ISO/IEC 27001 Lead Implementer: 10 preguntas de práctica con respuestas

Diez preguntas del banco de Mindset Prep, redactadas a partir de las siguientes normas: ISO/IEC 27001:2022, ISO/IEC 27002:2022. Son preguntas de práctica originales, no preguntas de un examen real.

Diez preguntas y, después, las soluciones: la opción correcta, su explicación y la referencia en la que se basa. Responda a las diez antes de pasar a las respuestas.

¿Prefiere ver su puntuación al instante? Tiene las mismas preguntas en línea en mindsetprep.com.au/es/simulador-examen/iso-27001-lead-implementer/.

PREGUNTA 1

El equipo de implantación del SGSI de Kestrel Analytics ha completado su evaluación de los riesgos, ha seleccionado opciones de tratamiento para cada riesgo y ha determinado los controles necesarios, varios de los cuales proceden de un marco de seguridad en la nube y no de ISO/IEC 27001. El director del programa quiere que el plan de tratamiento de los riesgos se declare completo en la reunión del comité de dirección del viernes. ¿Qué pasos pendientes exige primero el apartado 6.1.3?

A. Comparar los controles determinados con el Anexo A para verificar que no se ha pasado por alto ningún control necesario, elaborar una Declaración de Aplicabilidad que justifique las inclusiones y exclusiones, y obtener la aprobación del plan por parte de la alta dirección y la aceptación formal de los riesgos residuales a nivel del consejo.

B. Reelaborar cada control extraído del marco de seguridad en la nube para que se corresponda con un control del Anexo A, elaborar la Declaración de Aplicabilidad a partir de esa correspondencia con el Anexo A y conseguir que los dueños del riesgo confirmen que todos los controles aplicables del Anexo A se reflejan en el plan de tratamiento.

C. Comparar los controles determinados con el Anexo A para verificar que no se ha pasado por alto ningún control necesario, elaborar una Declaración de Aplicabilidad que justifique las inclusiones y exclusiones, y obtener la aprobación del plan y la aceptación de los riesgos residuales por parte de los dueños del riesgo.

PREGUNTA 2

Un implementador planifica la actividad operacional de tratamiento de los riesgos exigida durante la fase de operación. ¿Qué enunciado describe correctamente lo que ese apartado obliga a hacer a la organización?

A. Elaborar la Declaración de Aplicabilidad y verificar que no se omitió ningún control necesario del Anexo A

B. Implementar el plan de tratamiento de los riesgos y conservar información documentada de los resultados del tratamiento

C. Formular el plan de tratamiento de los riesgos y obtener la aprobación de los dueños de los riesgos sobre los riesgos residuales

PREGUNTA 3

Un proveedor de servicios gestionados de cinco personas opera el SGSI de varios clientes. Un ingeniero sénior solicita cambios en el cortafuegos de producción de un cliente y, además, aprueba y despliega esos mismos cambios, porque ningún compañero tiene los conocimientos de redes necesarios para revisar el trabajo. La evaluación de los riesgos señala esta concentración de tareas como una fuente de alta probabilidad de fraude o error no detectado. El implementador debe decidir cómo tratarlo sin dejar de ser conforme. ¿Qué tratamiento concilia mejor el riesgo señalado con las limitaciones de un equipo pequeño?

A. Repartir los pasos de solicitud, aprobación y despliegue entre tres de las cinco personas de la plantilla, aunque solo ese ingeniero posee los conocimientos de cortafuegos necesarios para revisar.

B. Registrar la aceptación del riesgo residual en el registro de riesgos, ya que un equipo de cinco personas no puede separar las tareas en conflicto y no les resulta viable ninguna otra acción.

C. Transferir la administración del cortafuegos a un proveedor especializado externo para que las tareas en conflicto de solicitar, aprobar y desplegar queden fuera del propio personal de la organización.

D. Mantener el rol combinado del ingeniero, pero añadir un seguimiento independiente de los registros de cambios del cortafuegos y una revisión por la dirección documentada de cada despliegue en producción.

PREGUNTA 4

Está redactando la Declaración de Aplicabilidad de una empresa de software con sede central en Montreal y dos oficinas regionales de desarrollo que se conectan por VPN; varios desarrolladores trabajan además desde casa. Su borrador marca A.6.7 Teletrabajo como "No aplicable – la empresa no tiene una política formal de trabajo desde casa." El director de seguridad de la información le pide que confirme esta decisión de aplicabilidad antes de su aprobación. ¿Cuál es la forma más defendible de resolver la decisión de aplicabilidad de A.6.7?

