ISO/IEC 42001 Lead Auditor: 10 preguntas de práctica con respuestas

Diez preguntas del banco de Mindset Prep, redactadas a partir de las siguientes normas: ISO/IEC 42001:2023, ISO 19011:2018. 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-42001-lead-auditor/.

PREGUNTA 1

Durante la auditoría de etapa 2 de un SGIA, el auditado presenta su 'evaluación del impacto del sistema de IA' para un nuevo producto de IA orientado al cliente. Al revisarlo, el documento evalúa solo los riesgos financieros y reputacionales que el producto podría suponer para la organización, puntuados según su probabilidad e impacto y priorizados para su tratamiento. No aborda las consecuencias para las personas o comunidades afectadas por el sistema. ¿Cuál es la conclusión más defendible a la que debería llegar el auditor?

A. Una oportunidad de mejora relativa al apartado 6.3

B. Una oportunidad de mejora relativa al apartado 6.1.4

C. Una no conformidad con el apartado 6.3

D. Una no conformidad con el apartado 6.1.4

PREGUNTA 2

Un líder del equipo auditor está iniciando una auditoría de certificación de tercera parte de Talveras, una empresa cuya plataforma de IA de selección de personal criba a los candidatos a un puesto. Durante el contacto inicial, el auditado entrega su declaración del alcance del SGIA, que dice: «todos los sistemas de IA utilizados en el cribado de candidatos en las oficinas de Londres y Dublín». El líder del equipo auditor está acordando ahora los objetivos, el alcance y los criterios de la auditoría para el encargo. Al acordarse los términos del encargo, el líder del equipo auditor debe confirmar los criterios de auditoría para esta auditoría. ¿Qué opción identifica correctamente cuáles son los criterios de auditoría?

A. El resultado previsto que la auditoría se propone lograr - para Talveras, confirmar que el SGIA es conforme con la norma y está implementado eficazmente para que pueda recomendarse la certificación.

B. La extensión y los límites de lo que se examinará - para Talveras, las oficinas de Londres y Dublín y los sistemas de IA de cribado de candidatos nombrados en la declaración del alcance del SGIA.

C. El conjunto de requisitos de referencia con el que se compara la evidencia recopilada - para Talveras, ISO/IEC 42001:2023, la política de IA y la Declaración de Aplicabilidad del auditado, y los requisitos legales y reglamentarios aplicables.

D. La determinación de que existen información adecuada, cooperación del auditado, tiempo y recursos - para Talveras, la comprobación que se hace antes de permitir que el encargo siga adelante.

PREGUNTA 3

Durante una auditoría de etapa 2 del SGIA, el auditado, Meridian Lending, obtiene bajo licencia un modelo de IA de calificación crediticia de un tercero, lo integra en su plataforma de originación de préstamos y ofrece esa plataforma como servicio a bancos asociados. El análisis de contexto del apartado 4.1 de Meridian documenta las cuestiones externas e internas pertinentes y registra el rol de la organización con respecto a los sistemas de IA simplemente como 'usuario de IA'. Según el escenario, ¿cuál es la base MÁS apropiada para la evaluación que hace el líder del equipo auditor de la determinación de roles del apartado 4.1 de Meridian?

A. No hay carencia: la licencia del modelo hace de 'usuario de IA' el registro correcto para Meridian.

B. Hay una carencia: el servicio de plataforma a los bancos asociados añade un rol que 'usuario de IA' omite.

C. No hay carencia: el servicio de plataforma a los bancos asociados es una cuestión del apartado 4.2.

D. Hay una carencia: la licencia del modelo hace que el único rol de Meridian sea cliente de IA, no usuario de IA.

PREGUNTA 4

Un auditado ha desplegado un gran sistema de contenidos de IA generativa que requiere una capacidad de cómputo considerable para el entrenamiento y el reentrenamiento. Durante la auditoría de etapa 2, el auditor revisa la evaluación del impacto documentada del sistema de IA. Aborda a fondo los impactos sobre los usuarios individuales y los grupos afectados: equidad, privacidad y bienestar psicológico. El auditor observa que la evaluación no aborda la huella ambiental del entrenamiento de modelos a gran escala ni la posibilidad de que el sistema contribuya a la desinformación a gran escala. El responsable del SGIA responde que «evaluamos los impactos sobre los individuos y los grupos, tal como exige la norma». ¿Contra qué control se plantea con MAYOR exactitud el hallazgo del auditor?

