ISO 31000 Risk Manager: 10 preguntas de práctica con respuestas

Diez preguntas del banco de Mindset Prep, redactadas a partir de la norma ISO 31000:2018. 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-31000-risk-manager/.

PREGUNTA 1

Un fabricante dispone de una excelente presentación unidireccional de informes sobre el riesgo: informes trimestrales para el consejo, cuadros de mando y un registro mantenido al día. Sin embargo, sus criterios de riesgo siguen sin reflejar la realidad operativa de la primera línea, y el personal de planta aplica los controles de forma inconsistente porque no comprende los factores de riesgo subyacentes. El responsable de riesgos observa que las decisiones se siguen tomando sin el conocimiento de la primera línea y quiere corregir la causa raíz en lugar de los síntomas. ¿Qué incorporación al proceso de gestión del riesgo aborda de forma más directa esta carencia conforme a ISO 31000:2018?

A. Asignar responsabilidades más claras a los propietarios del riesgo, de modo que cada control tenga un propietario designado que responda de aplicarlo de forma consistente y de informar sobre su estado.

B. Aumentar la frecuencia y el detalle de los informes de riesgo existentes, de modo que el personal de primera línea reciba información más completa y oportuna sobre los riesgos y los controles que se espera que aplique.

C. Añadir comunicación y consulta en dos direcciones a lo largo de todas las etapas, para que la retroalimentación de las partes interesadas configure decisiones como el establecimiento de los criterios de riesgo y la valoración del riesgo, y el personal comprenda por qué se requieren las acciones.

D. Reforzar el seguimiento y la revisión en todo el proceso, de modo que la aplicación inconsistente de los controles se detecte antes y se corrija mediante el ciclo de gestión del desempeño antes de que las brechas afecten a los resultados.

PREGUNTA 2

Rivervale Health Services se preparaba para lanzar un servicio de diálisis comunitaria. Antes de finalizar los criterios de riesgo y la evaluación del riesgo, el responsable de riesgos convocó a personal médico, a personal de enfermería de primera línea, a un grupo de representación de los pacientes y al regulador del sector, de modo que sus conocimientos, opiniones y percepciones sobre los riesgos del nuevo servicio quedaran recogidos mientras la evaluación aún se estaba configurando. Varias preocupaciones planteadas por los representantes de los pacientes, desconocidas para el equipo de proyecto, cambiaron de forma material cómo se plantearon dos de los riesgos. La decisión del responsable de riesgos de incorporar a esas partes de forma temprana, para que sus percepciones configuraran la evaluación, ¿qué principio de la norma ISO 31000 refleja de forma más directa?

A. Factores humanos y culturales: el comportamiento humano y la cultura influyen de forma significativa en todos los aspectos de la gestión del riesgo, y configuran cómo las personas de cada nivel y etapa perciben, juzgan y responden al riesgo.

B. Inclusiva: participación apropiada y oportuna de las partes interesadas para que se consideren sus conocimientos, opiniones y percepciones, lo que da lugar a una mayor toma de conciencia y a una gestión del riesgo más informada.

C. Mejor información disponible: entradas extraídas de datos históricos y actuales y de expectativas futuras, teniendo en cuenta de forma explícita las limitaciones y las incertidumbres de esa información.

D. Comunicación y consulta: compartir información con las partes interesadas y obtener su retroalimentación a lo largo de las etapas de la gestión del riesgo, de modo que se consideren distintas opiniones y se construya un sentido de apropiación.

PREGUNTA 3

La dirección de NnanTech quiere tener criterios de riesgo cuanto antes para que las divisiones puedan empezar a puntuar los riesgos de forma coherente. Un consultor ha redactado una pulida matriz de cinco por cinco con bandas numéricas de probabilidad y umbrales de impacto financiero, comparada con las referencias habituales del sector y lista para implantarse la semana que viene. Al consejo le gusta que parezca rigurosa y comparable con la de sus homólogos. El gestor de riesgos, Devon, duda y señala que la dirección aún no ha acordado cuánto riesgo y de qué tipo está realmente preparada la organización para asumir en la consecución de sus objetivos. ¿Qué debería decidir primero la alta dirección para que los criterios sean sólidos?

