ISO/IEC 27001 Lead Auditor: 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 19011:2018, 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-auditor/.

PREGUNTA 1

Trustingo Pagos es un procesador de pagos con tarjeta de Uruguay cuya plataforma de autorización opera desde una sala de servidores segura protegida por una doble puerta con control por tarjeta y una recepción sujeta a seguimiento, con cada entrada registrada en un rastro electrónico de accesos. Mientras es acompañado por las instalaciones durante la Etapa 2, un auditor observa que un empleado pasa su tarjeta y a continuación mantiene abierta la puerta interior a un contratista de mantenimiento que va unos pasos por detrás, quien entra sin presentar ninguna credencial. El guía que lo acompaña comenta que el contratista 'viene todas las semanas y todo el mundo lo conoce.' ¿Cuál es el siguiente paso MÁS apropiado para el auditor?

A. Emitir una no conformidad menor por la única desviación del empleado en la puerta.

B. Comprobar en el rastro de accesos las visitas semanales del contratista.

C. Emitir una no conformidad mayor por la entrada del contratista sin credencial.

D. Comprobar en el rastro de accesos las demás entradas del empleado.

PREGUNTA 2

Un líder del equipo auditor revisa el programa de auditoría interna de un auditado: cada área se audita con una rotación uniforme de 36 meses, secuenciada alfabéticamente por departamento. Durante el último año, dos incidentes significativos afectaron a procesos de los capítulos 8 y 9, y las últimas auditorías internas de esas áreas plantearon hallazgos reiterados en cada caso, pero la rotación no ha cambiado. ¿Cómo debería tratar el líder del equipo el programa?

A. Plantear una no conformidad, porque la planificación del programa tiene que reflejar cuánto importa cada proceso y qué encontraron las auditorías anteriores, y una rotación alfabética plana no refleja ninguna de esas entradas.

B. No plantear ningún hallazgo, porque el apartado deja el intervalo a la organización, y una rotación de 36 meses documentada, dotada de recursos y ejecutada de forma consistente satisface el requisito de intervalos planificados que establece.

C. Registrar una observación, porque ponderar el programa según el riesgo y los resultados anteriores es orientación procedente de ISO 19011 sobre la gestión del programa, y un hallazgo certificable necesita un requisito de la propia ISO/IEC 27001.

PREGUNTA 3

Devon Okafor está auditando Northwind Compliance. Para satisfacer el control de revisión independiente, Northwind encarga a su Responsable de Seguridad de la Información que revise cada año el enfoque global de la organización para gestionar la seguridad de la información y que informe de los resultados al propio superior jerárquico de ese mismo Responsable de Seguridad de la Información, el Director de Operaciones de TI, que es propietario de la mayoría de los controles revisados. Northwind sostiene que el revisor es sénior, competente y no forma parte de los equipos operativos, por lo que la revisión es independiente. Aplicando el control de revisión independiente a este planteamiento, ¿qué debería concluir el auditor?

A. Una oportunidad de mejora sobre el control 5.35

B. Sin hallazgo: se cumple el control 5.35

C. Una no conformidad con el control 5.35

PREGUNTA 4

Usted está realizando la auditoría de etapa 2 de Brindhal Freight, un operador logístico en Portugal. Su gestión documentada del acceso privilegiado otorga a cada administrador una identidad privilegiada personal, deshabilita las cuentas genéricas "root" y concede derechos elevados solo justo a tiempo para las ventanas de cambio aprobadas, tras las cuales los derechos caducan automáticamente. La política de control de acceso y el registro de administradores autorizados están completos y actualizados, y el responsable de seguridad de la información confirma que la herramienta de gestión del acceso privilegiado (PAM) aplica estas reglas. ¿Qué acción demostraría de forma más fiable que el control de gestión de privilegios de acceso opera según lo diseñado y no está meramente documentado?

A. Muestrear sesiones privilegiadas y comprobar que cada una se grabó íntegramente y la revisó un segundo administrador.

B. Inspeccionar la configuración de la herramienta PAM y comprobar que las concesiones requieren aprobación previa y caducan con su ventana.

C. Inspeccionar la configuración de la herramienta PAM y comprobar que graba cada sesión para su revisión por un segundo administrador.