A. Anexo A.5.5 (Evaluación de los impactos sociales de los sistemas de IA), porque no se evaluaron impactos sociales como la huella ambiental y la desinformación.

B. Anexo A.5.4 (Evaluación del impacto del sistema de IA sobre individuos o grupos de individuos), porque la evaluación del impacto está incompleta.

C. Anexo A.4.5 (Recursos de sistema e informáticos), porque el impacto ambiental del cómputo no está documentado.

D. Apartado 6.1.2 (Evaluación del riesgo de la IA), porque la evaluación organizativa del riesgo está incompleta.

PREGUNTA 5

Una auditoría de tercera parte del SGIA cubre los 30 modelos de IA desplegados de una empresa de tecnología financiera. Doce modelos impulsan decisiones crediticias automatizadas que afectan a las personas; los otros dieciocho son herramientas de eficiencia interna (por ejemplo, el enrutamiento de documentos) con un impacto insignificante sobre las personas. El tiempo de auditoría permite examinar en profundidad unos ocho modelos. Entre los ocho modelos de crédito de alto impacto que muestrea el auditor, la evaluación del impacto del sistema de IA (apartado 6.1.4) de un modelo nunca se realizó antes del despliegue. Aplicando un enfoque basado en riesgos al muestreo y a la evidencia, ¿cuál es la mejor línea de actuación?

A. Mantener la muestra ponderada hacia los modelos de crédito y registrar una oportunidad de mejora.

B. Trasladar parte de la muestra a las herramientas internas y emitir ahora una no conformidad.

C. Trasladar parte de la muestra a las herramientas internas y registrar una oportunidad de mejora.

D. Mantener la muestra ponderada hacia los modelos de crédito y emitir ahora una no conformidad.

PREGUNTA 6

Una empresa de software cuenta con un consejo permanente de ética de la IA con miembros sénior de los departamentos jurídico, de ingeniería y de producto. Se reúne mensualmente, revisa las nuevas funcionalidades de IA, y su carta constitutiva, sus actas y sus registros de asistencia están bien documentados. El auditor confirma que el consejo funciona realmente. Sin embargo, cuando el auditor pregunta quién tiene la autoridad asignada para asegurarse de que el sistema de gestión de la IA es conforme con la norma y para informar a la alta dirección sobre el desempeño del SGIA, el personal responde vagamente «el consejo en su conjunto», y ningún registro muestra que la alta dirección haya asignado esas dos responsabilidades a una función definida. Dado el consejo de ética activo y bien documentado, ¿cuál es la posición más defendible del auditor?

A. Plantear una no conformidad contra el apartado 9.3

B. Plantear una no conformidad contra el control A.3.2

C. Plantear una no conformidad contra el apartado 5.3

D. Plantear una no conformidad contra el apartado 5.1

PREGUNTA 7

En la auditoría de etapa 2 de la entidad de crédito al consumo LumenScore, el equipo confirma una evaluación del impacto del SGIA para el modelo de puntuación crediticia en producción. Los registros operativos revelan un segundo modelo no declarado: un retador que recibe de forma silenciosa alrededor del diez por ciento de los solicitantes reales y cuyas puntuaciones toman la decisión efectiva de concesión de crédito para ellos. No se ha realizado ninguna evaluación del impacto para él. El responsable de MLOps afirma que el retador es un piloto interno controlado, no publicado formalmente, y que se documentará cuando se promocione; los pilotos, sostiene el auditado, quedan fuera del requisito de información documentada hasta entonces. Como líder del equipo auditor, ¿cuál es la posición MÁS defendible respecto al modelo retador?

A. Levantar una no conformidad contra el apartado 8.2 por el modelo retador.

B. Levantar una no conformidad contra el apartado 8.4 por el modelo retador.

C. Aceptar la condición de piloto y revisar el retador cuando se promocione.

PREGUNTA 8

Vantage Health AI se certificó conforme a la Norma ISO/IEC 42001 el año pasado. Desde entonces ha desplegado un nuevo sistema de IA importante, un modelo de triaje clínico, lo que constituye un cambio significativo en su SGIA. Un auditor está planificando la primera auditoría de seguimiento del ciclo de certificación. En la auditoría de certificación inicial se había levantado una no conformidad menor relativa a las evaluaciones del impacto de los sistemas de IA y se había aceptado su corrección. ¿Qué enfoque refleja mejor el propósito y el alcance de esta auditoría de seguimiento?