A. Qué riesgos asumirá y cuáles no, y en qué medida cada uno

B. Quién tiene la autoridad y la obligación de rendir cuentas sobre los criterios de riesgo

C. Cómo se definirán y medirán las consecuencias y la probabilidad

PREGUNTA 4

Meridian Freight, un operador logístico, estaba estableciendo su proceso de gestión del riesgo para el año siguiente. Antes de que se hubiera identificado o analizado ningún riesgo, el director de riesgos trabajó con el consejo de administración para acordar declaraciones escritas que establecían cuánta pérdida financiera estaba dispuesta a absorber la organización por evento, qué categorías de consecuencias para la seguridad eran inaceptables y cómo se medirían la probabilidad y la consecuencia. Las declaraciones estaban alineadas con los objetivos y las políticas declaradas de la organización. ¿Qué etapa del proceso de gestión del riesgo de ISO 31000:2018 está llevando a cabo el director de riesgos?

A. Establecer el contexto externo e interno, el entorno en el que la organización persigue sus objetivos.

B. Realizar la valoración del riesgo, comparando los riesgos analizados con los umbrales de la organización para decidir cuáles requieren tratamiento.

C. Realizar el análisis del riesgo para comprender el nivel de cada riesgo a partir de sus consecuencias y su probabilidad.

D. Definir los criterios de riesgo frente a los cuales se valora la importancia del riesgo.

PREGUNTA 5

Cuatro meses antes de su entrada en vigor, un regulador anunció una norma de localización de datos que afectaba directamente a los acuerdos de nube externalizados de una empresa. La empresa actualizaba su registro de riesgos con un ciclo anual fijo, y la siguiente actualización programada estaba a nueve meses vista. El responsable de riesgos indicó al equipo que añadiera y evaluara el nuevo riesgo regulatorio de inmediato, que reasignara la propiedad y que revisara los planes de tratamiento afectados, en lugar de esperar al ciclo anual. ¿Qué principio de la norma ISO 31000:2018 está respetando principalmente el responsable de riesgos?

A. Dinámica, la gestión del riesgo responde de manera oportuna a los cambios en el contexto de la organización.

B. Mejora continua, el marco de referencia se mejora a lo largo del tiempo mediante las lecciones que aprende la organización.

C. Mejor información disponible, el registro refleja la información regulatoria actual, obtenida de sus fuentes y mantenida al día.

D. Seguimiento y revisión, el seguimiento y la revisión continuos mantienen actualizado el registro de riesgos a lo largo del proceso.

PREGUNTA 6

Aldermere, una cooperativa regional de alimentación, está realizando la identificación del riesgo para una nueva línea de productos de marca propia. El responsable de riesgos enumera las interrupciones de suministro de los productores contratados, pero propone dejar dos elementos fuera del registro: una sequía regional prolongada, con el argumento de que el clima queda fuera del control de la cooperativa, y el daño a la promesa de marca de 'cultivo local', con el argumento de que no puede expresarse en dólares. Aplicando el apartado 6.4.2 de la ISO 31000:2018, ¿cómo debería tratar el responsable de riesgos estas dos exclusiones propuestas?

A. Mantener ambas exclusiones y dejar constancia del motivo para los responsables de la toma de decisiones.

B. Retirar ambas exclusiones e incluir ambos elementos en el registro.

C. Retirar la exclusión de la promesa de marca y dejar constancia de por qué la sequía queda fuera.

D. Retirar la exclusión de la sequía y dejar constancia de por qué la promesa de marca queda fuera.

PREGUNTA 7

Una empresa de logística trata un riesgo de interrupción de la cadena de suministro mediante el doble abastecimiento de un componente crítico. Una vez operativo el acuerdo, el dueño del riesgo evalúa el riesgo tratado frente a los criterios de riesgo de la empresa y constata que la exposición restante sigue por encima del nivel que el consejo fijó como tolerable. El tratamiento funcionó según lo diseñado y no introdujo problemas nuevos; simplemente, el riesgo de interrupción era mayor de lo que una sola medida podía reducir. El dueño del riesgo ha documentado la exposición restante, ha informado al consejo y la ha programado para revisión. Según el proceso de tratamiento del riesgo, ¿qué debería hacer el dueño del riesgo con esta exposición restante?