D. Muestrear cambios completados y comprobar que cada concesión utilizada se aprobó previamente y caducó con su ventana.

PREGUNTA 5

Marcus Patel está auditando la gestión de las vulnerabilidades técnicas en Kestrel Financial Services. La organización ejecuta un escaneo de vulnerabilidades autenticado semanal en todo su parque de servidores y corrige los hallazgos críticos dentro de un plazo acordado, con tiques que lo evidencian. Cuando Marcus pide el inventario de activos en el que se apoya el programa de escaneo, el director de Operaciones de TI admite que no existe un inventario mantenido de software y sistemas; el escaneo simplemente barre los rangos de direcciones IP que responden. Varias cargas de trabajo en la nube se crean y se destruyen a diario y nunca están dentro del alcance cuando se ejecuta el escaneo semanal. ¿Cuál es el hallazgo más apropiado que debería plantear el auditor?

A. Ningún hallazgo: se cumple el control 8.8

B. Una oportunidad de mejora respecto al control 8.8

C. Una no conformidad con el control 8.8

PREGUNTA 6

En una empresa de 40 personas usted revisa el programa de auditoría interna. El propietario-gerente auditó las áreas de finanzas y de recursos humanos; el responsable de TI auditó todas las áreas de controles técnicos, incluidas la configuración de la red y las restauraciones de copias de seguridad que él mismo administra a diario. Ambos auditores están formados, los registros están completos, los hallazgos se comunicaron a la dirección y el programa de auditoría se ejecuta según lo previsto. ¿Cuál es el hallazgo más defendible respecto a esta disposición de auditoría interna?

A. Una oportunidad de mejora en las auditorías de las áreas de finanzas y de recursos humanos

B. Una no conformidad frente al apartado 9.2.2 en las auditorías de las áreas técnicas

C. Una oportunidad de mejora en las auditorías de las áreas técnicas

D. Una no conformidad frente al apartado 9.2.2 en las auditorías de las áreas de finanzas y de recursos humanos

PREGUNTA 7

Brightmoor Health Analytics, una oficina de tratamiento de datos en Nueva Zelanda, está orgullosa de su programa de seguimiento. Unos cuadros de mando recogen la latencia de aplicación de parches, el número de inicios de sesión fallidos, las tasas de clic en simulaciones de phishing y el volumen de incidencias, se actualizan a diario y se archivan mensualmente; el auditado ofrece doce meses de métricas conservadas como evidencia de que su SGSI impulsa la mejora continua. Cuando usted pregunta cómo se utilizan las cifras, el responsable de seguridad dice que se recopilan y se almacenan para que estén «disponibles por si alguien las pide». No encuentra usted ningún registro de que alguien haya interpretado las cifras, las haya comparado con los objetivos del SGSI o haya actuado sobre lo que revelaban. ¿Qué afirmación caracteriza MEJOR la carencia que el auditor debería registrar?

A. Las cifras se recopilan y se conservan, pero nadie las analiza ni las evalúa.

B. Las cifras se analizan y se evalúan, pero ninguna información documentada lo demuestra.

C. Las cifras se recopilan y se conservan, pero no dan lugar a ninguna acción correctiva.

D. Las cifras dan lugar a acciones correctivas, pero ninguna información documentada lo demuestra.

PREGUNTA 8

Halcyon Risk Advisory se apoya en un estándar de bastionado emitido por un proveedor externo para configurar sus servidores; el personal lo considera autorizado y lo sigue a diario. La delegada de protección de datos, Maren Holloway, mantiene un control de versiones, unas reglas de acceso y una retención estrictos sobre los documentos redactados por la empresa, pero afirma que el documento del proveedor se deja exactamente como se recibió, sin identificación interna ni seguimiento de cambios porque, al ser externo, es responsabilidad del proveedor controlarlo, no de Halcyon. ¿Qué postura de auditoría refleja mejor el apartado 7.5.3 de ISO/IEC 27001:2022 en relación con el documento suministrado por el proveedor?

