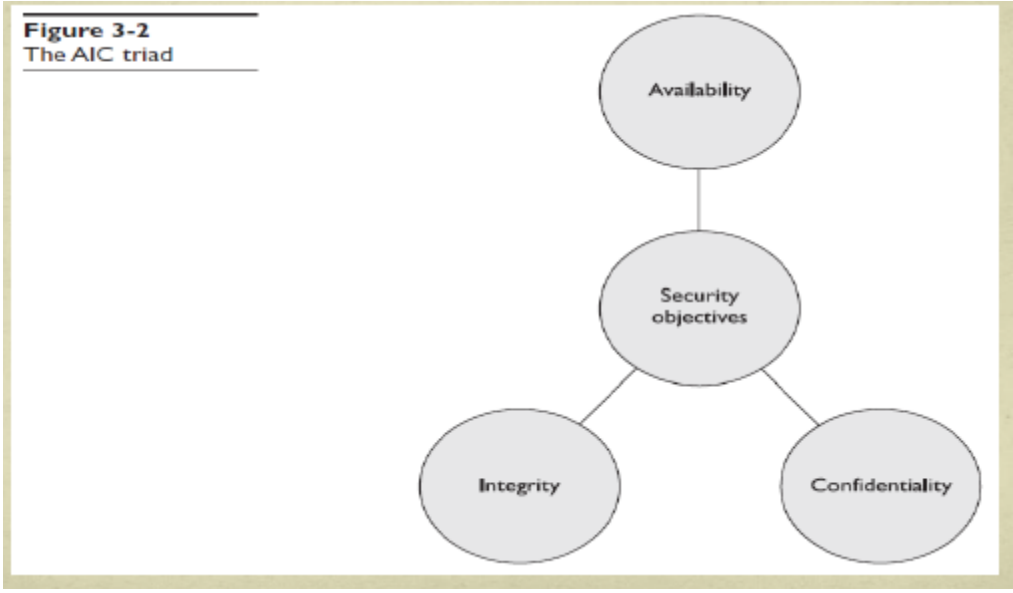
5. Cuáles son los controles que se deben utilizar para lograr las directivas de gestión de seguridad:
   - Controles administrativos
   - Controles técnicos
   - Controles físicos

6. Que incluyen los controles administrativos
   Incluyen desarrollar y publicar políticas, estándares, procedimientos y directrices, manejo de riesgo, selección de personal e implementar procedimientos de cambios de control.

7. Qué son los controles técnicos
   Consisten en implementar y mantener los mecanismos de control de acceso, contraseñas y manejo de recursos, métodos de identificación y autenticación, etc.

8. Qué son los controles físicos
   Conllevan el control de acceso individual a las instalaciones y los diferentes departamentos, sistemas de bloqueo y la eliminación de dispositivos innecesarios, protección del perímetro y control de intrusión.

9. Qué se quiere lograr con los controles de apoyo



10. Qué es un modelo de seguridad Organizacional
    Es una estructura formada por muchas entidades, mecanismos de protección, componentes lógicos, administrativos y físicos, procedimientos, procesos de negocio que trabajan en conjunto para proporcional un nivel de seguridad para un ambiente.

11. Cuáles son los tipos de metas
    - Metas operacionales: a corto plazo
    - Metas tácticas: a mediano plazo
    - Metas estratégicas: a largo plazo

12. Cuáles son los tipos de planes estratégicos
    - Plan estratégico de seguridad
    - Plan táctico
    - Plan operacional

13. Cuál es el plan estratégico de seguridad
    Es el que se alinea con los objetivos de negocio y los objetivos de tecnología.

14. Cuál es el plan táctico
    Se refiere a las iniciativas y otros soportes que deben de implementarse, para alcanzar los objetivos más amplios que han sido presentados por el plan estratégico.

15. Cuál es el plan operacional
    Es la planificación de ofertas con planes muy específicos, sus plazos y objetivos.

16. Métodos de reducción de riesgos
    - Instalar los controles de seguridad y componentes
    - Mejorar procedimientos

- Proporcionar métodos de detección temprana para enfrentar la amenaza.
- Elaborar plan de contingencia
- Llevar a cabo la sensibilización de formación

17. Cálculo de expectativa de perdida simple – SLE- cantidad de dólares asignada a un solo evento.

    Valor del activo * factor de exposición(EF)

    Factor de exposición = porcentaje de la perdida de una debilidad o amenaza realizada.

