CISSP Dominio 1: Gestión de riesgos y seguridad

Este dominio incluye preguntas de los siguientes temas:

• Terminología y principios de seguridad

• Tipos de control de protección

• Marcos de seguridad, modelos, estándares y mejores prácticas

• Leyes y delitos informáticos

• Propiedad intelectual

• Violaciones de datos

• Gestión de riesgos

• Modelado de amenazas

• Continuidad comercial y recuperación ante desastres

• Personal de Seguridad

• Gobernanza de seguridad

Las responsabilidades de un profesional de la seguridad se extienden mucho más allá de reaccionar a los titulares de noticias más recientes de un nuevo Exploit o violación de seguridad. Las responsabilidades diarias de los profesionales de la seguridad son mucho menos emocionantes en la superficie, pero son vitales para mantener a las organizaciones protegidas contra intrusiones para que no se conviertan en el próximo titular. La función de la seguridad dentro de una organización es compleja, ya que afecta a todos los empleados y debe gestionarse en toda la empresa. Es importante que comprenda la seguridad más allá de los detalles técnicos para incluir cuestiones de gestión y comerciales, tanto para el examen CISSP como para su función en el campo.

Conteste estas preguntas con la opción más correcta.

1 . ¿Cuál de las siguientes opciones describe mejor la relación entre COBIT e ITIL?

A. COBIT es un modelo de gobierno de TI, mientras que ITIL es un modelo de gobierno corporativo.

B. COBIT proporciona una hoja de ruta de gobierno corporativo, mientras que ITIL es un marco personalizable para la gestión de servicios de TI.

C. COBIT define los objetivos de TI, mientras que ITIL proporciona los pasos a nivel de proceso sobre cómo alcanzarlos.

D. COBIT proporciona un marco para lograr los objetivos comerciales, mientras que ITIL define un marco para lograr los objetivos de nivel de servicio de TI.

2 . Las organizaciones globales que transfieren datos a través de fronteras internacionales deben cumplir con las pautas y reglas de flujo de información transfronterizas desarrolladas por una organización internacional que ayuda a diferentes gobiernos a unirse y abordar los desafíos económicos, sociales y de gobernanza de una economía globalizada. ¿Qué organización es esta?

A. Comité de Organizaciones Patrocinadoras de la Comisión Treadway

B. La Organización de Cooperación y Desarrollo Económicos

C. COBIT

D. Organización Internacional de Normalización

3 . A Steve, un gerente de departamento, se le ha pedido que se una a un comité que es responsable de definir un nivel aceptable de riesgo para la organización, revisar la evaluación de riesgos y los informes de auditoría, y aprobar cambios significativos en las políticas y programas de seguridad. ¿A qué comité se une?

A. Comité de políticas de seguridad

B. Comité de auditoría

C. Comité de gestión de riesgos

D. Comité directivo de seguridad

4 . ¿Cuál de los siguientes no está incluido en una evaluación de riesgos?

A. Interrupción de actividades que presenten riesgo

B. Identificación de activos

C. Identificación de amenazas

D. Analizar el riesgo en orden de costo o criticidad

5 . ¿La integridad de los datos no está relacionada con cuál de los siguientes?

A. Manipulación no autorizada o cambios en los datos

B. La modificación de datos sin autorización

C. La sustitución intencional o accidental de datos

D. La extracción de datos para compartir con entidades no autorizadas

6 . Como CISO de su empresa, George necesita demostrarle a la junta directiva la necesidad de un programa sólido de gestión de riesgos. ¿Cuál de las siguientes opciones debería utilizar George para calcular el riesgo residual de la empresa?