A. Pedir al consejo que reconsidere el nivel tolerable que fijó para este riesgo.

B. Sustituir el doble abastecimiento por una opción de tratamiento diferente.

C. Seleccionar un tratamiento adicional que se aplique junto con el doble abastecimiento.

D. Dejar la exposición tal como está y mantenerla en revisión continua.

PREGUNTA 8

Thandi Krause, Gerente de Riesgos Corporativos en Currentline Power Distribution, reserva dos días cada seis meses para un ejercicio que mantiene separado de las revisiones del registro que su equipo ya realiza. Reúne evidencias de lo que el comité ejecutivo ha obtenido realmente del programa de riesgos en este periodo, compara el estado actual del programa con lo que se esperaba que hubiera entregado a estas alturas, y se forma una opinión para el consejo de administración sobre una única pregunta: ¿el programa de riesgos que la empresa puso en marcha hace dos años sigue justificando su lugar en el apoyo a las decisiones estratégicas? No vuelve a calificar ningún riesgo ni propone aún ningún rediseño. ¿Qué actividad de ISO 31000 está realizando Thandi?

A. Valoración del riesgo: comparar los resultados del análisis del riesgo con los criterios de riesgo de la organización para decidir si se requiere alguna acción adicional sobre un riesgo determinado

B. Valorar el marco de referencia de la gestión del riesgo: juzgar periódicamente si las disposiciones creadas para apoyar la toma de decisiones siguen logrando aquello para lo que se establecieron

C. Seguimiento y revisión dentro del proceso de la gestión del riesgo: comprobar periódicamente que las evaluaciones del riesgo siguen vigentes y que los tratamientos siguen funcionando a medida que cambia el contexto de la organización

PREGUNTA 9

Una empresa de logística realizó una prueba estacional de reparto con drones sobre un concurrido puerto costero. El análisis del riesgo mostró que los drones creaban un riesgo de colisión en el aire sobre el puerto que superaba los criterios de riesgo de la empresa. Tras sopesar las opciones, el dueño del riesgo decidió interrumpir por completo la prueba de reparto con drones y volver al servicio de reparto por carretera existente de la empresa. ¿Cuál de las siete opciones de tratamiento del riesgo de la ISO 31000 representa la decisión del dueño del riesgo?

A. Eliminar la fuente de riesgo

B. Compartir el riesgo

C. Modificar la probabilidad

D. Evitar el riesgo

PREGUNTA 10

La alta dirección de una empresa de logística está adoptando ISO 31000 y quiere mostrar un liderazgo y un compromiso tangibles. Ya ha delegado el trabajo de identificación del riesgo y de análisis en un equipo de riesgos de segunda línea de reciente creación. El consejo de administración ha pedido al ejecutivo que señale una acción, realizada por la propia alta dirección, que demuestre su liderazgo y su compromiso antes de la próxima revisión trimestral. ¿Qué acción demuestra de la manera más directa el liderazgo y el compromiso tal como se describen en el apartado 5.2 de ISO 31000:2018?

A. Confirmar que los sistemas utilizados para gestionar el riesgo están implementados en toda la organización y operan eficazmente.

B. Facilitar los talleres en los que el personal identifica los riesgos para que la organización pueda elaborar y mantener su registro de riesgos.

C. Emitir una política que establezca el enfoque de la gestión del riesgo de la organización y asignar los recursos necesarios para gestionar el riesgo.

D. Completar análisis DAFO y PEST del contexto operativo para trazar un mapa de las fortalezas, las debilidades y las presiones externas de la organización.

Respuestas

Q1 Respuesta correcta: **C.** Añadir comunicación y consulta en dos direcciones a lo largo de todas las etapas, para que la retroalimentación de las partes interesadas configure decisiones como el establecimiento de los criterios de riesgo y la valoración del riesgo, y el personal comprenda por qué se requieren las acciones.

El apartado 6.2 establece que el propósito de la comunicación y consulta es ayudar a las partes interesadas a comprender el riesgo y la base de las decisiones, que la comunicación promueve la toma de conciencia mientras que la consulta obtiene retroalimentación para apoyar la toma de decisiones, y que ambas deberían tener lugar dentro de todas las etapas del proceso y a lo largo de ellas, asegurando que se consideren diferentes puntos de vista al definir los criterios de riesgo y al valorar los riesgos, y construyendo un sentido de inclusión y pertenencia. El fabricante ya cuenta con una sólida presentación de informes hacia fuera; lo que le falta es el bucle interno de consulta en dos direcciones, por lo que añadir consulta a lo largo de cada etapa es la solución. Aumentar la presentación de informes (apartado 6.7), reforzar el seguimiento (apartado 6.6) y clarificar las responsabilidades de los propietarios del riesgo (apartado 5.4.3) son todas palancas legítimas, pero cada una apunta a una etapa distinta y deja sin abordar el bucle de retroalimentación ausente.

