ISO 27001 Foundation (I27001F)

Preguntas de Apoyo V092020

1. La aprobación del plan de tratamiento de riesgos y la aceptación del riesgo residual es la responsabilidad de: (Selecciona la mejor respuesta)

a) Alta dirección.
b) Dueño del riesgo.
c) Director de Información.
d) Director de Seguridad.

2. ¿Cuál de los siguientes no es un requerimiento de ISO/IEC 27001? (Selecciona la mejor respuesta)

a) Tener un rol dedicado como Gerente de Seguridad de la Información.
b) Que la alta dirección promueva una mejora continua.
c) Que sean comunicados los objetivos de seguridad de la información.
d) Documentar el plan de tratamiento del riesgo.

3. Los objetivos de seguridad de la información deben ser consistentes con: (Selecciona la mejor respuesta)

a) El plan de tratamiento de riesgo.
b) La política de seguridad de la información.
c) La declaración de aplicabilidad.
d) La metodología de evaluación de riesgo.

4. Una organización tiene múltiples locaciones ejecutando respaldos de información y ha determinado que necesitan documentar su proceso para poder mantener consistencia y asegura la efectividad. Este documento debe ser: (Selecciona la mejor respuesta)

a) Aprobado por el comité de dirección de seguridad de la información.
b) Disponible y apropiado para uso, cuando y donde sea necesario.
c) Enlistado en la matriz maestro de documentos.
d) Disponible en formato electrónico e impreso.

5. Un proveedor de seguros de salud mantiene bases de datos de información confidencial de clientes. La consecuencia potencial de divulgar información privada de cualquier cliente debe ser abordado en: (Selecciona la mejor respuesta)

a) La declaración de misión de la organización.
b) El plan de tratamiento de riesgo.
c) El plan de conformidad.
d) La evaluación de riesgo.

6. El alcance del SGSI de una organización que gira en torno a proveer servicios financieros. En la política de seguridad de la información, la alta gerencia ha declarado su intención de operar dentro de los requerimientos estatales y federales. El resto de la política de seguridad de la información se enfoca en como TI entregará los servicios financieros. Esta política: (Selecciona la mejor respuesta)

a) No está conforme con ISO/IEC 27001.
b) Está conforme con ISO/IEC 27001.
c) Está conforme con ISO/IEC 27001 pero podría ser mejorada.
d) No aplica a líneas de negocio especificas.

7. Una organización de desarrollo de software ha decidido subcontratar su mesa de ayuda, la que también maneja las llamadas de incidentes de seguridad. La organización recibe un reporte de parte de la mesa de ayuda, subcontratada de manera mensual, que contiene métricas de desempeño de llamadas consistente en tiempo de espera promedio, tiempo ocioso del agente y número promedio de llamadas en cola. La organización usa el reporte como un medio para demostrar control sobre la mesa de ayuda desde el punto de vista de requerimientos de seguridad de la información. ¿Esto está conforme con la ISO/IEC 27001?

a) Verdadero.
b) Falso.

8. Las actividades coordinadas para dirigir y controlar una organización con relación al riesgo son conocidas como: (Selecciona la mejor respuesta)

a) Evaluación de riesgo.
b) Tratamiento de riesgo.
c) Gestión de riesgo.
d) Estimación de riesgo.

9. La propiedad de proteger la precisión y la completitud de los bienes es: (Selecciona la mejor respuesta)

a) Integridad.
b) Corrección.
c) Inter-operatividad.
d) No repudio.

10. Una medida que está modificando riesgo puede ser referido como: (Selecciona la mejor respuesta)

a) Remediación de riesgo.
b) Sistema de Gestión de Seguridad de la Información (SGSI).
c) Control.
d) Análisis de impacto de negocio.

11. Se puede decir que el SGSI de una organización es efectivo sí: (Selecciona la mejor respuesta)

a) La mesa de ayuda ha minimizado su personal y aún siguen cumpliendo sus objetivos.
b) Se ha mostrado que todas las áreas del proceso tienen planes y han establecido objetivos, han tomado acciones para mejorar.
c) Los equipos de auditoría interna y de cumplimiento han identificado numerosas.
d) La gerencia ha dado al gerente de TI la autoridad absoluta sobre la seguridad y ha dado al departamento de IT un presupuesto limitado.

12. Un control físico fue implementado en el SGSI de un hospital. Han determinado que su control particular debe ser medido y aseguran que es medido. Como cambian constantemente las cargas de trabajo y agendas, no han determinado una sola persona para hacer la medición. Esto está conforme con ISO/IEC 27001:

a) Verdadero.
b) Falso.

