ISO/IEC 27001 Foundation: 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-foundation/.

PREGUNTA 1

Hollis & Brandt Accountants indica a su personal de oficina que guarde los papeles de los clientes y bloquee la pantalla de su equipo siempre que se ausente de su puesto. ¿Qué tema del Anexo A contiene el control que exige ambas reglas?

A. Personas

B. Físico

C. Tecnológico

PREGUNTA 2

Un equipo del SGSI fija un objetivo de crear una cultura en la que el personal notifique los errores de seguridad sin miedo, y no encuentra ninguna forma factible de medirlo. ¿Cuál de los siguientes sigue exigiendo el apartado 6.2 para este objetivo?

A. Aprobación como excepción por parte de la alta dirección

B. Una justificación registrada en la Declaración de Aplicabilidad

C. Seguimiento de su progreso a lo largo del tiempo

PREGUNTA 3

Una organización informa a todo el personal sobre su nueva política de seguridad y hace que su equipo de cortafuegos curse la formación de certificación del fabricante, y conserva sus certificados. ¿Qué apartado de ISO/IEC 27001:2022 cubre la formación del equipo?

A. Apartado 7.2 Competencia

B. Apartado 7.4 Comunicación

C. Apartado 7.3 Concienciación

PREGUNTA 4

El sistema documental de una empresa añade una marca oculta «Restringido» a las propiedades de cada archivo, de modo que su pasarela de correo electrónico puede impedir automáticamente que esos archivos salgan. ¿Qué control se implementa al añadir la marca?

A. Control 5.12 Clasificación de la información

B. Control 5.13 Etiquetado de la información

C. Control 5.14 Transferencia de la información

PREGUNTA 5

Una organización tiene previsto trasladar su base de datos de clientes a un nuevo proveedor de alojamiento el próximo trimestre. ¿Qué apartado de la norma ISO/IEC 27001:2022 exige que se realice una evaluación de los riesgos debido a este cambio?

A. Apartado 6.3 Planificación de los cambios

B. Apartado 6.1.2 Evaluación de los riesgos de seguridad de la información

C. Apartado 8.2 Evaluación de los riesgos de seguridad de la información

PREGUNTA 6

Durante un corte de electricidad, los servidores siguen funcionando con un generador de respaldo, pero el aire acondicionado de la sala de servidores no está conectado a él y se detiene, por lo que los servidores se sobrecalientan. ¿Qué control del Anexo A cubre MÁS directamente esta carencia?

A. Instalaciones de suministro

B. Emplazamiento y protección de equipos

C. Mantenimiento de los equipos

PREGUNTA 7

Un documento indica que las copias de seguridad de la información, el software y los sistemas deberían mantenerse y probarse periódicamente de acuerdo con la política temática específica sobre copias de seguridad. ¿De qué documento se trata?

A. ISO/IEC 27003

B. Anexo A de la ISO/IEC 27001

C. ISO/IEC 27002

PREGUNTA 8

La política de seguridad de la información de una empresa no dice nada sobre cómo se gestionan las solicitudes de excepción a la política. ¿Cómo debería clasificarse esta laguna?

A. Una desviación de la orientación de la ISO/IEC 27002

B. Una no conformidad con el apartado 5.2

C. Una no conformidad con el control 5.1 del Anexo A

PREGUNTA 9

¿Qué requisito de la ISO/IEC 27001 refleja de forma más directa el enfoque a procesos?

A. Incluir en el SGSI los procesos y sus interacciones

B. Definir y aplicar un proceso de evaluación de los riesgos

C. Considerar las interfaces y dependencias para el alcance

PREGUNTA 10

Un ransomware que llegó a un PC de oficina cifró todos los servidores de la empresa en el plazo de una hora. Cada dispositivo podía conectarse directamente con todos los demás. ¿Qué control habría limitado MÁS directamente hasta dónde se propagó?

A. Control 8.7 (controles contra el código malicioso)

B. Control 8.22 (segregación en redes)

C. Control 8.20 (seguridad de redes)

Respuestas

P1 Respuesta correcta: **B.** Físico

El Anexo A de ISO/IEC 27001:2022 sitúa las reglas de puesto de trabajo despejado y pantalla limpia (control 7.7) en el tema físico. Que el personal aplique las reglas, o que un software pueda bloquear las pantallas, no traslada el control al tema de personas ni al tema tecnológico.

`Referencia: ISO/IEC 27001:2022 Anexo A`

`Trampa: T-01 Controles parecidos`

P2 Respuesta correcta: **C.** Seguimiento de su progreso a lo largo del tiempo

El apartado 6.2 establece que los objetivos de seguridad de la información deben ser medibles si es factible, por lo que se admite un objetivo sólido que no puede medirse de forma razonable. Los demás requisitos del apartado siguen aplicándose a él, y el seguimiento es uno de ellos. El seguimiento consiste en mantenerse al tanto del estado, lo cual no depende de disponer de una cifra que comunicar.

