ISO 27001 Internal Auditor (I27001IA)

Preguntas de Apoyo V112023

1. En cuál de sus cláusulas la ISO 27001:2022 pide considerar:

a. Las partes interesadas que son relevantes para el sistema de gestión de la seguridad de la información
b. Los requisitos de estas partes interesadas que son relevantes para la seguridad de la información.
c. Cuáles de estos requisitos se abordarán a través del Sistema de Gestión de Seguridad de la Información.

2. La norma ISO 27001:2022 establece que cuando la organización determine la necesidad de cambios en el SGSI, los cambios se llevarán a cabo de manera planificada en su cláusula:

a) Cláusula 6.3
b) Cláusula 10.2
c) Cláusula 4.2

3. El anexo A de la ISO 27001:2022 define 4 categorías (organizacionales, de personas, físicos y tecnológicos) para agrupar los 93 controles de seguridad de la información.

a) Cierto
b) Falso

4. Una vez realizada la auditoría, el auditor encargado de realizarla debe hacer el Informe de Auditoría. En dicho Informe se establecen:

    a. Objetivos de la auditoría
    b. Alcance de la auditoría.
    c. Auditados y el período de la auditoría.
    d. Documentación de la persona de contacto.
    e. Documentación del auditor líder y otros auditores.
    f. Fechas y ubicaciones donde se desarrollaron las actividades de la auditoría.
    g. Criterio de auditoría.
    h. Declaraciones de auditoría.
    i. Conclusiones de la auditoría.

a) Todas son correctas.
b) Todas excepto d y e.
c) Sólo i

5. Los objetivos de la auditoría definen qué se va a lograr con la auditoría individual

a) Verdadero.
b) Falso.

6. La Declaración de Aplicabilidad (SoA) debe contener:

    a. Los controles necesarios para implementar la(s) opción(es) elegida(s) de tratamiento de riesgos de seguridad de la información.
    b. La justificación de las inclusiones.
    c. Si los controles necesarios están implementados o no
    d. La justificación de las exclusiones de cualquiera de los controles del anexo A

a) Todas son correctas.
b) Todas excepto b y c.
c) Sólo a

7. Durante la reunión de cierre el auditor líder debe explicar, por ejemplo, cualquier actividad posterior a la auditoría relacionada (por ejemplo, implementación y revisión de acciones correctivas, tratamiento de quejas de auditoría, proceso de apelación).

a) Cierto.
b) Falso.

8. Con respecto a la información documentada, la norma ISO 27001:2022 indica puede incluir:

a) La información documentada de origen externo, determinada por la organización como necesaria para la planificación y operación del sistema de gestión de seguridad de la información.
b) La información documentada requerida por el sistema de gestión de la seguridad de la información y por esta norma internacional.
c) La información documentada que la organización ha determinado que es necesaria para la efectividad del sistema de gestión de la seguridad de la información
d) Todas las anteriores.

9. El plan de auditoría se refiere a:

a) Conjunto de una o más auditorías planificadas para un periodo de tiempo determinado y dirigidas hacia un propósito específico.
b) Descripción de las actividades y los arreglos para una auditoría.

10. La ISO 19011:2018 determina a las no conformidades y a las oportunidades de mejora como incumplimientos a requisitos de la norma auditada.

a) Cierto.
b) Falso.

11. Es el mejor momento para dar a conocer las condiciones bajo las cuales puede darse por terminada la auditoría.

a) Al inicio de una auditoría individual.
b) En la reunión de apertura.
c) Durante la definición del alcance de la auditoría.

12. La ISO 17011:2018 establece que los auditores deberían tener conocimiento y habilidades como:

a) Comprender los tipos de riesgos y oportunidades asociados con la auditoría.
b) Planificar y organizar el trabajo de manera efectiva.
c) Realizar la auditoría dentro del cronograma acordado.
d) Tomarse demasiado tiempo para redactar correctamente sus notas.
e) Priorizar y enfocarse en asuntos importantes.
f) Empoderarse en la auditoría para tratar de obtener la mayor cantidad de evidencias.
g) Comunicarse de manera efectiva, oralmente y por escrito (ya sea personalmente o mediante el uso de intérpretes).
h) Recopilar información mediante entrevistas efectivas, escuchar, observar y revisar información documentada, incluidos registros y datos.
i) Todas las anteriores son habilidades que debe desarrollar un auditor
j) Todas excepto D y F.

