ISO 22301 Internal Auditor/Lead Auditor (I22301IA/LA)

Preguntas de Apoyo V092020

1. La organización debe asegurar que solo los requisitos legales y reglamentarios se tienen en cuenta al establecer, implantar y mantener su SGCN.

a) Verdadero.

b) Falso.

2. La organización debe establecer, implantar y mantener un único procedimiento que permita la comunicación interna y la comunicación externa en el SGCN.

a) Verdadero.

b) Falso.

3. La información documentada requerida por el SGCN y por la norma ISO 22301, se debe controlar para asegurar que está protegida adecuadamente (por ejemplo, contra la pérdida de confidencialidad, uso incorrecto, o pérdida de su integridad).

a) Verdadero.

b) Falso.

4. En el alcance de los requisitos de la norma la información documentada de origen externo no debe ser considerada por la organización como necesaria para la planificación y operación del SGCN.

a) Verdadero.

b) Falso.

5. La organización debe establecer, implantar y mantener un proceso formal y documentado de análisis de impacto en el negocio y de apreciación del riesgo.

a) Verdadero.

b) Falso.

6. La estrategia de continuidad del negocio se refiere a que la organización debe establecer, implantar y mantener un proceso de evaluación formal y documentado para determinar las prioridades de recuperación y de continuidad.

   a) Verdadero.

   b) Falso.

7. Apreciación del riesgo se refiere en la norma a que la organización debe establecer, implantar y mantener un proceso formal y documentado de apreciación del riesgo que identifique, analice, y evalúe sistemáticamente el riesgo de incidentes disruptivos para la organización.

   a) Verdadero.

   b) Falso.

8. La organización podría determinar una estrategia apropiada de continuidad del negocio para la mitigación, la respuesta y la gestión de los impactos solo si está definido en el alcance del SGCN.

   a) Verdadero.

   b) Falso.

9. Para implantar las estrategias seleccionadas en el SGCN la organización debe determinar los requisitos relativos a los recursos. Los tipos de recursos considerados deben incluir personas, informaciones y datos, edificios entre otros.

   a) Verdadero.

   b) Falso.

10. La organización debe considerar medidas reactivas que reduzcan la probabilidad y periodo de interrupción durante la invocación del plan del SGCN.

    a) Verdadero.

    b) Falso.

11. La organización debe documentar procedimientos para establecer un protocolo de comunicaciones internas y externas.

a) Verdadero.

b) Falso.

12. Entre los requisitos de la norma se requiere que la organización debe establecer, documentar, e implantar procedimientos y una estructura de gestión para responder a incidentes disruptivos.

a) Verdadero.

b) Falso.

13. Se debe documentar la decisión de si se realiza o no comunicación externa sobre sus riesgos e impactos significativos considerando la seguridad de las personas como prioridad principal.

a) Verdadero.

b) Falso.

14. La organización debe establecer, implantar y mantener procedimientos para detectar un incidente de seguridad y garantizar la confiabilidad de los sistemas de comunicación durante un incidente así este no sea disruptivo.

a) Verdadero.

b) Falso.

15. De acuerdo a la norma 22301, los procedimientos de comunicación y de aviso se deben probar al menos dos veces durante un periodo de auditoría interna.

a) Verdadero.

b) Falso.

16. La organización puede utilizar los procesos del SGCN, tales como el de liderazgo, para conseguir la mejora.

a) Verdadero.

b) Falso.

17. De acuerdo con los criterios de seguridad de la información la norma deja a decisión del representante de la dirección si se conservan documentos como prueba de las no conformidades y de las acciones tomadas frente a las acciones correctivas.

a) Verdadero.

b) Falso.

18. Cuando se produzca una no conformidad, la organización podría tomar acción para controlarla y corregirla solo si se encuentra bajo el presupuesto aprobado.

a) Verdadero.

b) Falso.

19. Si se tiene implementada la norma ISO 27001 la organización que implemente la norma ISO 22301 está exenta de conservar la información de los resultados de las revisiones de la dirección debido a que esta se hace en el alcance de la ISO 27001.

a) Verdadero.

b) Falso.

20. La alta dirección debe revisar el SGCN de la organización cada seis meses para asegurarse que continúa siendo idóneo, adecuado y eficaz.

a) Verdadero.

b) Falso.