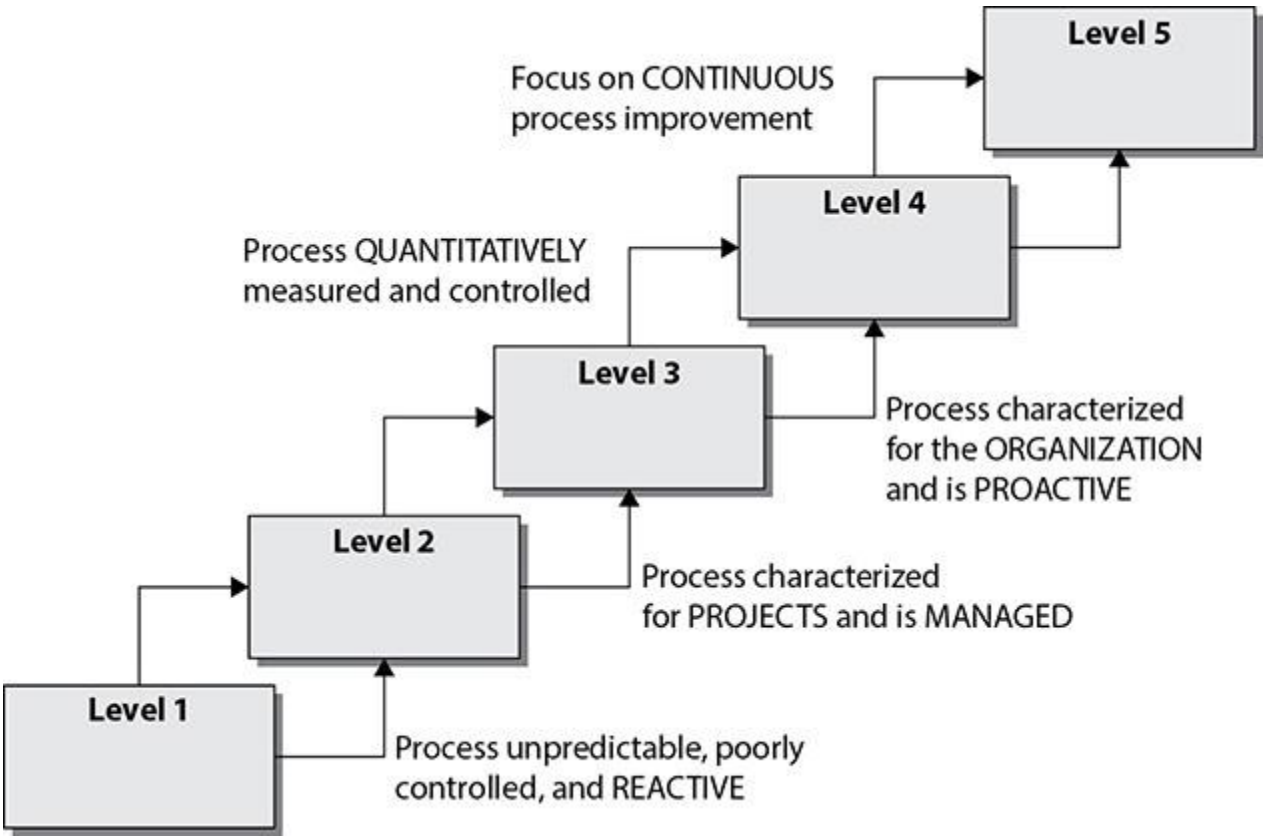
A. amenazas × vulnerabilidad × valor del activo = riesgo residual

B. SLE × frecuencia = ALE, que es igual al riesgo residual

C. (amenazas × vulnerabilidad × valor del activo) × brecha de controles = riesgo residual

D. (riesgo total - valor del activo) × contramedidas = riesgo residual

7 . La Integración del modelo de madurez de capacidades (CMMI) proviene del mundo de la ingeniería de software y se utiliza dentro de las organizaciones para ayudar a trazar un camino de cómo se pueden llevar a cabo las mejoras incrementales. Este modelo es utilizado por las organizaciones en la autoevaluación y para desarrollar pasos estructurados que se pueden seguir para que una organización pueda evolucionar de un nivel a otro y mejorar constantemente sus procesos. En el gráfico del modelo CMMI que se muestra, ¿cuál es la secuencia correcta de los niveles?



A. Inicial, definida, gestionada, gestionada cuantitativamente, optimización

B. Inicial, definida, gestionada cuantitativamente, optimización, gestionada

C. Definido, gestionado, gestionado cuantitativamente, optimizando

D. Inicial, repetible, definido, administrado cuantitativamente, optimizando

8 . La evaluación de riesgos tiene varias metodologías diferentes. ¿Cuál de las siguientes metodologías oficiales de riesgos no se creó con el fin de analizar los riesgos de seguridad?

A. FAP

B. OCTAVA

C. AS / NZS 4360

D. NIST SP 800-30

9 . ¿Cuál de las siguientes opciones no es una característica de una empresa que cuenta con un programa de gobierno de la seguridad?