A. Una oportunidad de mejora relativa al apartado 7.5.3

B. Sin hallazgo: el apartado 7.5.3 se cumple

C. Una no conformidad con el apartado 7.5.3

PREGUNTA 9

Está auditando a Meridian Health Analytics. Su Declaración de Aplicabilidad incluye el control 5.18 (Derechos de acceso), seleccionado para garantizar que el acceso de quienes dejan la organización se retire con prontitud. Las cuatro últimas revisiones trimestrales de derechos de acceso están documentadas y firmadas por el propietario del sistema como «revisado, sin incidencias». Su muestra detecta tres exempleados que se marcharon hace entre tres y cinco meses y que siguen teniendo cuentas activas en la plataforma; los tres se marcharon antes de la revisión más reciente. El propietario del sistema insiste en que el control es conforme: la revisión se realiza cada trimestre y se firma exactamente como exige la política de control de acceso. ¿Cómo debería responder el auditor a la postura del propietario del sistema?

A. Levantar la no conformidad contra el apartado 9.2 auditoría interna, porque la propia revisión de la organización debería haber identificado siempre las cuentas y, por tanto, es la propia función de auditoría interna la que incumplió el requisito.

B. Registrar una observación en lugar de una no conformidad, ya que las cuentas residuales son un problema aislado de calidad de los datos y los cuatro registros de revisión firmados son evidencia objetiva de que el control de derechos de acceso funciona según lo previsto.

C. Aceptar que el control es conforme durante este periodo: la revisión de derechos de acceso se ha realizado con la frecuencia trimestral exigida, y cada una de las cuatro últimas revisiones está documentada y firmada por el propietario del sistema exactamente como especifica la política de control de acceso de la organización, que es la evidencia que el procedimiento se diseñó para generar.

D. La conformidad depende de si el control logra su objetivo, la retirada oportuna del acceso de los exempleados, no de si la revisión se programó y se firmó; la revisión pasó por alto a tres exempleados que conservaron el acceso, por lo que el control es ineficaz y procede una no conformidad.

PREGUNTA 10

Al revisar el tratamiento de los riesgos en una pyme de logística, encuentra una Declaración de Aplicabilidad que enumera todos los controles necesarios con la justificación de su inclusión, un estado de implementación declarado para cada uno y los motivos de cada control del Anexo A excluido. Existe un plan de tratamiento de los riesgos independiente y es realista. Sin embargo, el plan lleva la nota de versión 'borrador, pendiente de aprobación', y no encuentra ningún registro de que los dueños del riesgo lo hayan aprobado o hayan aceptado el riesgo residual. ¿Cuál es la conclusión más defendible?

A. Procede una no conformidad porque no se puede confiar en un borrador del plan de tratamiento, por lo que debe repetirse toda la evaluación de los riesgos antes de que la Declaración de Aplicabilidad pueda aceptarse como válida.

B. La Declaración de Aplicabilidad está completa, pero no se cumple el requisito de tratamiento de los riesgos porque los dueños del riesgo no han aprobado el plan ni han aceptado el riesgo residual.

C. El requisito de tratamiento de los riesgos se cumple, ya que la Declaración de Aplicabilidad recoge los controles necesarios, las justificaciones de inclusión y exclusión, y el estado de implementación de cada control.

D. Se trata de una oportunidad de mejora que recomienda a la empresa finalizar pronto la aprobación, ya que las decisiones sustantivas de tratamiento se han documentado y el plan en sí es realista y viable.

Respuestas

Q1 Respuesta correcta: **B.** Comprobar en el rastro de accesos las visitas semanales del contratista.

Un único incidente observado de acceso tras una persona autorizada es una pista, no una conclusión clasificada. El contratista entró sin presentar ninguna credencial, por lo que se eludió el control de entrada mediante tarjeta (control 7.2 de ISO/IEC 27001:2022, Controles físicos de entrada) y su entrada no figura en el rastro electrónico de accesos. La clasificación de una no conformidad (mayor = fallo sistémico; menor = desviación aislada) depende del alcance, e ISO 19011:2018 recomienda que las conclusiones se extraigan de evidencia verificable adecuada. El comentario del guía sugiere que al contratista se le deja entrar de forma rutinaria, pero no es evidencia verificada. Comprobar en el rastro las visitas semanales que describe el guía permite contrastarlo; las entradas con tarjeta del propio empleado no pueden hacerlo, ya que solo muestran los movimientos del empleado. Así pues, el auditor comprueba el rastro antes de clasificar nada.