13. El SGSI de un hospital está sujeto a requerimientos legales. Desde la perspectiva de un sistema de gestión, la evaluación de cumplimiento legal consistirá de: (Selecciona la mejor respuesta)

a) Confirmar que existe un proceso dentro del hospital para mantener cumplimiento con los requerimientos legales y regulatorios.
b) Ninguna acción adicional dado que los estándares ISO manejan solo conformidad.
c) Contactar con el departamento legal para confirmar que no existen situaciones legales sobresalientes.
d) Revisar una declaración del Consejo de Dirección del hospital donde se estipulen que mantendrán los requerimientos legales.

14. La conformidad es vista como el satisfacer requerimientos desde la perspectiva de un sistema de gestión, mientras que el cumplimiento es visto como el satisfacer requerimientos desde una perspectiva legal; esto es:

a) Verdadero.
b) Falso.

15. Una operación financiera ha seleccionado sus operaciones de intercambio de valores como el alcance de su SGSI, revisando su política de seguridad de la información, no se puede ver donde la organización se compromete a cumplir las regulaciones de seguridad gubernamental. ¿Esto cumple los requerimientos de ISO/IEC 27001?

a) Verdadero.
b) Falso.

16. Una organización ha hecho de las operaciones de su procesamiento de reclamaciones el alcance de su SGSI. ¿Los controles que han seleccionado están determinados en qué proceso? (Selecciona la mejor respuesta)

a) Política de seguridad.
b) Revisión de gerencia.
c) Evaluación de riesgo.
d) Tratamiento de riesgo.

17. Una organización consiste en diez laboratorios médicos a donde los pacientes van por pruebas y están bajo la dirección de una sede central. La alta dirección ha determinado que el alcance de su SGSI será la protección de toda la información personal de los pacientes y cubrirá la sede central. ¿Esto cumple los requerimientos de ISO/IEC 27001?

a) Verdadero.
b) Falso.

18. Según ISO/IEC 27001, una evaluación de riesgo incluirá: (Selecciona la mejor respuesta)

a) Posibilidad de ocurrencia de un riesgo.
b) Partes interesadas del SGSI.
c) Opciones para tratamiento de riesgo de seguridad.
d) Resultados de medidas de control.

19. Una organización ha definido un proceso de evaluación de riesgo. Este anualmente es empleado en sus instalaciones locales y todas sus locaciones foráneas. ¿Esto produce consistencia y resultados comparables?

a) Verdadero.
b) Falso.

20. Una organización que ha identificado requerimientos regulatorios como un factor externo y el mantener cumplimiento regulatorio como un objetivo de seguridad de la información requerirá de qué en su evaluación de riesgo: (Selecciona la mejor respuesta)

a) El riesgo asociado con no cumplir obligaciones contractuales.
b) La posibilidad de ser descubierto operando fuera de los requerimientos regulatorios.
c) Las consecuencias potenciales asociadas con no satisfacer los requerimientos regulatorios.
d) Un proceso documentado para mantener cumplimiento con los requerimientos legales y regulatorios.

21. Una organización ha hecho de las operaciones de Ventas el alcance de su SGSI. Una evaluación de riesgo para la información de ventas de una organización debe incluir: (Selecciona la mejor respuesta)

a) El valor financiero asociado con la perdida de confidencialidad en la información de ventas.
b) El riesgo asociado con vendedores que transportan la información de ventas en sus laptops.
c) Una política de uso aceptable de bienes de la compañía.
d) Cifrado de los nombres y direcciones de los clientes.

22. Una gran cadena de distribución nacional tiene el objetivo de asegurar que los clientes puedan ingresar a la información de su cuenta al menos 98 % de las veces. La evaluación de riesgo deberá: (Selecciona la mejor respuesta)

a) Incluir el riesgo asociado con disponibilidad de la información.
b) Asegurar que permitir acceso a los clientes satisface los requerimientos regulatorios.
c) Incluir el riesgo asociado con que el software del cliente sea desarrollado por una compañía de desarrollo subcontratada.
d) Ser completado por el departamento de TI dado que son los custodios de los archivos de cuenta de los clientes.

23. La Declaración de Aplicabilidad debe contener los controles necesarios para implementar la opción de tratamiento de riesgo escogida, sean implementados o no, y... (Selecciona la mejor respuesta)

a) Una lista de todos los bienes a los que se aplican los controles y riegos asociados.
b) La justificación para la selección de controles y la exclusión de cualquier control.
c) Una lista de todas las políticas y procedimientos asociados y los controles con los que se relacionan.
d) Los valores totales de riesgo calculado, ordenado de mayor a menor.

24. Si uno de los objetivos de seguridad de la información de una organización fuera prevenir divulgación no autorizada de información confidencial en caso de que un equipo portátil fuera robado, los controles seleccionados para tratar el riesgo y en Declaración de Aplicabilidad deben incluir: (Selecciona la mejor respuesta)

a) Responsabilidades de usuario.
b) Cifrado.
c) Protección contra malware.
d) Seguridad de RH – Previa a contratación.