A. Marcar A.6.7 como aplicable y tratarlo con una nueva política de teletrabajo.

B. Marcar A.6.7 como no aplicable, ya que las oficinas regionales son instalaciones de la empresa.

C. Marcar A.6.7 como aplicable y registrar la VPN existente como su implementación.

D. Marcar A.6.7 como no aplicable hasta que se apruebe una política de teletrabajo.

PREGUNTA 5

Meridian Legal es un despacho de abogados de tamaño medio con un SGSI certificado en operación de régimen estable. Su procedimiento de evaluación de los riesgos establece que las evaluaciones se realizan anualmente cada marzo; la de este año se completó hace tres meses. En junio el despacho firma un contrato para migrar todo su sistema de gestión de casos y todos los documentos de los clientes desde un servidor local a una nueva plataforma de software como servicio, con la puesta en servicio prevista en ocho semanas. El responsable del SGSI está planificando la migración. Con respecto a la evaluación de los riesgos del SGSI, ¿qué exige el apartado 8.2 que haga el responsable del SGSI con esta migración?

A. Evaluar los riesgos del traspaso antes de la puesta en servicio; los de la plataforma de software como servicio, una vez operativa

B. Evaluar los riesgos de la migración antes de la puesta en servicio; mantener el ciclo de marzo según lo previsto

C. Controlar la migración como un cambio planificado antes de la puesta en servicio; sus riesgos, en marzo

D. Examinar la seguridad del proveedor de software como servicio antes de la puesta en servicio; los riesgos de la migración, en marzo

PREGUNTA 6

Su análisis del riesgo está completo: algunos riesgos prevé reducirlos con controles, hay un riesgo de alto coste y baja probabilidad que el negocio pretende retener y otro que evitará desmantelando un servicio heredado. Un consultor de seguridad le entrega una hoja de cálculo con los 93 controles del Anexo A y le dice: 'Este es su tratamiento, implemente todos y cada uno y estará cubierto.' Al patrocinador del programa le gusta la simplicidad y le pide que proceda sobre esa base. ¿Qué enfoque refleja mejor los requisitos de tratamiento de los riesgos de la norma ISO/IEC 27001:2022?

A. Seguir adelante con parte del plan, tomando un control de la hoja de cálculo para cada uno de los riesgos.

B. Rechazar el plan y dejar que los resultados del análisis del riesgo determinen los controles, sin comprobación posterior.

C. Rechazar el plan y conservar la hoja de cálculo como comprobación una vez fijados los controles de cada riesgo.

D. Seguir adelante con el plan y conservar los resultados del análisis del riesgo como comprobación una vez implantados sus controles.

PREGUNTA 7

Marco, el responsable del SGSI, está preparando el expediente para la revisión anual por la dirección de la empresa con la alta dirección. Su borrador de orden del día ya cubre: el estado de las acciones de la revisión anterior, los cambios en las cuestiones internas y externas y en las partes interesadas, las tendencias del desempeño (no conformidades y acciones correctivas, resultados de seguimiento y medición, resultados de auditoría y cumplimiento de los objetivos), la retroalimentación de las partes interesadas y las oportunidades de mejora continua. Un colega que revisa el orden del día señala que sigue faltando una entrada exigida por el apartado 9.3.2. ¿Qué elemento debe añadir Marco para que las entradas de la revisión estén completas según el apartado 9.3.2?

A. El resultado de las evaluaciones de los riesgos más recientes de la organización, junto con la situación actual del plan para tratar esos riesgos.

B. El inventario de activos y la Declaración de Aplicabilidad, nuevamente aprobados por la alta dirección durante la reunión.

C. La confirmación de que las acciones correctivas arrastradas de la revisión anterior ya se han cerrado.

D. Las decisiones documentadas sobre cualquier cambio en el SGSI que la revisión concluya que es necesario.

PREGUNTA 8

Una empresa decide incorporar al alcance del SGSI una filial recién adquirida y, al mismo tiempo, flexibilizar sus criterios de aceptación del riesgo para que una franja más amplia de riesgos pueda aceptarse sin escalado. Ambas decisiones se han aprobado en principio. El implementador debe decidir cómo llevar a cabo estos dos cambios a nivel del SGSI de forma controlada. ¿Cómo deberían gestionarse estos cambios para satisfacer el requisito de cambio controlado?