`Referencia: ISO 19011:2018 (enfoque basado en la evidencia; clasificación de las no conformidades)`

`Trampa: T-01 Evidencia o hallazgo`

Q2 Respuesta correcta: **A.** Plantear una no conformidad, porque la planificación del programa tiene que reflejar cuánto importa cada proceso y qué encontraron las auditorías anteriores, y una rotación alfabética plana no refleja ninguna de esas entradas.

El deber de consideración está en la propia norma certificable: el apartado 9.2.2 exige que el programa de auditoría tenga en cuenta la importancia de los procesos afectados y los resultados de auditorías previas. Una rotación alfabética de 36 meses que se deja sin cambios tras incidentes significativos y hallazgos reiterados no supera ninguna de las dos pruebas, por lo que una no conformidad está justificada. Fijar la frecuencia de auditoría es una parte del apartado, no la totalidad de él, y el deber de consideración pertenece a la propia ISO/IEC 27001, no solo a la orientación de ISO 19011.

`Referencia: ISO/IEC 27001:2022 Apartado 9.2.2`

`Trampa: T-02 «Debe» o «debería»`

Q3 Respuesta correcta: **C.** Una no conformidad con el control 5.35

Aquí la independencia es estructural, no solo una cuestión de competencia. La guía del control indica que la revisión debería llevarla a cabo alguien independiente del área revisada y ajeno a su línea de autoridad, como la función de auditoría interna, un responsable independiente o una organización externa especializada en este tipo de revisiones. Un responsable cuyo propio superior jerárquico es propietario de la mayoría de los controles revisados está dentro de esa línea de autoridad y no puede ofrecer esa evaluación independiente, por muy capaz que sea. Dado que el control 5.35 del Anexo A de la ISO/IEC 27001 exige que el enfoque se revise de forma independiente, la carencia es una no conformidad y no un punto de mejora.

`Referencia: ISO/IEC 27002:2022 control 5.35`

`Trampa: T-03 Competencia o independencia`

Q4 Respuesta correcta: **D.** Muestrear cambios completados y comprobar que cada concesión utilizada se aprobó previamente y caducó con su ventana.

No toda la evidencia de la auditoría tiene el mismo peso: la documentación, el testimonio y la configuración de la herramienta establecen que un control existe y está diseñado; solo la evidencia de que actúa sobre sucesos reales establece que opera. Esos sucesos deben ser los que rige el diseño, en este caso derechos elevados concedidos justo a tiempo para las ventanas de cambio aprobadas y que caducan automáticamente. El control 8.2 de ISO/IEC 27002:2022 indica que la asignación de derechos de acceso privilegiado debería controlarse mediante un proceso de autorización, y entre las medidas a considerar incluye conceder acceso privilegiado temporal solo durante la ventana de tiempo necesaria para implementar los cambios aprobados. Rastrear los cambios completados hasta el acceso utilizado y confirmar después la autorización previa y la caducidad pone a prueba la operación misma. Ese es el enfoque basado en la evidencia de ISO 19011:2018.

`Referencia: ISO/IEC 27002:2022 Control 8.2 (Gestión de privilegios de acceso)`

`Trampa: T-01 Evidencia o hallazgo`

Q5 Respuesta correcta: **C.** Una no conformidad con el control 8.8

La gestión de las vulnerabilidades técnicas es más que escanear y parchear. La ISO/IEC 27002 describe un inventario de activos preciso como requisito previo para una gestión eficaz de las vulnerabilidades técnicas. Aquí no existe un inventario mantenido, y las cargas de trabajo efímeras en la nube nunca entran en el escaneo, de modo que la organización no puede demostrar que gestiona sus vulnerabilidades. El control 8.8 del Anexo A de la ISO/IEC 27001 exige que se evalúe la exposición a las vulnerabilidades de los sistemas de información en uso, por lo que esto es una no conformidad y no un punto de mejora.