18. Qué es la tasa anual de ocurrencia (ARO)
    Valor que representa la frecuencia estimada de una amenaza específica, dentro de un periodo de un año

19. Que indica el valor ALE
    El monto que se propone implementar en los controles o salvaguardas, para proteger los activos ante la debilidad o amenaza.
    Formula: SLE * ARO

20. Que es el modo de falla y análisis de efectos (AMFE)
    Es un método para determinar las funciones de identificación de fallas funcionales, y la evaluación de las causas del fracaso, a través de un proceso estructurado.

21. Matriz de AMFE

Prepared by:							
Approved by:							
Date:							
Revision:							
				Failure Effect on . . .			
Item Identification	Function	Failure Mode	Failure Cause	Component or Functional Assembly	Next Higher Assembly	System	Failure Detection Method
IPS application content filter	Inline perimeter protection	Fails to close	Traffic overload	Single point of failure Denial of service	IPS blocks ingress traffic stream	IPS is brought down	Health check status sent to console and e-mail to security administrator
Central antivirus signature update engine	Push updated signatures to all servers and workstations	Fails to provide adequate, timely protection against malware	Central server goes down	Individual node's antivirus software is not updated	Network is infected with malware	Central server can be infected and/ or infect other systems	Heartbeat status check sent to central console, and page network administrator
Fire suppression water pipes	Suppress fire in building 1 in 5 zones	Fails to close	Water in pipes freezes	None	Building 1 has no suppression agent available	Fire suppression system pipes break	Suppression sensors tied directly into fire system central console
Etc.							

Table 3-3 How an FMEA Can Be Carried Out and Documented

22. Árbol de Fallas

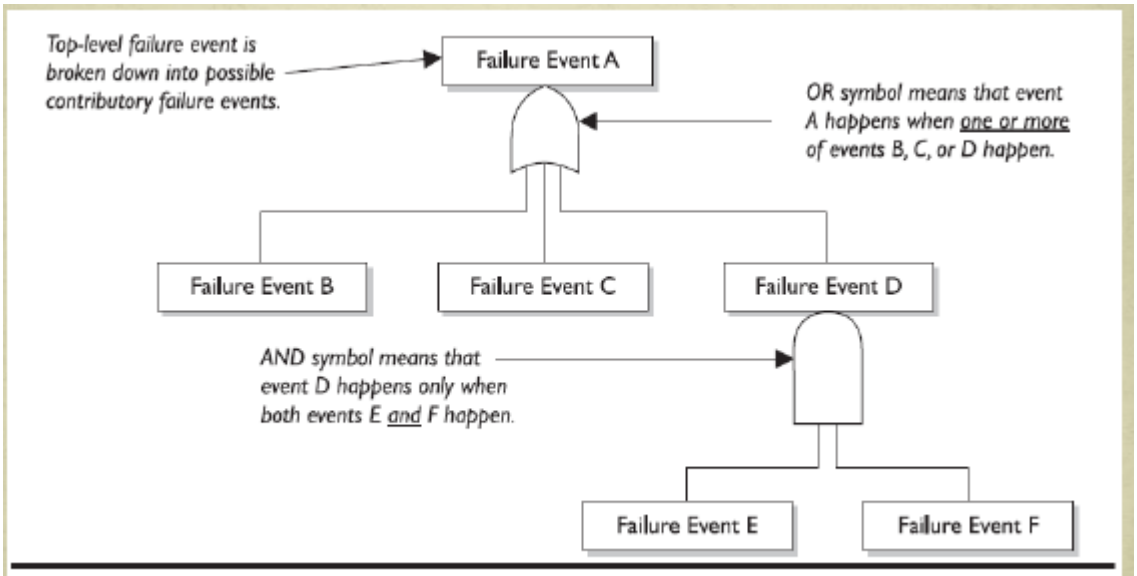


Figure 3-7 Fault tree and logic components

23. Que es la gobernanza
    Es el conjunto de responsabilidades y practicas ejercidas por la Junta y La Gerencia ejecutiva, con el objetivo de proporcionar una orientación estratégica asegurando que se alcancen los objetivos.

24. Esquema de Gobierno de TI

25. Que es Security Governance
    Es un sistema coherente de los componentes de seguridad integrados, que existen para asegurar que la organización sobreviva y prospere.

26. Que es un programa de seguridad
    Es la colección de los controles que una organización debe tener.

27. Cuáles son las áreas del Gobierno TI
    - Alineamiento estratégico
    - Entrega de valor
    - Gestión del Riesgo
    - Gestión de Recursos
    - Medición del Rendimiento

28. Que es el alineamiento estratégico
    Se centra en:
    - Asegurar la conexión e integración del negocio con los planes de TI
    - Definir, mantener y validar las propuestas de valor de TI
    - Alinear operaciones de TI con las de la empresa
    - Obtener mejor alineación que la competencia

29. Que es entrega de valor
    Se refiere a ejecutar las propuestas de valor durante el ciclo de entrega, asegurando que TI entrega los beneficios relacionados con la estrategia del negocio.