A. Planificar ambos como actualizaciones del registro de riesgos y de la Declaración de Aplicabilidad

B. Planificar ambos como cambios de TI conforme al procedimiento de gestión de cambios

C. Planificar ambos como puntos de la próxima revisión por la dirección programada

D. Planificar ambos como cambios en el SGSI antes de que entren en vigor

PREGUNTA 9

Está implementando controles para la migración de una carga de trabajo con datos de clientes a una plataforma SaaS pública. El proveedor solo ofrece un acuerdo estándar de aceptación con un clic cuyos términos son fijos y no pueden negociarse. Su responsable sostiene que, una vez que los datos residen en la nube del proveedor, la seguridad de la información pasa a ser por completo responsabilidad del proveedor y no queda nada más que hacer para el SGSI. ¿Cuál es la acción más apropiada del implementador conforme al Control 5.23 de ISO/IEC 27002:2022?

A. Delimitar qué controles nos corresponden y después revisar los términos del proveedor y obtener la aceptación del riesgo residual.

B. Buscar aseguramiento sobre los controles del proveedor y después exigir una cláusula de derecho de auditoría antes de migrar.

C. Buscar aseguramiento sobre los controles del proveedor y después revisar los términos del proveedor y obtener la aceptación del riesgo residual.

D. Delimitar qué controles nos corresponden y después exigir una cláusula de derecho de auditoría antes de migrar.

PREGUNTA 10

El responsable de la implementación organiza la primera evaluación de los riesgos de seguridad de la información de la organización. El equipo prevé celebrar un taller, hacer una lluvia de ideas sobre los riesgos para la confidencialidad, la integridad y la disponibilidad de la información incluida en el alcance, puntuar la probabilidad y el impacto de cada riesgo en una escala de 1 a 5, multiplicar ambos valores para obtener un nivel de riesgo y clasificar los resultados. Prevén determinar qué niveles de riesgo está dispuesta a tolerar la organización solo más adelante, una vez que la dirección haya revisado la lista clasificada. Según el apartado 6.1.2, ¿qué requisito ha dejado de satisfacer más claramente el equipo antes de llevar a cabo esta evaluación de los riesgos?

A. Utilizar un método de puntuación que dé resultados coherentes y comparables.

B. Identificar los riesgos para la confidencialidad, la integridad y la disponibilidad.

C. Definir qué información ha de abarcar la evaluación.

D. Fijar los niveles de riesgo que la organización está dispuesta a aceptar.

Respuestas

Q1 Respuesta correcta: **C.** Comparar los controles determinados con el Anexo A para verificar que no se ha pasado por alto ningún control necesario, elaborar una Declaración de Aplicabilidad que justifique las inclusiones y exclusiones, y obtener la aprobación del plan y la aceptación de los riesgos residuales por parte de los dueños del riesgo.

El apartado 6.1.3 concluye el proceso de tratamiento con tres pasos: comparar los controles determinados con el Anexo A para verificar que no se ha omitido nada necesario, elaborar una Declaración de Aplicabilidad que justifique las inclusiones y exclusiones, y conseguir que los dueños del riesgo aprueben el plan de tratamiento y acepten los riesgos residuales. Los controles pueden proceder de cualquier fuente, por lo que los controles derivados del marco no necesitan reasignarse al Anexo A, y la aprobación corresponde a los dueños del riesgo, no a la alta dirección ni al consejo.

`Referencia: ISO/IEC 27001:2022 apartado 6.1.3`

`Trampa: T-01 Declaración de Aplicabilidad o plan de tratamiento de los riesgos`

Q2 Respuesta correcta: **B.** Implementar el plan de tratamiento de los riesgos y conservar información documentada de los resultados del tratamiento

El apartado de tratamiento de la fase de operación trata sobre la ejecución: implementar el plan de tratamiento y conservar los resultados documentados. Formular el plan, obtener la aprobación de los dueños de los riesgos y elaborar la Declaración de Aplicabilidad son todas actividades de la fase de planificación. Mantener las dos fases diferenciadas evita atribuir obligaciones de diseño a la etapa de operación.

`Referencia: ISO/IEC 27001:2022, apartado 8.3`

`Trampa: T-02 Planificación u operación`

Q3 Respuesta correcta: **D.** Mantener el rol combinado del ingeniero, pero añadir un seguimiento independiente de los registros de cambios del cortafuegos y una revisión por la dirección documentada de cada despliegue en producción.