21. La organización debe planificar, establecer, implantar y mantener programa(s) de auditoría, que incluya(n) la frecuencia, los métodos, las responsabilidades, la planificación de requisitos y la realización de informes.

a) Verdadero.

b) Falso.

22. Por la naturaleza de la norma ISO 22301, es la única norma que permite que un auditor audite su propio trabajo por el grado de conocimiento que tiene del negocio y su continuidad necesaria.

a) Verdadero.

b) Falso.

23. El programa de auditoría, incluyendo su calendario se debe basar únicamente en los resultados de las apreciaciones de riesgo de las actividades de la organización.

a) Verdadero.

b) Falso.

24. El responsable de la gestión del área que se esté auditando debe garantizar que se realizan todas las correcciones y acciones correctoras necesarias.

a) Verdadero.

b) Falso.

25. En lo que se refiere a las auditorías internas la organización debe realizarlas sin previo aviso y sorpresivamente para obtener información de si se cumple el sistema de gestión de la continuidad del negocio en cualquier momento.

a) Verdadero.

b) Falso.

26. Las evaluaciones de los procedimientos de continuidad del negocio se deben realizar por medio de revisiones periódicas, pruebas, ensayos, informes posteriores a los incidentes y evaluaciones del rendimiento.

a) Verdadero.

b) Falso.

27. La organización debe someter a pruebas y ensayos sus procedimientos de continuidad del negocio para garantizar que son coherentes con sus objetivos de continuidad del negocio.

a) Verdadero.

b) Falso.

28. Se debe definir un portavoz apropiado que brinde los detalles de la respuesta de la organización a los medios de comunicación después de un incidente.

a) Verdadero.

b) Falso.

29. La organización debe establecer procedimientos documentados para responder a un incidente disruptivo y proseguir o restablecer sus actividades en un periodo de tiempo definido dentro de la invocación.

a) Verdadero.

b) Falso.

30. La estrategia de continuidad debe incluir la aprobación de los plazos de tiempo prioritarios para la reanudación de las actividades.

a) Verdadero.

b) Falso.

31. De acuerdo con la norma ISO 22301, la organización debe evaluar los riesgos relacionados con interrupciones que requieren tratamiento y los que no requieren tratamiento por estar fuera de la asignación de recursos financieros.

a) Verdadero.

b) Falso.

32. Por sus siglas en inglés (BIA), el análisis de impacto en el negocio debe la identificación de las actividades que apoyan el abastecimiento de productos y servicios.

a) Verdadero.

b) Falso.

33. Durante el análisis de riesgos y su mitigación se deben establecer los plazos para la reanudación de las actividades de impacto a los sistemas de información a un nivel mínimo especificado dentro de los acuerdos de nivel de servicio (SLAs).

a) Verdadero.

b) Falso.

34. La amplitud de la información documentada de un SGCN puede variar de una organización a otra, debido a la competencia de las personas.

a) Verdadero.

b) Falso.

35. La política de continuidad del negocio debe ser comunicada y entendida al grupo de interés dentro de la organización y por seguridad no divulgada a quienes no estén en el alcance del SGCN.

a) Verdadero.

b) Falso.

36. La organización debe garantizar que estas personas involucradas en el SGCN son competentes sobre la base de una formación inicial, una formación profesional y una experiencia apropiada.

a) Verdadero.

b) Falso.

37. La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, la implantación, el mantenimiento y la mejora continua del SGCN.

a) Verdadero.

b) Falso.

38. La alta dirección debe asegurar que los objetivos de continuidad del negocio se establecen y se comunican a las funciones y niveles aplicables dentro de la organización.

a) Verdadero.

b) Falso.

39. El director de Tecnología de la Información o CIO por sus siglas en inglés (Chief information officer) debe asignar la responsabilidad y la autoridad para garantizar que el sistema de gestión es conforme con los requisitos de la ISO 22301 e informar sobre el rendimiento del SGCN.

a) Verdadero.

b) Falso.

40. La alta dirección debe garantizar que las responsabilidades y la autoridad para las funciones principales se asignan y se comunican dentro de la organización participando siempre en las pruebas y los ensayos del SGCN.

a) Verdadero.

b) Falso.

RESPUESTAS

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