30. Que requiere la gestión del riesgo
    Requiere la concienciación por parte de la alta dirección y comprender la necesidad del cumplimiento con los requisitos.

31. Cuál es el objetivo del Gobierno de TI – ISO/38500
    Proporcionar un marco de principios para que las direcciones de las organizaciones los utilicen al evaluar, dirigir y monitorizar el uso de las TICS

32. Cuál es el alcance de la norma ISO 38500
    Se aplica al gobierno de los procesos de gestión de las TICs, en todo tipo de organizaciones que utilicen las TICs, facilitando las bases para la evaluación objetiva del gobierno de TICs.

33. Cuáles son los beneficios de un buen gobierno de TI
    En cuanto a la conformidad de la organización con:
    - Los estándares de seguridad
    - Legislación de privacidad
    - Legislación sobre SPAM y otras modalidades
    - Derechos de propiedad intelectual
    - Regulación ambiental

34. Aspectos de la búsqueda del buen rendimiento de las TICs

- Apropiada implementación y operación de los activos de TI
- Clarificación de responsabilidades y rendición de cuentas
- Alineamiento de las TICs con las necesidades del negocio
- Innovación de servicios
- Reducción de costos

35. Que es Gobierno corporativo de TI (norma ISO/38500)
    Sistema mediante el cual se dirige y controla el uso actual y futuro de las TI

36. Que es gestión (norma ISO/38500)
    Sistema de controles y procesos requeridos para lograr los objetivos estratégicos, establecidos por la dirección de la organización.

37. Que es un stakeholder (norma ISO/38500)
    Individuo, grupo u organización que puede afectar, ser afectado o percibir que va a ser afectado, por una decisión o una actividad.

38. Qué es uso de TI
    Planificación, diseño, desarrollo, despliegue, operación, gestión y aplicación de la TI para cumplir con las necesidades del negocio

39. Que es conducta humana
    Comprensión de las interacciones entre personas y otros elementos de un sistema con la intención de asegurar el bienestar de las personas y el buen rendimiento del sistema.

40. Cuáles son los principios de un buen gobierno corporativo de TI según la norma ISO/38500
    - Responsabilidad
    - Estrategia
    - Adquisición
    - Rendimiento
    - Conformidad
    - Conducta humana

41. A que se refiere Responsabilidad
    Todo el mundo debe comprender y aceptar sus responsabilidades en la oferta o demanda de TI.

42. Qué es estrategia
    Tiene en cuenta las capacidades actuales y futuras de las TI.

43. Porque se hacen las Adquisiciones
    Se realizan por razones válidas, basándose en un análisis apropiado y continuo, con decisiones claras y transparentes.

44. A que se refiere Rendimiento
    La TI esta dimensionada para dar soporte a la organización, proporcionando los servicios con la calidad adecuada, para cumplir con las necesidades actuales y futuras.

45. A qué se refiere la conformidad
    A que la función de TI cumple todas las legislaciones y normas aplicables.

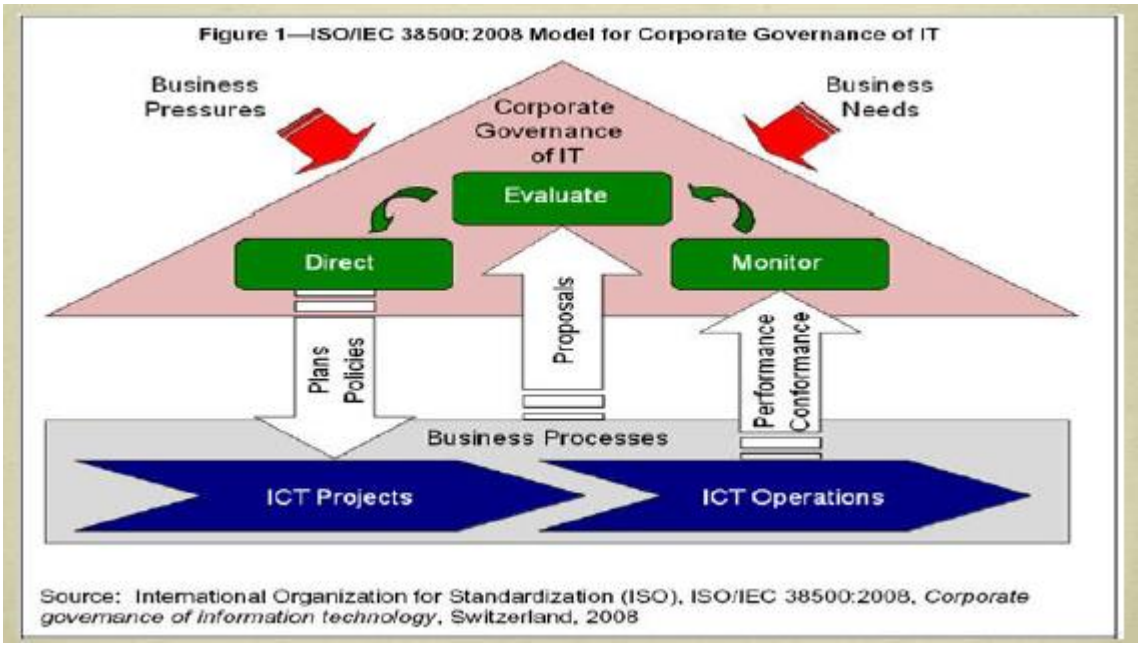
46. Cuáles son las tareas principales que debe tomar en cuenta la dirección al gobernar la TI
    - Evaluar
    - Dirigir
    - Monitorizar