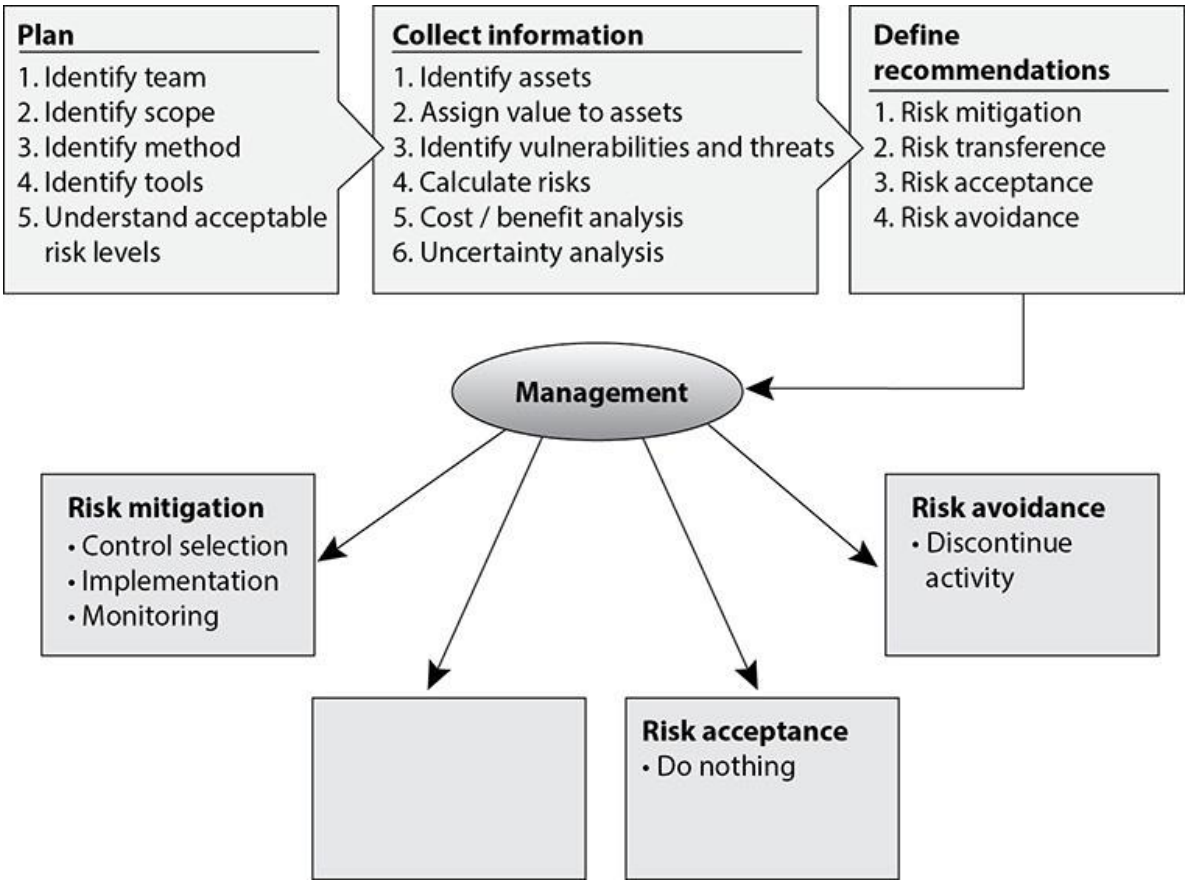
R. Los miembros de la junta reciben información actualizada trimestralmente sobre el estado de seguridad de la empresa.

B. Toda la actividad de seguridad se lleva a cabo dentro del departamento de seguridad.

C. Los productos, servicios y consultores de seguridad se implementan de manera informada.

D. La organización ha establecido métricas y objetivos para mejorar la seguridad.

10 . Hay cuatro formas de afrontar el riesgo. En el gráfico que sigue, ¿qué método falta y cuál es el propósito de este método?