La segregación de tareas es un principio que se aplica en la medida en que sea posible y factible, no una regla absoluta. Las organizaciones pequeñas que no pueden separar por completo las tareas en conflicto deberían considerar controles compensatorios (seguimiento, pistas de auditoría, supervisión de la dirección) en lugar de aceptar el riesgo sin tratarlo o simular una separación.

`Referencia: ISO/IEC 27002:2022 control 5.3`

`Trampa: T-03 Reducir, retener, evitar o compartir`

Q4 Respuesta correcta: **A.** Marcar A.6.7 como aplicable y tratarlo con una nueva política de teletrabajo.

El control 6.7 de la ISO/IEC 27002:2022 establece que existe teletrabajo siempre que el personal trabaja desde una ubicación externa a las instalaciones de la organización, accediendo a información en cualquier forma. Las oficinas regionales son instalaciones propias, pero los desarrolladores que trabajan desde casa cumplen esa definición, por lo que el riesgo que aborda el control existe y A.6.7 es aplicable. La aplicabilidad la determina el perfil de riesgo, no la existencia previa de una política - la política que falta es precisamente el tratamiento (una política temática específica sobre teletrabajo), y el apartado 6.1.3 de la ISO/IEC 27001 exige que la Declaración de Aplicabilidad contenga los controles necesarios, la justificación de su inclusión y si están implementados. Excluir un control cuyo riesgo está presente, o registrarlo como implementado antes de que sus medidas lleguen a las personas que teletrabajan, tergiversa el contexto de la organización.

`Referencia: ISO/IEC 27002:2022 control 6.7`

`Trampa: T-01 Declaración de Aplicabilidad o plan de tratamiento de los riesgos`

Q5 Respuesta correcta: **B.** Evaluar los riesgos de la migración antes de la puesta en servicio; mantener el ciclo de marzo según lo previsto

El apartado 8.2 establece que la organización «debe realizar evaluaciones de los riesgos de seguridad de la información a intervalos planificados o cuando se propongan u ocurran cambios significativos, teniendo en cuenta los criterios establecidos en 6.1.2 a)» y «debe conservar información documentada de los resultados». Se aplican dos desencadenantes independientes: el intervalo anual de marzo es uno; una migración propuesta en todo el despacho del sistema central de gestión de casos y de los datos de los clientes es el otro. Dado que el apartado se activa por cambios que se «proponen», y no solo por los que han ocurrido, la evaluación de los riesgos corresponde ahora, antes de la puesta en servicio, para que su resultado pueda configurar cómo se lleva a cabo la migración y para que la transición de ocho semanas no quede sin evaluar.

`Referencia: ISO/IEC 27001:2022, apartado 8.2`

`Trampa: T-02 Planificación u operación`

Q6 Respuesta correcta: **C.** Rechazar el plan y conservar la hoja de cálculo como comprobación una vez fijados los controles de cada riesgo.

El tratamiento de los riesgos lo determina la evaluación de los riesgos, no un catálogo de controles. Según el apartado 6.1.3, la organización (a) selecciona una opción de tratamiento adecuada para cada riesgo teniendo en cuenta los resultados de la evaluación de los riesgos, reducir, retener, evitar o compartir según corresponda al riesgo, después (b) determina todos los controles necesarios para implementar esas opciones, recurriendo a cualquier fuente adecuada (NOTA 1), y solo entonces (c) compara ese conjunto determinado con el Anexo A para verificar que no se ha omitido nada necesario (NOTA 2). El Anexo A es una red de seguridad de exhaustividad, no un mandato de implementar los 93 controles (lo que refuta la propuesta del consultor) ni la única fuente admisible (NOTA 1, NOTA 3). La comparación del 6.1.3 c) es en sí misma un requisito que no se puede omitir, y sus resultados sustentan las justificaciones de exclusión de la Declaración de Aplicabilidad (6.1.3 d).

`Referencia: ISO/IEC 27001:2022 apartado 6.1.3`

`Trampa: T-03 Reducir, retener, evitar o compartir`

Q7 Respuesta correcta: **A.** El resultado de las evaluaciones de los riesgos más recientes de la organización, junto con la situación actual del plan para tratar esos riesgos.