47. Qué es evaluar
    Examinar y juzgar el uso actual y futuro de las TI, incluyendo estrategias, propuestas y acuerdos de aprovisionamiento.

48. Qué es dirigir
    Asegurar la transición correcta de los proyectos a la producción, considerando los impactos en la operación, el negocio y la infraestructura.

49. Que es monitorizar
    Vigilar el rendimiento de la TI, mediante sistemas de medición.

50. Modelo para el gobierno de la TI



51. Qué es delito informático
    Operaciones ilícitas realizadas por medio de internet o que tienen como objetivo destruir y dañar ordenadores, medios electrónicos y redes de internet

52. Actividades delictivas
    - Ingreso ilegal a sistemas
    - Intercepción ilegal de redes
    - Daños en la información
    - Ataques a sistemas
    - Violación de los derechos de autor
    - Pornografía infantil

53. Cuáles son los grupos en que se dividen los delitos informáticos.
    - Crímenes que tienen como objetivo las redes de computadoras
    - Crimines realizados por medio de ordenadores y de internet.

54. Crímenes específicos
    - Spam: correos electrónicos no solicitados para propósito comercial
    - Fraude: Inducir a otro a hacer o a restringirse en hacer alguna cosa, de lo cual el criminal obtendrá un beneficio.
    - Contenido obsceno u ofensivo
    - Hostigamiento/Acoso: contenido que se dirige de manera específica a un individuo o grupo, con comentarios derogativos.
    - Tráfico de drogas
    - Terrorismo virtual

55. Qué son regulaciones legales
    Análisis de la situación de la legislación local, regional, convenciones adoptadas por el país.

56. Qué es un hacker
    Es una persona que descubre las debilidades de una computadora o de una red informática.

57. Cuáles son las clasificaciones de un hacker
    - De sombrero blanco
    - de sombrero gris
    - de sombrero negro
    - de elite
    - de sombrero azul
    - hacktivista
    - estado de la nación

58. Que es un hacker de sombrero blanco
    Rompe la seguridad por razones no maliciosas, para poner a prueba la seguridad de su propio sistema.

59. Qué es un hacker de sombrero negro
    Es un hacker que viola la seguridad informática por razones más allá de la malicia o para beneficio personal
60. Qué es un hacker de sombrero gris
    Es una combinación de un hacker de sombrero negro con uno de sombrero blanco. Él puede navegar por la internet y hackear un sistema con el propósito de notificar al administrador que su sistema ha sido hackeado.

61. Qué es un hacker de elite
    Hackers expertos

62. Qué es un hacker de sombrero azul
    Es una persona fuera de las empresas de consultoría informática de seguridad, que es utilizado para hacer una prueba de errores de un sistema antes de su lanzamiento, en busca de exploits para que puedan se cerrados.

63. Qué es un hacktivista
    Es un hacker que utiliza la tecnología para anunciar un mensaje social, ideológico, religioso o político.

64. Qué es estado de la nación
    Se refiere a los servicios de inteligencia y a los operativos de guerra informática.

65. Que es Certified Ethical Hacker
    Es una certificación profesional promovida por el Consorcio Internacional de Consultas de Comercio electrónico.

66. Que es el análisis forense informático
    Es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica, que permiten identificar, preservar, analizar y presentar datos, que sean válidos dentro de un proceso legal.