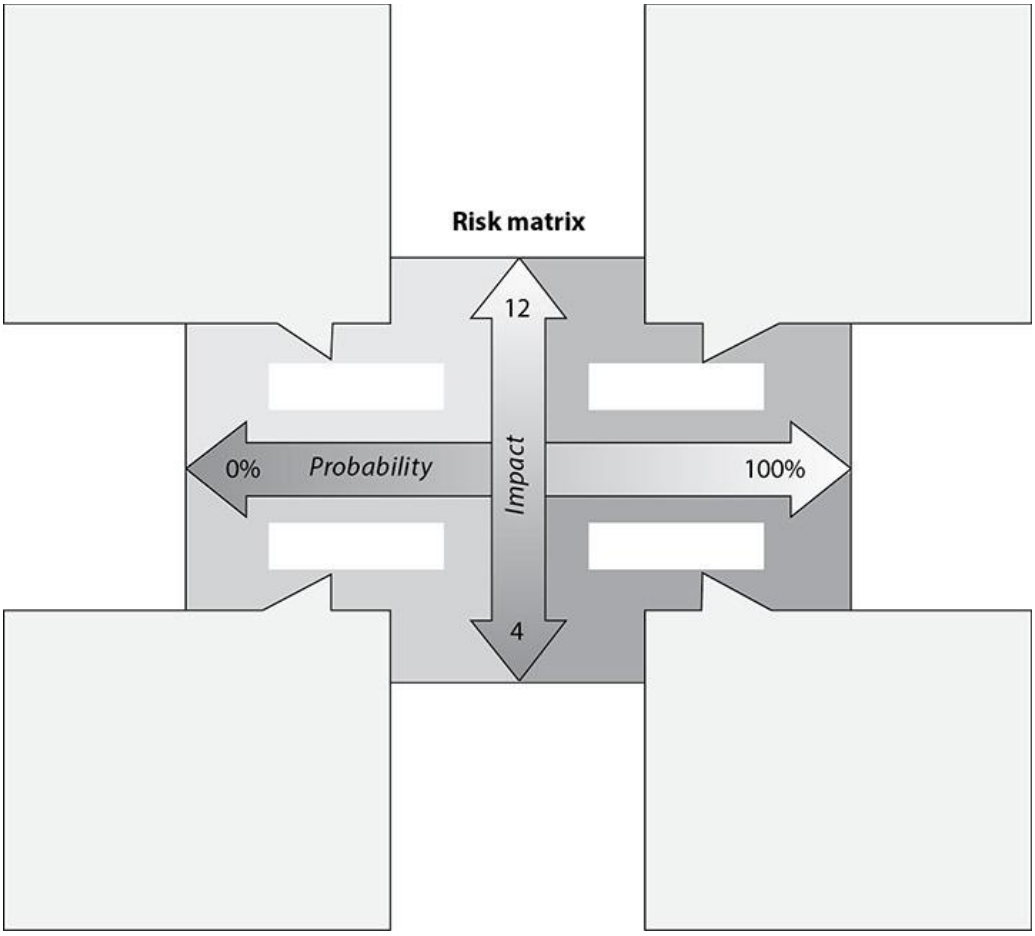
A. Transferencia de riesgo. Comparta el riesgo con otras entidades.

B. Reducción de riesgos. Reducir el riesgo a un nivel aceptable.

C. Riesgo de rechazo. Acepta el riesgo actual.

D. Asignación de riesgos. Asignar el riesgo a un propietario específico.

11 . El siguiente gráfico contiene un cuadro de mando de gestión de riesgos de uso común. Identifique el cuadrante adecuado y su descripción.



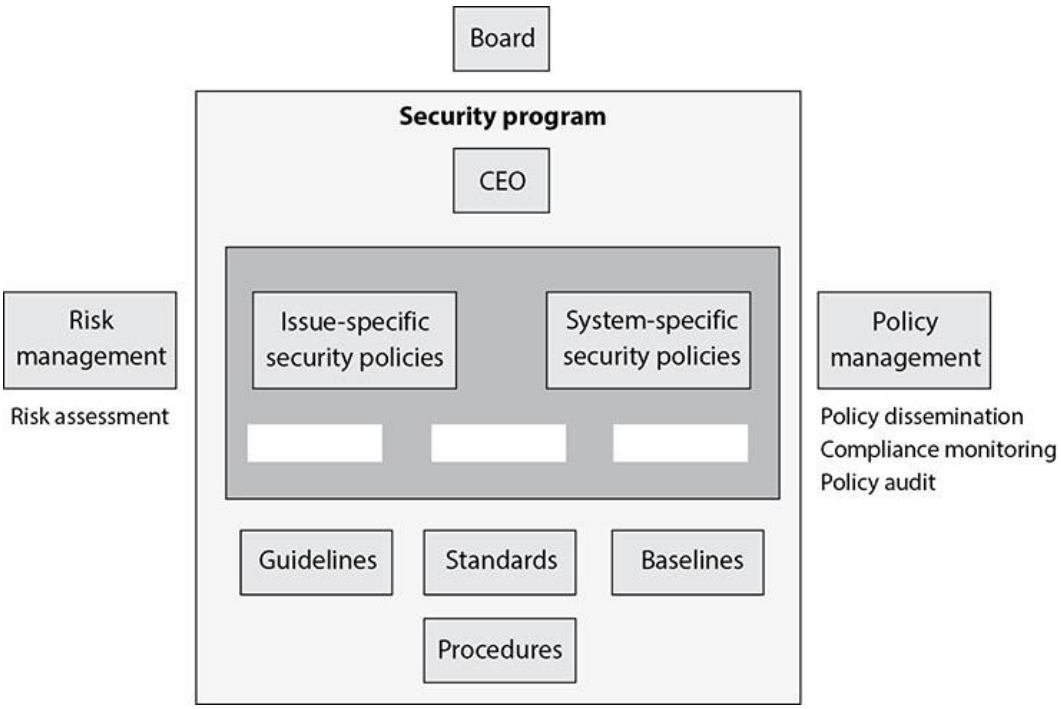
R. El cuadrante superior derecho es de alto impacto, baja probabilidad.