El apartado 9.3.2 enumera las entradas que una revisión por la dirección debe considerar: (a) el estado de las acciones previas; (b) los cambios en las cuestiones internas y externas; (c) los cambios en las necesidades y expectativas de las partes interesadas; (d) la retroalimentación y las tendencias del desempeño de la seguridad de la información; (e) la retroalimentación de las partes interesadas; (f) los resultados de la evaluación de los riesgos y el estado del plan de tratamiento de los riesgos; (g) las oportunidades de mejora continua. El borrador de Marco contiene a, b, c, d, e y g, de modo que la única laguna es (f), el panorama del riesgo. La entrada (a) es el estado de las acciones de las revisiones anteriores, no la prueba de que estén cerradas; las decisiones sobre cambios en el SGSI son resultados de la revisión según el apartado 9.3.3, no entradas a ella; y ni el inventario de activos ni una nueva aprobación de la Declaración de Aplicabilidad, que se elabora conforme al apartado 6.1.3 d), figuran entre las entradas enumeradas.

`Referencia: ISO/IEC 27001:2022 apartado 9.3.2`

`Trampa: T-01 Declaración de Aplicabilidad o plan de tratamiento de los riesgos`

Q8 Respuesta correcta: **D.** Planificar ambos como cambios en el SGSI antes de que entren en vigor

Lo que importa aquí es qué requisito de cambio se aplica. El alcance y los criterios de aceptación del riesgo son elementos del sistema de gestión, por lo que rige el apartado 6.3: el cambio debe llevarse a cabo de manera planificada. El control técnico de gestión de cambios se refiere a los sistemas de información, no al SGSI, y ni el aplazamiento hasta la revisión por la dirección ni la edición de registros derivados satisfacen el cambio planificado.

`Referencia: ISO/IEC 27001:2022 apartado 6.3`

`Trampa: T-02 Planificación u operación`

Q9 Respuesta correcta: **A.** Delimitar qué controles nos corresponden y después revisar los términos del proveedor y obtener la aceptación del riesgo residual.

Un acuerdo fijo y no negociable no elimina las responsabilidades del cliente. El Control 5.23 de ISO/IEC 27002:2022 señala que el uso de la nube puede implicar una responsabilidad compartida y afirma que es esencial que las responsabilidades de ambas partes se definan e implementen de forma apropiada; entre lo que la organización debería definir figura qué controles de seguridad gestiona el proveedor y cuáles gestiona ella como cliente. También figura la obtención de aseguramiento sobre los controles del proveedor, pero eso no resuelve quién opera cada control. Aunque los acuerdos de servicios en la nube a menudo están predefinidos y no están abiertos a negociación, la organización debería revisarlos igualmente frente a sus requisitos de confidencialidad, integridad, disponibilidad y tratamiento de la información, llevar a cabo una evaluación pertinente de los riesgos y tener el riesgo residual identificado y aceptado por la dirección apropiada.

`Referencia: ISO/IEC 27002:2022 Control 5.23`

`Trampa: T-03 Reducir, retener, evitar o compartir`

Q10 Respuesta correcta: **D.** Fijar los niveles de riesgo que la organización está dispuesta a aceptar.

El apartado 6.1.2(a) exige que el proceso de evaluación de los riesgos establezca y mantenga criterios de riesgo de seguridad de la información que comprendan (1) los criterios de aceptación de riesgos y (2) los criterios para llevar a cabo la evaluación de los riesgos. Son fundamentales: 6.1.2(e)(1) evalúa los riesgos comparando los resultados del análisis con esos criterios y, a continuación, los prioriza para su tratamiento. Determinar qué niveles de riesgo son tolerables solo después de clasificar los riesgos invierte ese orden exigido. Otras dos partes del plan se sostienen: el equipo identifica los riesgos para la confidencialidad, la integridad y la disponibilidad de la información incluida en el alcance (6.1.2(c)(1)), y el apartado es agnóstico respecto al método siempre que las evaluaciones repetidas de los riesgos sean coherentes, válidas y comparables (6.1.2(b)), por lo que un modelo de probabilidad por impacto es aceptable.

Referencia: ISO/IEC 27001:2022 apartado 6.1.2

Trampa: T-02 Planificación u operación

¿Quiere el banco completo?

Mindset Prep tiene más de 2500 preguntas para cinco certificaciones de PECB, cada una con su explicación, y le vuelve a presentar las preguntas que falla. Empiece con una prueba gratuita de 3 días.

Empezar la prueba gratuita de 3 días

app.mindsetprep.com.au/start

Mindset Prep es independiente de PECB y no cuenta con su aval.