A. Muestrear el SGIA y la acción correctiva anterior, tratando el modelo de triaje como incluido en el alcance.

B. Reauditar todos los apartados y controles del Anexo A, tratando el modelo de triaje como incluido en el alcance.

C. Muestrear el SGIA y la acción correctiva anterior, tratando el modelo de triaje como todavía no incluido en el alcance.

D. Reauditar todos los apartados y controles del Anexo A, tratando el modelo de triaje como todavía no incluido en el alcance.

PREGUNTA 9

Renji Stenmark está auditando Granitepath AI Logistics, cuyo sistema de IA de enrutamiento combina un modelo de terceros, datos de entrenamiento obtenidos externamente y código de integración interno. El responsable de cumplimiento presenta los contratos de suministro del modelo y de los datos, cada uno con cláusulas de responsabilidad y garantía, y explica que estos determinan quién responde de qué. Por ello, Granitepath no mantiene ningún registro propio que establezca qué parte es responsable de cada tramo del ciclo de vida del sistema de IA. Según el escenario, ¿qué respuesta se ajusta mejor a lo que realmente espera de Granitepath la orientación sobre la asignación de responsabilidades?

A. Se espera un registro de asignación, pero tiene que abarcar el trabajo de integración interno que Granitepath controla directamente; las responsabilidades sobre el modelo adquirido y los datos de entrenamiento corresponde definirlas y documentarlas a sus proveedores.

B. La orientación espera que la propia Granitepath documente todas las partes que intervienen a lo largo del ciclo de vida del sistema de IA y sus respectivas responsabilidades, por lo que la falta del registro de asignación es una brecha, independientemente de lo que asignen los contratos.

C. Dado que cada elemento obtenido externamente está cubierto por un contrato con cláusulas de responsabilidad y garantía, la responsabilidad queda resuelta mediante la orientación sobre las relaciones con los proveedores, y un registro de asignación separado duplicaría el expediente de compras.

PREGUNTA 10

VeridicAI vende a empleadores un modelo de cribado para la selección de personal. En la etapa 2, el líder del equipo revisa la evaluación del impacto del sistema de IA. Abarca las consecuencias para los empleadores que compran la herramienta, cada una reflejada en el registro de riesgos con un propietario y un plan de tratamiento. No examina la situación jurídica ni las oportunidades vitales de los solicitantes a los que puntúa el modelo, ni ningún efecto diferencial entre grupos protegidos. El responsable de gobernanza de la IA afirma que la evaluación del impacto y la evaluación del riesgo se mantienen deliberadamente coherentes, todos los impactos se han trasladado al registro y se han tratado, por lo que el proceso está completo y cerrado. El líder del equipo auditor está decidiendo cómo calificar esta carencia. ¿Qué respuesta es la MÁS defendible?

A. No registrar ningún hallazgo: la evaluación y el registro son coherentes y están cerrados.

B. Levantar una no conformidad respecto al apartado 6.1.3 contra el plan de tratamiento del riesgo.

C. Levantar una no conformidad respecto al apartado 6.1.4 contra la evaluación del impacto.

Respuestas

Q1 Respuesta correcta: **D.** Una no conformidad con el apartado 6.1.4

Las consecuencias que importan aquí son las que recaen fuera de la organización. El apartado 6.1.4 de ISO/IEC 42001:2023 exige una evaluación del impacto del sistema de IA que determine las posibles consecuencias del despliegue, el uso previsto y el uso indebido previsible de un sistema de IA para las personas o grupos de personas y para las sociedades, y cuyos resultados se tengan en cuenta en la evaluación del riesgo de la IA del apartado 6.1.2. El documento presentado como esa evaluación solo puntúa el riesgo financiero y reputacional para la organización, por lo que deja sin hacer esa determinación. No se cumple un requisito, lo que convierte esto en una no conformidad con el apartado 6.1.4 y no en un punto de mejora.

`Referencia: ISO/IEC 42001:2023 apartado 6.1.4`

`Trampa: T-01 Evaluación del riesgo o evaluación del impacto`

Q2 Respuesta correcta: **C.** El conjunto de requisitos de referencia con el que se compara la evidencia recopilada - para Talveras, ISO/IEC 42001:2023, la política de IA y la Declaración de Aplicabilidad del auditado, y los requisitos legales y reglamentarios aplicables.