`Referencia: ISO 31000:2018 apartado 6.2`

`Trampa: T-01 Qué etapa del proceso`

Q2 Respuesta correcta: **B.** Inclusiva: participación apropiada y oportuna de las partes interesadas para que se consideren sus conocimientos, opiniones y percepciones, lo que da lugar a una mayor toma de conciencia y a una gestión del riesgo más informada.

El capítulo 4(d), Inclusiva, es la participación apropiada y oportuna de las partes interesadas para que se consideren sus conocimientos, opiniones y percepciones, mejorando la toma de conciencia y una gestión del riesgo informada, exactamente lo que logró el responsable al convocar a las partes afectadas antes de que los criterios y la evaluación quedaran finalizados. La comunicación y consulta es la actividad del proceso (apartado 6.2) que operacionaliza la inclusividad, pero no es uno de los principios del capítulo 4 que pide la pregunta. Los factores humanos y culturales (capítulo 4(g), influencia conductual y cultural) y la mejor información disponible (capítulo 4(f), entradas de datos y sus limitaciones) también son principios del capítulo 4, pero las particularidades del escenario no los respaldan.

`Referencia: ISO 31000:2018, capítulo 4(d), Inclusiva`

`Trampa: T-02 Principio, marco de referencia o proceso`

Q3 Respuesta correcta: **A.** Qué riesgos asumirá y cuáles no, y en qué medida cada uno

Los criterios de riesgo expresan cuánto riesgo y qué tipo de riesgo está dispuesta a asumir una organización en relación con sus objetivos, de modo que la dirección tiene que decidir primero ese apetito. Una matriz comparada con el sector puede parecer rigurosa, pero hasta que no se define el apetito los umbrales no tienen significado para esta organización.

`Referencia: ISO 31000:2018, apartado 5.2`

`Trampa: T-03 Riesgo, consecuencia o probabilidad`

Q4 Respuesta correcta: **D.** Definir los criterios de riesgo frente a los cuales se valora la importancia del riesgo.

Todo depende del momento: el patrón de medida se está creando, no aplicando. El apartado 6.3.4 de ISO 31000:2018 define los criterios de riesgo como la cantidad y el tipo de riesgo que la organización puede o no puede asumir en relación con sus objetivos, además de los criterios utilizados para valorar la importancia; se fijan al inicio de la evaluación del riesgo, en coherencia con los objetivos y las políticas, y reflejan cómo se medirán las consecuencias y la probabilidad. Acordar las tolerancias de pérdida, las categorías de consecuencias inaceptables y la base de medición antes de que exista ningún riesgo que evaluar es precisamente esa actividad.

`Referencia: ISO 31000:2018 apartado 6.3.4`

`Trampa: T-01 Qué etapa del proceso`

Q5 Respuesta correcta: **A.** Dinámica, la gestión del riesgo responde de manera oportuna a los cambios en el contexto de la organización.

El principio e) Dinámica establece que los riesgos pueden surgir, cambiar o desaparecer a medida que cambia el contexto externo e interno de una organización, y que la gestión del riesgo anticipa, detecta, reconoce y responde a esos cambios de manera apropiada y oportuna. Una norma de localización de datos recién anunciada es un cambio en el contexto externo; añadir, evaluar y tratar ese riesgo fuera de ciclo, en lugar de esperar a la actualización anual, es esa respuesta oportuna. El seguimiento y la revisión (apartado 6.6) es la etapa del proceso que detectaría el cambio, no un principio. La mejora continua se refiere a la mejora del marco de referencia impulsada por el aprendizaje, y la mejor información disponible se refiere al origen y la vigencia de las entradas de información; ninguno de los dos describe el juicio sobre la oportunidad que aquí se realiza.

`Referencia: ISO 31000:2018 capítulo 4 (Principios), principio e) Dinámica`

`Trampa: T-02 Principio, marco de referencia o proceso`

Q6 Respuesta correcta: **B.** Retirar ambas exclusiones e incluir ambos elementos en el registro.

El apartado 6.4.2 indica que la organización debería identificar los riesgos, estén o no sus fuentes bajo su control, y enumera las 'fuentes de riesgo tangibles e intangibles' entre los factores a considerar, añadiendo que los resultados pueden tener 'consecuencias tangibles o intangibles'. Ninguno de los dos argumentos del responsable de riesgos es motivo para dejar un elemento fuera en la identificación, y dejar constancia de los motivos no cambia eso. La sequía queda fuera del control de la cooperativa, pero el apartado 6.5.2 sigue enumerando opciones de tratamiento como cambiar las consecuencias o compartir el riesgo. Aunque el daño a la promesa de marca de 'cultivo local' no pueda expresarse en dólares, el apartado 6.4.3 indica que las técnicas de análisis pueden ser cualitativas. Por tanto, deberían identificarse ambos elementos.