13. Durante una entrevista lo mejor es hacer preguntas inductivas (preguntas cuya respuesta sea SÍ o NO) las preguntas abiertas podrían generar confusión al auditado.

a) Cierto
b) Falso

14. Las preguntas: ¿quién?, ¿cómo?, ¿por qué?, ¿cuándo?, ¿dónde?; son:

a) Preguntas Abiertas.
b) Preguntas cerradas.

15. Las listas de verificación utilizadas por los auditores:

a) Aseguran que nada importante se pase por alto.
b) Ayudan a proporcionar información sobre cualquier actividad posterior a la auditoría relacionada (por ejemplo, implementación y revisión de acciones correctivas, tratamiento de quejas de auditoría, proceso de apelación).
c) Ayudan a brindar continuidad a la auditoría.
d) Ayudan a proporcionar información sobre posibles consecuencias de no abordar adecuadamente los hallazgos de la auditoría.
e) (E): Todas las anteriores.
f) (F): Todas excepto B y D.
g) (G): Solo B y D.

16. Tienen la responsabilidad de nombrar a los miembros del equipo de auditoría, incluyendo el líder del equipo y cualquier expertos técnicos necesarios para la auditoría específica.

a) El CISO.
b) El(los) individuo(s) que gestiona(n) el programa de auditoría.
c) El Auditor Líder.
d) El responsable de la dirección.

17. Es un conjunto de una o más auditorías planificadas para un periodo de tiempo determinado y dirigidas hacia un propósito específico.

a) Programa de auditoría.
b) Plan de auditoría.
c) Las listas de verificación.
d) El alcance de la auditoría.

18. Son tipos de auditoria:

a) Primera parte.
b) Segunda parte.
c) Tercera parte.
d) Todas las anteriores
e) Las auditorías sólo se clasifican en internas o externas.

19. Auditoría realizada por o en nombre de la organización misma, es decir con sus mismos recursos.

a) Primera parte.
b) Segunda parte.
c) Tercera parte.

20. La evidencia objetiva:

a) Son los datos que respaldan la existencia o la verdad de algo.
b) Se puede obtener a través de observación, medición, prueba o por otros medios.
c) Es un método de auditoría para llegar a conclusiones fiables.
d) Todas las anteriores
e) Solo A y B
f) Solo A y C

21. Los resultados de la auditoría:

a) Son los resultados de la evaluación de la evidencia de auditoría recopilada contra los criterios de auditoría.
b) Son considerados hallazgos y pueden ser clasificados en conformidad o no conformidad.
c) Es un método de auditoría para llegar a conclusiones fiables.
d) Si los criterios de auditoría se seleccionan de entre los requisitos legales o los requisitos reglamentarios, el hallazgo de la auditoría se denomina cumplimiento o incumplimiento.
e) Sólo B y C
f) Solo A y C
g) Todas las anteriores

22. Establece que la organización debe definir un proceso de evaluación de riesgos:

a) Cláusula 6.1.1
b) Cláusula 6.1.2
c) Cláusula 8.1
d) B y C Son válidas

23. Establece que la organización debe implementar el proceso de tratamiento de riesgos:

a) Cláusula 6.1.2
b) Cláusula 6.1.3
c) Cláusula 8.3
d) B y C Son válidas

24. Son estrategias de gestión de riesgos excepto:

a) Mitigar
b) transferir
c) Asumir
d) Retener
e) Controlar

25. Tipo de estrategia donde se define la implementación de un control para reducir el nivel del riesgo:

a) Mitigar
b) transferir
c) Asumir
d) Retener

26. La Declaración de Aplicabilidad" debe contener:

a) Los controles necesarios para reducir el nivel del riesgo
b) La justificación de las inclusiones de los controles considerados como necesarios.
c) Si los controles necesarios están implementados o no
d) La justificación de las exclusiones de cualquiera de los controles del anexo A
e) Todas son válidas
f) (C) Solo B y D

27. Según la ISO 17011:2018 la auditoría se define como un proceso sistemático, independiente, documentado, para obtener evidencia y evaluarla objetivamente, con el fin de determinar en qué grado se cumplen los criterios de la auditoría.