Los criterios de auditoría se confunden con facilidad con los demás asuntos que se fijan al iniciar la auditoría: el alcance, la viabilidad y los objetivos. Los criterios son los requisitos de referencia con los que se compara la evidencia objetiva (ISO 19011:2018), y el término 3.18 de ISO/IEC 42001:2023 remite a ISO 19011 para «criterios de auditoría» y «evidencia de la auditoría», por lo que esa definición rige esta auditoría de certificación de 42001. Por tanto, los criterios son la norma normativa más la propia información documentada del SGIA del auditado y los requisitos legales aplicables.

`Referencia: ISO 19011:2018 (inicio de la auditoría)`

`Trampa: T-02 Alcance del SGIA o alcance del sistema de IA`

Q3 Respuesta correcta: **B.** Hay una carencia: el servicio de plataforma a los bancos asociados añade un rol que 'usuario de IA' omite.

El apartado 4.1 exige que la organización considere el propósito previsto de los sistemas de IA que desarrolla, proporciona o utiliza y que determine sus roles con respecto a ellos; la norma enumera roles posibles (proveedor de IA, productor, cliente, socio, sujeto, autoridades pertinentes) y una organización puede desempeñar varios a la vez. Meridian es cliente de IA del suministrador del modelo y, como suministra un servicio habilitado por IA a bancos asociados, también es proveedor/socio de IA. Por tanto, registrar un único rol de 'usuario de IA' deja incompleta la determinación del contexto. Identificar a los bancos asociados como partes interesadas conforme al apartado 4.2 no resuelve el propio rol de Meridian con respecto a ellos.

`Referencia: ISO/IEC 42001:2023 apartado 4.1`

`Trampa: T-03 Roles con respecto a la IA o roles del sistema de gestión`

Q4 Respuesta correcta: **A.** Anexo A.5.5 (Evaluación de los impactos sociales de los sistemas de IA), porque no se evaluaron impactos sociales como la huella ambiental y la desinformación.

A.5 exige que la organización evalúe los impactos del sistema de IA a lo largo de todo el ciclo de vida, separando la perspectiva de las personas (A.5.4, individuos o grupos de individuos) de la perspectiva de la sociedad (A.5.5, impactos sociales). B.5.5 enumera la sostenibilidad ambiental y la desinformación entre los impactos sociales. El auditado completó la dimensión de A.5.4 pero omitió A.5.5, de modo que el hallazgo corresponde a A.5.5. El detalle ambiental es un señuelo deliberado hacia A.4.5, cuya guía B.4.5 sí menciona el impacto ambiental del hardware, pero A.4.5 trata de documentar los recursos informáticos, no de evaluar consecuencias sociales. La evaluación del impacto (consecuencias para los individuos y las sociedades) tampoco debe confundirse con la evaluación organizativa del riesgo de la IA del 6.1.2, que se refiere a los riesgos para los objetivos de IA de la organización.

`Referencia: ISO/IEC 42001:2023 Anexo A.5.5 (con B.5.5)`

`Trampa: T-01 Evaluación del riesgo o evaluación del impacto`

Q5 Respuesta correcta: **D.** Mantener la muestra ponderada hacia los modelos de crédito y emitir ahora una no conformidad.

Una muestra ponderada por riesgo puede demostrar unas cosas y otras no. ISO 19011:2018 y el enfoque basado en riesgos orientan el muestreo basado en el juicio hacia los elementos de mayor riesgo, los doce modelos de crédito que afectan a las personas, y no hacia una cobertura igualitaria o estadísticamente representativa. La evidencia de muestreo es asimétrica: una deficiencia sustenta un hallazgo y puede indicar un alcance más amplio, pero una muestra limpia nunca demuestra la conformidad de la población. Una evaluación del impacto que nunca se realizó (ISO/IEC 42001:2023, apartado 6.1.4) es un incumplimiento verificable, es decir, una no conformidad, por lo que se emite y la conclusión arrastra el riesgo residual.

`Referencia: ISO 19011:2018`

`Trampa: T-02 Alcance del SGIA o alcance del sistema de IA`

Q6 Respuesta correcta: **C.** Plantear una no conformidad contra el apartado 5.3

El requisito en cuestión es una asignación específica, por parte de la alta dirección, de la responsabilidad y la autoridad sobre dos cuestiones expresamente nombradas (la conformidad del SGIA y el informe sobre el desempeño del SGIA), no una asignación general de funciones, el liderazgo y compromiso, ni la revisión por la dirección. Un consejo de ética activo evidencia actividad, pero no esa asignación, y la carencia se sitúa en el apartado 5.3, no en el control de funciones del Anexo A.