67. A qué ayuda la informática forense
    A detectar pistas sobre ataques informáticos, robo de información, conversaciones o pistas de emails y chats.

68. Qué es cadena de custodia
    La identidad de personas que manejan la evidencia en el tiempo del suceso y la última revisión del caso.

69. Qué es imagen forense
    Es una copia bit a bit de un medio electrónico de almacenamiento.

70. Qué es el análisis de archivo
    Examinar cada archivo digital descubierto y crear una base de datos de información relacionada al archivo.

71. Cuáles son las áreas de gestión del análisis forense informático
    - Manejo de incidentes de seguridad
    - Marco normativo para la gestión de incidentes de seguridad
    - Metodologías de análisis forense informático
    - Experiencias concretas de la gestión de incidentes de seguridad
    - Evidencia digital.

72. Qué es ingeniería social
    Es la práctica de obtener información confidencial, a través de la manipulación de usuarios legítimos.

73. Cuál es el principio por el cual se sustenta la Ingeniería Social
    En cualquier sistema los usuarios son el eslabón débil.

74. Cuál es la principal defensa contra la ingeniería social
    Educar, capacitar y entrenar a los usuarios en el uso de políticas de seguridad y asegurarse de que estas sean seguidas

75. Cuáles son los principios de la ingeniería social según Kevin Mitnick
    - Todos queremos ayudar
    - El primer movimiento es siempre de confianza hacia el otro
    - No nos gusta decir No,
    - A todos nos gusta que nos alaben

76. Qué es criptología
    Es la disciplina científica que se dedica al estudio de la escritura secreta, estudia mensajes que, procesados de cierta manera, se convierten en difíciles o imposibles de descifrar.

77. Cuál es el objetivo de la criptología
    Estudiar técnicas que se encarguen de proporcionar seguridad a la información.

78. Qué disciplinas comprende la criptología
    - Criptografía
    - Criptoanálisis
    - Esteganografía
    - Estegoanálisis

79. Que es criptografía
    Se ocupa del estudio de los algoritmos, protocolos y sistemas, que se utilizan para proteger la información y dotar de seguridad a las comunicaciones y a las entidades que se comunican.

80. Qué es criptoanálisis
    Su objetivo es buscar el punto débil de las técnicas criptográficas para explotarla y eliminar la seguridad que teóricamente aportaba la técnica criptográfica.

81. Qué es esteganografía
    Se ocupa de ocultar mensajes con información privada por un canal inseguro, de forma que el mensaje no sea ni siquiera percibido.

82. Que es Estegoanálisis
    Se ocupa de detectar mensajes ocultos con técnicas esteganográficas.

83. Que es esquema esteganográfico
    Es el conjunto de componentes que permite llevar a cabo la comunicación esteganográfica.

84. Qué es el portador
    Es todo aquel conjunto de datos que es susceptible de ser alterado, para incorporarle el mensaje que queremos mantener en secreto.

85. Qué es mensaje legitimo
    Mensaje transportado por el portador

86. Que es mensaje esteganográfico
    Mensaje que se quiere mantener en secreto y esconder dentro del portador.

87. Qué es estego-algoritmo
    Es el algoritmo esteganográfico que indica cómo realizar el procedimiento de incorporación del mensaje que queremos mantener en secreto en el portador.

88. Qué es embeber
    Acción de ocultar el mensaje dentro del portador.

89. Que es estego-mensaje
    Resultado de embeber el mensaje esteganográfico dentro del portador.

90. Qué es extraer
    Acción de la recuperación, a partir del estego-mensaje, del mensaje oculto esteganográfico.

91. Que es estegoanalista
    Persona que intenta determinar la existencia o ausencia de un mensaje esteganográfico.

92. Qué son los canales de selección.
    Son canales adicionales al portador utilizado para embeber, donde se comunica qué posiciones del portador se utilizan para la comunicación esteganográfica.

93. Qué son clases de equivalencia
    Corresponden a pares de elementos del portador utilizado, que tiene una interpretación semántica equivalente en la comunicación legitima, pero el uso de un elemento tiene un significado acordado en la comunicación esteganográfica.

94. Cuáles son los tipos de esteganografía según el estego-algoritmo
    Esteganografía pura y esteganografía de clave secreta.

95. Qué es esteganografía pura
    En este tipo el estego-algoritmo establece un método fijo para incorporar el mensaje esteganográfico en el portador para obtener el estego-mensaje.

96. Qué es esteganografía de clave secreta.
    En este tipo el estego-algoritmo está parametrizado por una clave esteganográfica, a la que se le llama estego-clave que define como aplicar el algoritmo.