25. La evaluación de riesgo de seguridad de la información debe ser desempañada: (Selecciona la mejor respuesta)

a) Anualmente.
b) Semestralmente.
c) En intervalos planeados.
d) Solo como sea especificado por el auditor.

26. Si una organización que planea hacer un cambio a un proceso dentro del alcance de su SGSI, debe: (Selecciona la mejor respuesta)

a) Calcular los costos del cambio.
b) Actualizar la política de SGSI.
c) Controlar el cambio.
d) Actualizar los objetivos de SGSI.

27. Si cambios significativos ocurren o son propuestos, la organización debe: (Selecciona la mejor respuesta).

a) Implementar controles para mitigar el nuevo riesgo.
b) Tener una junta de revisión por la gerencia.
c) Revisar y actualizar sus objetivos de seguridad de la información.
d) Realiza una evaluación de riesgo de seguridad de la información.

28. Para mantener cumplimiento con requerimientos de licenciamiento de software, ¿Una organización empleará cuál control? (Selecciona la mejor respuesta)

a) A.5.1.1- Políticas para la seguridad de la información.
b) A.18.1.2 - Derechos de Propiedad Intelectual (DPI).
c) A.9.2.3 - Gestión de privilegios de acceso.
d) A.12.1.4 - Separación de los recursos de desarrollo, prueba y operación.

29. ¿Cuál control del anexo A sería seleccionado para mitigar el riesgo de que los empleados usen equipo de formación que es propiedad de la organización, para su uso personal? (Selecciona la mejor respuesta)

a) A.8.1.3 – Uso aceptable de los activos.
b) A.7.1.2 – Términos y condiciones del empleo.
c) A.7.2.3 – Proceso Disciplinario.
d) A.18.2.2 – Cumplimiento de las políticas y normas de seguridad.

30. ¿Cuál control podría ser seleccionado para mitigar el riego asociado con actualizar software en servidores empresariales? (Selecciona la mejor respuesta)

a) A.14.2.2 – Procedimiento de control de cambios en sistemas.
b) A.12.7.1 – Controles de auditoría de sistemas de información.
c) A.12.1.2 – Gestión de Cambios.
d) A.9.4.5 – Control de acceso al código fuente de los programas.

31. El término “hallazgo de auditoría” automáticamente significa No Conformidad.

a) Verdadero
b) Falso

32. A una persona u organización que solicita una auditoría se le refiere como: (Selecciona la mejor respuesta).

a) Auditor.
b) Auditado.
c) Cliente de Auditoría.
d) Equipo de Auditoría.

33. Cuando se establece un programa de auditoría para un sistema de gestión, la organización deberá dar prioridad a los recursos de auditoría para tratar: (Selecciona la mejor respuesta).

a) Necesidades del Negocio.
b) Riesgos.
c) Oportunidades de mercado.
d) Integración a los planes de continuidad de negocio.

34. Los objetivos de auditoría pueden incluir:

a) Evaluación de efectividad del sistema de gestión.
b) Mantenimiento de los registros de auditoría.
c) Selección de un líder de equipo.
d) Ofrecimiento de certificación para una norma.

35. El alcance de una auditoría siempre es el mismo que el alcance del sistema de gestión.

a) Verdadero.
b) Falso.

36. ¿Cuál de los siguientes factores se tomaría en consideración para determinar la viabilidad de una auditoría? (Selecciona la mejor respuesta).

a) Temas relacionados con el informe de auditoría.
b) Disponibilidad de información suficiente para planear la auditoría.
c) Cooperación adecuada del equipo de auditoría.
d) Directrices del encargado de la admisión.

37. Los documentos de trabajo del auditor pueden incluir: (Selecciona la mejor respuesta).

a) El código de conducta del auditor.
b) Identificación, incluyendo fotografía.
c) Listas de verificación, planos y formatos de levantamiento de evidencia.
d) Instrucciones para la instalación que se va a auditar.

38. La información aceptada como evidencia de auditoría deberá ser: (Selecciona la mejor respuesta).

a) Verificable.
b) Documentada.
c) Identificada por los menos dos veces.
d) Confirmada por el guía.

39. Un informe de auditoría deberá incluir, o referirse a:

a) Una lista completa de todos los empleados de la organización auditada.
b) Una lista completa de todos los documentos utilizados durante la auditoría.
c) Una descripción completa y detallada del proceso de auditoría.
d) Un resumen de los hallazgos de la auditoría.

40. El informe de auditoría deberá distribuirse a:

a) Los destinatarios definidos en el procedimiento o plan de auditoría.
b) Los destinatarios definidos por el líder del equipo de auditoría.
c) Los destinatarios definidos por la directiva de la organización auditada.
d) Los destinatarios definidos por el representante de la gestión de la organización auditada.

Respuestas

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