`Referencia: ISO/IEC 42001:2023 apartado 5.3`

`Trampa: T-03 Roles con respecto a la IA o roles del sistema de gestión`

Q7 Respuesta correcta: **B.** Levantar una no conformidad contra el apartado 8.4 por el modelo retador.

La lectura defendible se apoya en el fondo y no en la etiqueta. El apartado 8.4 exige evaluaciones del impacto del sistema de IA, realizadas conforme al apartado 6.1.4, cuando se propongan cambios significativos, y el retador ya está decidiendo resultados reales de concesión de crédito para alrededor del diez por ciento de los solicitantes sin que se haya realizado ninguna. Llamarlo piloto no suspende esa obligación. La evidencia es una evaluación del impacto ausente; nada de lo encontrado muestra que falte una evaluación del riesgo de la IA conforme al apartado 8.2. Quien memoriza se fija en el momento de la información documentada; un líder del equipo auditor se fija en si hay personas reales afectadas ahora.

`Referencia: ISO/IEC 42001:2023, apartado 8.4`

`Trampa: T-01 Evaluación del riesgo o evaluación del impacto`

Q8 Respuesta correcta: **A.** Muestrear el SGIA y la acción correctiva anterior, tratando el modelo de triaje como incluido en el alcance.

Según la Norma ISO/IEC 17021-1, que establece requisitos para los organismos de certificación, una auditoría de seguimiento tiene un cometido definido dentro del ciclo de certificación: una confirmación parcial, basada en muestreo, de que el SGIA sigue siendo conforme y sigue siendo eficaz. Abarca los elementos obligatorios (entre ellos, auditoría interna, revisión por la dirección, acciones sobre no conformidades previas, cambios, uso de marcas), la eficacia de la acción correctiva anterior y cualquier cambio significativo. Por eso se muestrea el nuevo despliegue de triaje clínico, incluidas su evaluación del riesgo de la IA, su evaluación del impacto y sus controles; el apartado 8.2 de la Norma ISO/IEC 42001:2023 exige una evaluación del riesgo de la IA cuando se proponen o se producen cambios significativos, y el apartado 8.4, una evaluación del impacto cuando se propone que se produzcan cambios significativos.

`Referencia: ISO/IEC 42001:2023 apartados 8.2 y 8.4`

`Trampa: T-02 Alcance del SGIA o alcance del sistema de IA`

Q9 Respuesta correcta: **B.** La orientación espera que la propia Granitepath documente todas las partes que intervienen a lo largo del ciclo de vida del sistema de IA y sus respectivas responsabilidades, por lo que la falta del registro de asignación es una brecha, independientemente de lo que asignen los contratos.

Asignar responsabilidades significa que la propia organización documenta quién responde de cada tramo del ciclo de vida del sistema de IA entre todas las partes - proveedor de datos, proveedor del modelo e integrador interno. Los contratos reparten la responsabilidad legal entre dos firmantes; son entradas para ese mapa, no un sustituto de él, y el abastecimiento externo no reduce el mapa a la parte interna. La ausencia del registro es una brecha, con independencia de quién haya construido el modelo.

`Referencia: ISO/IEC 42001:2023 control A.10.2`

`Trampa: T-03 Roles con respecto a la IA o roles del sistema de gestión`

Q10 Respuesta correcta: **C.** Levantar una no conformidad respecto al apartado 6.1.4 contra la evaluación del impacto.

Una evaluación del impacto del sistema de IA y una evaluación del riesgo de la IA responden a preguntas distintas. La evaluación del riesgo (apartado 6.1.2) identifica los riesgos que favorecen o impiden el logro de los objetivos de IA de la organización, y puede basarse en la evaluación del impacto al evaluar sus consecuencias; la evaluación del impacto (apartado 6.1.4) debe determinar las posibles consecuencias para las personas o grupos de personas, o ambos, y para las sociedades – aquí, los solicitantes a los que puntúa el modelo, incluidos los efectos entre grupos demográficos. Por tanto, omitir esas consecuencias es una carencia de la propia evaluación del impacto, no del tratamiento del riesgo, que trasladó fielmente sus resultados. Trasladar los impactos al registro de riesgos es una buena práctica, pero no sustituye el análisis de las personas a las que afecta el sistema.

Referencia: ISO/IEC 42001:2023 Anexo B.5.2

Trampa: T-01 Evaluación del riesgo o evaluación del impacto

¿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.