a) Cierto
b) Falso

28. La ISO 19011:2018 establece como métodos para evaluar a los auditores:

a) Observación
b) Examen
c) Entrevista
d) Llamada telefónica
e) Todas son válidas
f) Todas excepto D

29. Durante la auditoría se desea un comportamiento profesional por el auditor, por ejemplo, se espera que sea de mente abierta es decir dispuesto a considerar ideas o puntos de vista alternativos.

a) Cierto
b) Falso

30. Definir objetivos, alcance y criterios para cada auditoría individual, Seleccionar métodos de auditoría y Definir e implementar los controles operativos necesarios para la supervisión del programa de auditoría, forman parte de las actividades para:

a) Definir el alcance del SGSI.
b) Crear correctamente la política del SGSI.
c) Definir el programa de auditoría.

31. Es responsable de asignar responsabilidades al equipo auditor:

a) El auditor Líder.
b) El responsable del sistema de gestión.
c) La alta dirección
d) La(s) persona(s) que gestiona(n) el programa de auditoría.

32. Deben garantizar que se realicen las siguientes actividades como parte de la gestión de los resultados del programa de auditoría:

1. Evaluación del logro de los objetivos para cada auditoría dentro del programa de auditoría
2. Revisión y aprobación de informes de auditoría sobre el cumplimiento del alcance y los objetivos de la auditoría
3. Revisión de la efectividad de las acciones tomadas para abordar los hallazgos de auditoría
4. Distribución de informes de auditoría a las partes interesadas pertinentes
5. Determinación de la necesidad de cualquier auditoría de seguimiento

a) Los miembros del equipo auditor.
b) Todos en la organización.
c) La(s) persona(s) que gestiona(n) el programa de auditoría.

33. El plan de auditoría describe:

a) Las actividades y arreglos para cada auditoría planificada
b) Una planificación en un periodo de tiempo determinado de una o más auditorías.
c) Ambas son válidas ya que existe una relación entre el programa y el plan de auditorías.

34. El programa de auditoría describe:

a) Las actividades y arreglos para cada auditoría planificada
b) Una planificación en un periodo de tiempo determinado de una o más auditorías.
c) Ambas son válidas ya que existe una relación entre el programa y el plan de auditorías.

35. Durante una auditoría se recomienda hacer preguntas cerradas, preguntas cuya respuesta sea SÍ o NO esto permite que la auditoría sea más precisa.

a) Cierto
b) Falso

36. Durante una auditoría el auditado suministra poca información y constantemente reformula las preguntas del auditor, estas son:

a) Consideradas situaciones difíciles que el auditor debe ser capaz de manejar.
b) Temas que el auditor líder debe resolver.
c) Condiciones para dar por terminada la auditoría.

37. Un hallazgo indica:

a) Conformidad o no conformidad.
b) Cumplimiento o Incumplimiento.
c) Ambas son válidas.

38. Una oportunidad de mejora no es considerada una no conformidad, pero pueden ser revisadas por la organización, cuando lo estime conveniente para mejorar la eficacia del proceso.

a) Cierto
b) Falso

39. Seleccionan y Determinan los métodos para llevar a cabo las auditoría dependiendo de los objetivos de auditoría definidos, el alcance y criterios definidos.

a) El equipo auditor.
b) El auditor líder
c) La alta dirección
d) La(s) persona(s) que gestiona(n) el programa de auditoría.

40. Son métodos para ejecutar las auditorías

1. En sitio.
2. Remotas.
3. Con interacción humana
4. Sin interacción humana.

a) Solo 1 y 2
b) Todas excepto 4
c) Solo 3 y 4
d) Todas

41. El líder del equipo auditor, consultando con el equipo auditor, asigna a cada miembro del equipo responsabilidad para:

1. Auditar procesos.
2. Actividades.
3. Funciones.
4. Desarrollar el programa de auditoría.

a) Solo 1 y 2
b) Todas excepto 4
c) Solo 3 y 4
d) Todas

Respuestas

1. C
2. A
3. A
4. A
5. A
6. A
7. A
8. D
9. B
10. B
11. B
12. J
13. B
14. A
15. F
16. B
17. A
18. D
19. A
20. E
21. G
22. B
23. C
24. E
25. A
26. E
27. A
28. F
29. A
30. C
31. A
32. C
33. A
34. B
35. B
36. A
37. D
38. A
39. E
40. D
41. B