B. El cuadrante superior izquierdo es de alto impacto, probabilidad media.

C. El cuadrante inferior izquierdo es de bajo impacto, alta probabilidad.

D. El cuadrante inferior derecho es de bajo impacto, alta probabilidad.

12 . ¿Cuáles son los tres tipos de políticas que faltan en el siguiente gráfico?



A. Regulatorio, informativo, consultivo

B. Regulatorio, Obligatorio, Asesor

C. Regulatorio, Informativo, Público

D. Uso reglamentario, informativo e interno

13 . Enumere en el orden correcto de la tabla que se muestra los objetivos de aprendizaje que faltan y sus definiciones adecuadas.

	Awareness	Training	Education
Attribute:	"What"	"How"	"Why"
Level:	Information	Knowledge	Insight
Learning objective:			
Example teaching method:	**Media** • Videos • Newsletters • Posters	**Practical instruction** • Lecture and/or demo • Case study • Hands-on practice	**Theoretical instruction** • Seminar and discussion • Reading and study • Research
Test measure:	True/False Mutiple choice (Identify learning)	Problem solving, i.e., recognition and resolution (Apply learning)	Essay (Interpret learning)
Impact timeframe:	Short-term	Intermediate	Long-term

A. Comprensión, reconocimiento y retención, habilidad

B. Habilidad, reconocimiento y retención, habilidad

C. Reconocimiento y retención, habilidad, comprensión

D. Habilidad, reconocimiento y retención, comprensión

14 . ¿Qué tipo de enfoque de análisis de riesgos proporciona el siguiente gráfico?

High	7–10	7–10
Medium	4–6	4–6
Low	0–3	0–3

0	10	20	30	40	50	60	70	80	90	100
0	9	18	27	36	45	54	63	72	81	90
0	8	16	24	32	40	48	56	64	72	80
0	7	14	21	28	35	42	49	56	63	70
0	6	12	18	24	30	36	42	48	54	60
0	5	10	15	20	25	30	35	40	45	50
0	4	8	12	16	20	24	28	32	36	40
0	3	6	9	12	15	18	21	24	27	30
0	2	4	6	8	10	12	14	16	18	20
0	1	2	3	4	5	6	7	8	9	10

41–100	High
20–40	Medium
0–19	Low

A. Cuantitativo

B. Cualitativo

C. Operacionalmente correcto

D. Operacionalmente crítico

15 . ISO / IEC 27000 es parte de una familia creciente de estándares de sistemas de gestión de seguridad de la información (SGSI) ISO / IEC. Comprende estándares de seguridad de la información publicados conjuntamente por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC). ¿Cuál de los siguientes proporciona un mapeo incorrecto de los estándares individuales que componen esta familia de estándares?

A. ISO / IEC 27002: Código de prácticas para la gestión de la seguridad de la información

B. ISO / IEC 27003: Directriz para la implementación del SGSI

C. ISO / IEC 27004: Directriz para el marco de medición y métricas de la gestión de la seguridad de la información

D. ISO / IEC 27005: Directriz para organismos que realizan auditorías y certificaciones de sistemas de gestión de seguridad de la información.

El siguiente escenario se aplica a las preguntas 16 y 17.