`Referencia: ISO/IEC 27001:2022 apartado 6.2`

`Trampa: T-02 Requisito o buena práctica`

P3 Respuesta correcta: **A.** Apartado 7.2 Competencia

Una actividad puede parecerse a otra, así que hay que preguntarse qué consigue. Desarrollar las habilidades que necesita un rol, mediante educación, formación o experiencia, y conservar evidencias como los certificados es la competencia del apartado 7.2. Asegurarse de que las personas conozcan la política y su papel en el SGSI es la concienciación del apartado 7.3, y planificar qué se comunica, cuándo, con quién y cómo corresponde al apartado 7.4.

`Referencia: ISO/IEC 27001:2022 apartado 7.2`

`Trampa: T-03 Apartados vecinos`

P4 Respuesta correcta: **B.** Control 5.13 Etiquetado de la información

La clasificación (control 5.12) decide el nivel; el etiquetado (control 5.13) indica ese nivel en la información para que pueda reconocerse. La ISO/IEC 27002 incluye el apoyo a la automatización como parte de la finalidad del etiquetado y recomienda los metadatos para la información digital, de modo que los sistemas pueden tomar decisiones basadas en la etiqueta.

`Referencia: ISO/IEC 27002:2022 control 5.13`

`Trampa: T-01 Controles parecidos`

P5 Respuesta correcta: **C.** Apartado 8.2 Evaluación de los riesgos de seguridad de la información

La evaluación de los riesgos aparece dos veces en la norma ISO/IEC 27001:2022. El apartado 6.1.2, parte de la planificación, define el proceso y sus criterios. El apartado 8.2, parte de la operación, exige que las evaluaciones se realicen a intervalos planificados y siempre que se propongan o se produzcan cambios significativos, conservando los resultados como información documentada. Un traslado de alojamiento propuesto es exactamente ese tipo de desencadenante.

`Referencia: ISO/IEC 27001:2022 Apartado 8.2`

`Trampa: T-03 Apartados vecinos`

P6 Respuesta correcta: **A.** Instalaciones de suministro

Las instalaciones de suministro son más que la alimentación eléctrica de los servidores. ISO/IEC 27002 enumera la ventilación y el aire acondicionado junto con la electricidad, el agua y las telecomunicaciones. El control 7.11 del Anexo A exige que los recursos de tratamiento de la información estén protegidos contra las interrupciones causadas por fallos en los suministros, por lo que la refrigeración de los servidores también necesita protección frente a un corte de electricidad.

`Referencia: ISO/IEC 27002:2022 control 7.11`

`Trampa: T-01 Controles parecidos`

P7 Respuesta correcta: **C.** ISO/IEC 27002

El control 8.13 Copias de seguridad de la información tiene casi la misma redacción en ambos documentos, así que es el verbo el que decide. El Anexo A de la ISO/IEC 27001 lo formula con 'debe', la redacción propia de un requisito. La ISO/IEC 27002 lo formula con 'debería', la redacción propia de una orientación. La ISO/IEC 27003 también es un documento de orientación, pero abarca los capítulos del SGSI, no controles individuales.

`Referencia: ISO/IEC 27002:2022 control 8.13`

`Trampa: T-02 Requisito o buena práctica`

P8 Respuesta correcta: **A.** Una desviación de la orientación de la ISO/IEC 27002

El apartado 5.2 de la ISO/IEC 27001 establece los requisitos de contenido de la política de seguridad de la información, y la gestión de las excepciones no es uno de ellos. La ISO/IEC 27002 recomienda declaraciones adicionales, como la forma de gestionar las exenciones y las excepciones, pero su orientación no es obligatoria. Merece la pena subsanar la laguna, pero no es una no conformidad.

`Referencia: ISO/IEC 27002:2022 control 5.1`

`Trampa: T-02 Requisito o buena práctica`

P9 Respuesta correcta: **A.** Incluir en el SGSI los procesos y sus interacciones

El enfoque a procesos trata un sistema de gestión como un conjunto de procesos cuyas interacciones se identifican y se gestionan. El apartado 4.4 de la ISO/IEC 27001 lo refleja al exigir que el SGSI incluya los procesos necesarios y sus interacciones. Las interfaces del alcance (apartado 4.3) y el proceso de evaluación de los riesgos (apartado 6.1.2) también implican procesos o actividades, pero ninguno de los dos trata de cómo encajan entre sí los procesos del SGSI.

`Referencia: ISO/IEC 27001:2022 apartado 4.4`

`Trampa: T-03 Apartados vecinos`

P10 Respuesta correcta: **B.** Control 8.22 (segregación en redes)

El ransomware se propagó tanto porque nada se interponía entre los PC de oficina y los servidores. El control 8.22 del Anexo A exige que los grupos de servicios, usuarios y sistemas se mantengan separados dentro de las redes de la organización. La ISO/IEC 27002 describe la división de una red en dominios, como un dominio de equipos de escritorio y un dominio de servidores, con el tráfico entre ellos controlado en el perímetro.

`Referencia: ISO/IEC 27002:2022 control 8.22`

`Trampa: T-01 Controles parecidos`

¿Quiere el banco completo?

Mindset Prep tiene más de 3050 preguntas para siete exámenes 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.