`Referencia: ISO/IEC 27002:2022, control 8.8`

`Trampa: T-02 «Debe» o «debería»`

Q6 Respuesta correcta: **B.** Una no conformidad frente al apartado 9.2.2 en las auditorías de las áreas técnicas

Un programa de auditoría completo y bien llevado falla igualmente si un auditor revisa un área que él mismo opera. La imparcialidad es un elemento obligatorio del requisito de auditoría interna, por lo que esto es una no conformidad, no una oportunidad de mejora, y recae en las auditorías de las áreas técnicas, ya que nada en la pregunta muestra que el propietario-gerente realice a diario trabajo de finanzas o de recursos humanos.

`Referencia: ISO/IEC 27001:2022, apartado 9.2.2`

`Trampa: T-03 Competencia o independencia`

Q7 Respuesta correcta: **A.** Las cifras se recopilan y se conservan, pero nadie las analiza ni las evalúa.

La carencia aquí es medir frente a evaluar. El apartado 9.1 de la ISO/IEC 27001:2022 no se detiene en el seguimiento y la medición; también exige que los resultados se analicen y evalúen, y que se evalúen el desempeño de la seguridad de la información y la eficacia del SGSI. Unas métricas recopiladas, conservadas y dejadas «disponibles por si alguien las pide» son evidencia inerte: la fase de Verificar produce resultados que nunca llegan a la de Actuar, por lo que nada alimenta la mejora. Disponer de información documentada como evidencia de los resultados satisface una parte del apartado. Lo que falta es el propio análisis y la propia evaluación, no información documentada sobre ellos, y hasta que alguien interprete las cifras, nada en ellas ha salido a la luz para que una acción correctiva lo aborde.

`Referencia: ISO/IEC 27001:2022, apartado 9.1 Seguimiento, medición, análisis y evaluación`

`Trampa: T-01 Evidencia o hallazgo`

Q8 Respuesta correcta: **C.** Una no conformidad con el apartado 7.5.3

El apartado 7.5.3 no se detiene en los documentos que redacta la organización. La información documentada de origen externo que la organización considera necesaria para la planificación y la operación del SGSI debe identificarse según corresponda y controlarse. Un estándar de bastionado de un proveedor que el equipo sigue a diario es exactamente eso, de modo que dejarlo sin control porque vino de fuera deja un requisito sin cumplir: una no conformidad, no un punto de mejora.

`Referencia: apartado 7.5.3 de ISO/IEC 27001:2022`

`Trampa: T-02 «Debe» o «debería»`

Q9 Respuesta correcta: **D.** La conformidad depende de si el control logra su objetivo, la retirada oportuna del acceso de los exempleados, no de si la revisión se programó y se firmó; la revisión pasó por alto a tres exempleados que conservaron el acceso, por lo que el control es ineficaz y procede una no conformidad.

La conformidad se juzga frente a una sola cosa: el objetivo del control, no la completitud del registro de la actividad. El Anexo A 5.18 de ISO/IEC 27001:2022 exige que los derechos de acceso se aprovisionen, revisen, modifiquen y eliminen para que el acceso siga autorizado según los requisitos del negocio, incluida la retirada oportuna del acceso de quienes dejan la organización. Tres exempleados conservaron cuentas activas pese a una revisión firmada, por lo que el objetivo no se cumple y procede una no conformidad; las firmas solo evidencian que la revisión tuvo lugar.

`Referencia: ISO/IEC 27002:2022 Control 5.18 (derechos de acceso; retirada oportuna del acceso de quienes dejan la organización)`

`Trampa: T-01 Evidencia o hallazgo`

Q10 Respuesta correcta: **B.** La Declaración de Aplicabilidad está completa, pero no se cumple el requisito de tratamiento de los riesgos porque los dueños del riesgo no han aprobado el plan ni han aceptado el riesgo residual.

Una Declaración de Aplicabilidad completa no cierra por sí sola el requisito de tratamiento de los riesgos. La aprobación del plan por parte de los dueños del riesgo y la aceptación del riesgo residual son resultados obligatorios independientes, ausentes aquí, por lo que procede una no conformidad y no una oportunidad de mejora ni una nueva e innecesaria evaluación de los riesgos.

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

`Trampa: T-02 «Debe» o «debería»`

¿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.