Sam es el gerente de seguridad de una empresa que obtiene la mayor parte de sus ingresos de su propiedad intelectual. Sam ha implementado un programa de mejora de procesos que ha sido certificado por una entidad externa. Su empresa recibió un Nivel 2 durante un proceso de evaluación y él está tomando medidas para aumentarlo a un Nivel 3. Hace un año, cuando Sam llevó a cabo un análisis de riesgo, determinó que la empresa corría demasiado riesgo cuando llegó a perder potencialmente secretos comerciales. La contramedida que implementó su equipo redujo este riesgo, y Sam determinó que la expectativa de pérdida anualizada del riesgo de que un secreto comercial sea robado una vez en un período de cien años es ahora de $ 400.

16 . ¿Cuál de los siguientes es el criterio según el cual la empresa de Sam probablemente fue certificada?

A. SABSA

B. Integración del modelo de madurez de la capacidad

C. Biblioteca de infraestructura de tecnología de la información

D. Prince2

17 . ¿Cuál es el valor de expectativa de pérdida única asociado en este escenario?

A. $ 65 000

B. $ 400 000

C. $ 40 000

D. $ 4.000

18 . La organización NIST ha definido las mejores prácticas para crear planes de continuidad. ¿Cuál de las siguientes fases se ocupa de identificar y priorizar funciones y sistemas críticos?

A. Identificar controles preventivos.

B. Desarrollar la declaración de política de planificación de la continuidad.

C. Crear estrategias de contingencia.

D. Realizar el análisis de impacto comercial.

19 . Como coordinador de continuidad del negocio de su empresa, Matthew es responsable de ayudar a reclutar miembros para el comité de planificación de la continuidad del negocio (BCP). ¿Cuál de las siguientes opciones no describe correctamente este esfuerzo?

A. Los miembros del comité deben participar en las etapas de planificación, así como en las etapas de prueba e implementación.

B. Cuanto más pequeño sea el equipo, mejor será el control de las reuniones.

C. El coordinador de continuidad del negocio debe trabajar con la gerencia para nombrar a los miembros del comité.

D. El equipo debe estar formado por personas de diferentes departamentos de la empresa.

20 . Un análisis de impacto empresarial se considera un análisis funcional. ¿Cuál de las siguientes opciones no se lleva a cabo durante un análisis de impacto empresarial?

A. Una prueba de interrupción completa o en paralelo

B. La aplicación de un esquema de clasificación basado en niveles de criticidad

C. La recopilación de información mediante entrevistas

D. Documentación de las funciones comerciales

21 . ¿Cuál de los siguientes pasos es el primero en un análisis de impacto empresarial?

A. Calcule el riesgo para cada función comercial diferente.

B. Identificar las funciones comerciales críticas.

C. Crear técnicas de recopilación de datos.

D. Identificar vulnerabilidades y amenazas a las funciones comerciales.

22 . No es inusual que los planes de continuidad del negocio queden obsoletos. ¿Cuál de las siguientes opciones no es una razón por la que los planes se vuelven obsoletos?

A. Cambios en hardware, software y aplicaciones

B. Cambios en la infraestructura y el medio ambiente

C. Rotación de personal

D. Que el proceso de continuidad del negocio esté integrado en el proceso de gestión del cambio.

23 . Los procedimientos de continuidad del negocio planificados de antemano brindan a las organizaciones una serie de beneficios. ¿Cuál de las siguientes opciones no es una capacidad habilitada por la planificación de la continuidad del negocio?

A. Reanudación de funciones comerciales críticas

B. Informar a los socios comerciales que su empresa no está preparada

C. Proteger vidas y garantizar la seguridad

D. Garantizar la supervivencia de la empresa

24 . El apoyo a la gestión es fundamental para el éxito de un plan de continuidad empresarial. ¿Cuál de los siguientes es el más importante que debe proporcionarse a la gerencia para obtener su apoyo?

A. Caso de negocio

B. Análisis de impacto empresarial

C. Análisis de riesgos

D. Informe de amenazas

25 . ¿Cuál de los siguientes es un primer paso fundamental en la recuperación ante desastres y la planificación de contingencias?

A. Planifique las pruebas y los simulacros.

B. Complete un análisis de impacto empresarial.

C. Determinar alternativas de instalaciones de respaldo fuera del sitio.

D. Organizar y crear documentación relevante.

26 . ¿Cuál de las siguientes opciones no es motivo para desarrollar e implementar un plan de recuperación ante desastres?