`Referencia: ISO 31000:2018, apartado 6.4.2`

`Trampa: T-03 Riesgo, consecuencia o probabilidad`

Q7 Respuesta correcta: **C.** Seleccionar un tratamiento adicional que se aplique junto con el doble abastecimiento.

El tratamiento del riesgo es iterativo: tras implementar una opción, el dueño juzga si el riesgo restante es aceptable frente a los criterios y, si no lo es, se aplica un tratamiento adicional. Aquí la exposición sigue superando el nivel tolerable fijado por el consejo, por lo que el dueño vuelve a la selección de opciones. El doble abastecimiento funcionó según lo diseñado y el riesgo era simplemente mayor de lo que una sola medida podía reducir, por lo que se añade una opción adicional junto a él en lugar de sustituirlo; las opciones de tratamiento no son necesariamente mutuamente excluyentes. Documentar, informar y programar la revisión mantienen visible el riesgo restante, pero registrar y revisar por sí solo es adecuado cuando no hay opciones de tratamiento disponibles o estas no modifican suficientemente el riesgo, no ante un remanente que era simplemente demasiado grande para una sola medida.

`Referencia: ISO 31000:2018, apartado 6.5`

`Trampa: T-01 Qué etapa del proceso`

Q8 Respuesta correcta: **B.** Valorar el marco de referencia de la gestión del riesgo: juzgar periódicamente si las disposiciones creadas para apoyar la toma de decisiones siguen logrando aquello para lo que se establecieron

Dos fronteras lo deciden. La valoración del marco de referencia (apartado 5.6) mide periódicamente el marco de referencia frente a su propósito y a lo que se esperaba que entregara, y juzga su idoneidad continuada: eso es el ejercicio de Thandi. El seguimiento y la revisión dentro del proceso verifican los riesgos, las evaluaciones del riesgo y los tratamientos, que ella deja deliberadamente al margen; la valoración del riesgo compara riesgos individuales con los criterios, algo que nunca llega a hacer. El homónimo es la trampa: «valoración» nombra tanto una actividad del marco de referencia como un paso del proceso, y solo el objeto que se juzga permite distinguirlos.

`Referencia: ISO 31000:2018, apartado 5.6`

`Trampa: T-02 Principio, marco de referencia o proceso`

Q9 Respuesta correcta: **D.** Evitar el riesgo

El apartado 6.5.2 enumera siete opciones de tratamiento del riesgo, que no son necesariamente mutuamente excluyentes. La primera es evitar el riesgo 'decidiendo no iniciar o no continuar con la actividad que da lugar al riesgo'. El dueño del riesgo interrumpió por completo la prueba de reparto con drones, por lo que los vuelos que dan lugar al riesgo de colisión ya no se realizan: eso es evitación. Ningún dron vuela sobre el puerto y la posibilidad de una colisión desaparece, pero ambas cosas se derivan de detener la actividad, no de un tratamiento aplicado a vuelos que continúan. Volver al servicio de reparto por carretera propio de la empresa no traspasa el riesgo a ninguna otra parte, por lo que no se comparte nada.

`Referencia: ISO 31000:2018 apartado 6.5.2`

`Trampa: T-03 Riesgo, consecuencia o probabilidad`

Q10 Respuesta correcta: **C.** Emitir una política que establezca el enfoque de la gestión del riesgo de la organización y asignar los recursos necesarios para gestionar el riesgo.

El apartado 5.2 de ISO 31000:2018 describe cómo la alta dirección y los órganos de supervisión demuestran el liderazgo y el compromiso: la personalización e implementación de todos los componentes del marco de referencia, la emisión de una declaración o política que establezca un enfoque de la gestión del riesgo, el aseguramiento de que se asignan los recursos necesarios para gestionar el riesgo y la asignación de autoridad, responsabilidad y obligación de rendir cuentas. El acto que cuenta es emitir la política, no redactarla: un especialista en riesgos, como un CRO, puede redactarla, pero emitirla y asignar los recursos son actos que realiza la propia alta dirección. El trabajo delegado de identificación y análisis, así como el análisis del contexto, son actividades de proceso y de diseño, y no esta demostración.

Referencia: ISO 31000:2018, apartado 5.2

Trampa: T-02 Principio, marco de referencia o proceso

¿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.