A. Proporcione los pasos para una recuperación posterior a un desastre.

B. Amplíe las operaciones de respaldo para incluir más que simplemente respaldar datos.

C. Describir las funciones y los sistemas comerciales.

D. Proporcionar procedimientos para respuestas de emergencia.

27 . ¿Con qué fase de un plan de continuidad empresarial procede una empresa cuando está lista para volver a su sitio original oa un sitio nuevo?

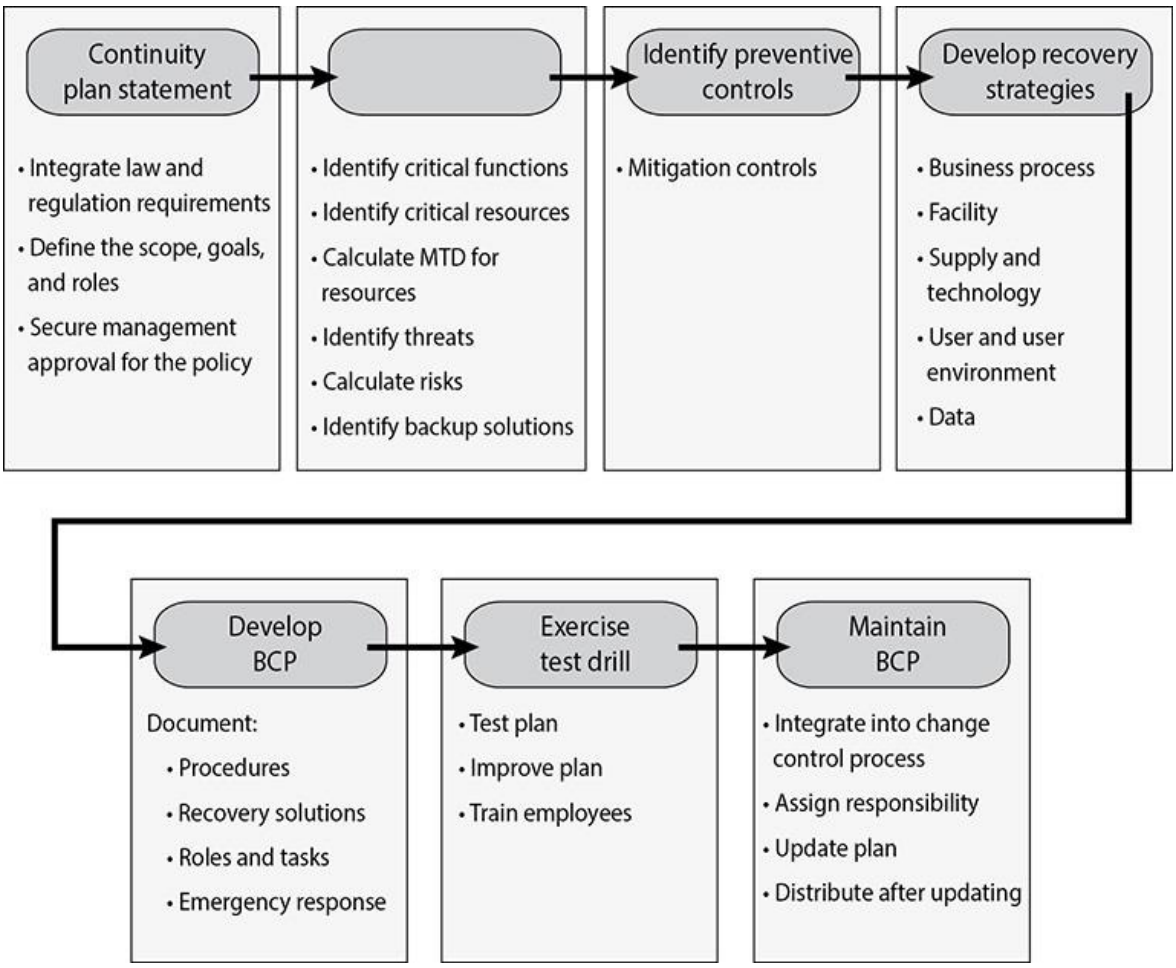
A. Fase de reconstitución

B. Fase de recuperación

C. Fase de inicio del proyecto

D. Fase de evaluación de daños

28 . ¿Cuál es el segundo paso que falta en el gráfico que sigue?



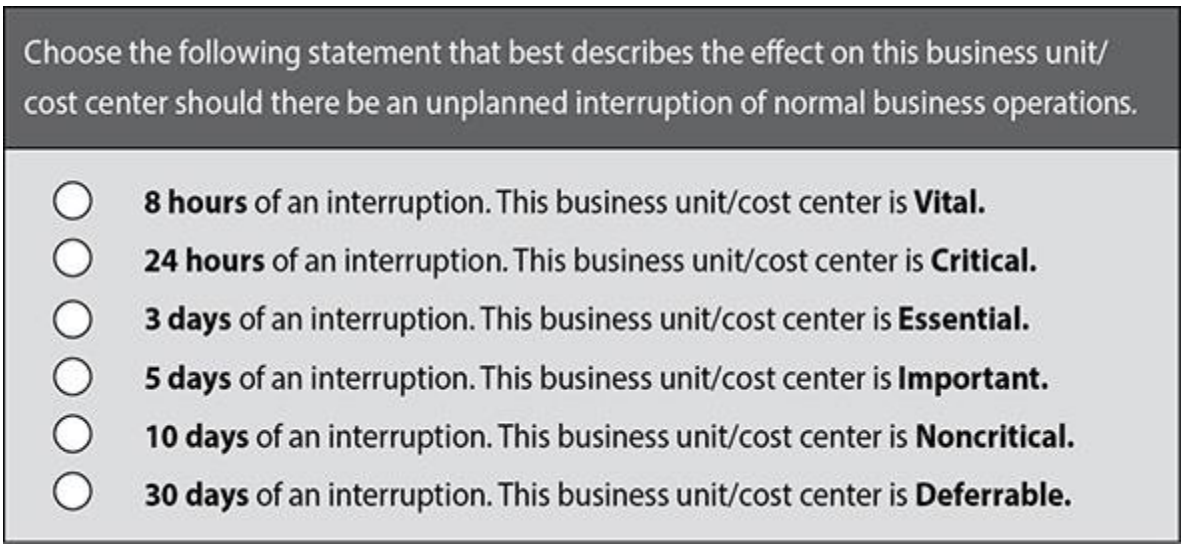
A. Identificar al coordinador de continuidad

B. Análisis de impacto empresarial

C. Identificar el comité de BCP

D. Identificación de la dependencia

29 . Las diferentes amenazas deben evaluarse y clasificarse en función de la gravedad del riesgo comercial al desarrollar un BCP. ¿Qué enfoque de clasificación se ilustra en el gráfico siguiente?



A. Tiempo medio para reparar

B. Tiempo medio entre fallos

C. Máximo tiempo de inactividad crítico

D. Máximo tiempo de inactividad tolerable

30 . Sean ha sido contratado como coordinador de continuidad empresarial. La gerencia le ha dicho que debe asegurarse de que la empresa cumpla con el estándar ISO / IEC que se refiere a la preparación de la tecnología para la continuidad del negocio. También se le ha instruido para que encuentre una manera de transferir el riesgo de no poder llevar a cabo funciones comerciales críticas durante un período de tiempo debido a un desastre. ¿Cuál de los siguientes es más probable que sea el estándar que se le ha pedido a Sean que cumpla?

A. ISO / IEC 27031

B. ISO / IEC 27005

C. ISO / IEC BS7799

D. ISO / IEC 2899

31 . ¿Qué organización se ha desarrollado para tratar los problemas económicos, sociales y de gobernanza y cómo se transportan los datos confidenciales a través de las fronteras?

A. Unión Europea

B. Consejo de Europa

C. Puerto seguro

D. Organización de Cooperación y Desarrollo Económicos

32 . Widgets, Inc. desea proteger su logotipo del uso no autorizado. ¿Cuál de las siguientes opciones protegerá el logotipo y garantizará que otros no puedan copiarlo y usarlo?

A. Patente

B. Copyright

C. Marca registrada

D. Secreto comercial

33 . ¿Cuál de las siguientes opciones significa que una empresa hizo todo lo que razonablemente pudo haber hecho para evitar una violación de la seguridad?

A. Responsabilidad posterior

B. Responsabilidad

C. Debida diligencia

D. Debido cuidado

34 . ¿Cuál de las siguientes es una ley de derechos de autor de EE. UU. que penaliza la producción y difusión de tecnología, dispositivos o servicios que eluden las medidas de control de acceso implementadas para proteger el material con derechos de autor?

A. Ley de derechos de autor

B. Ley de derechos de autor del milenio digital

C. Ley Federal de Privacidad

D. SOPA

35 . ¿Qué papel juega la Junta de Arquitectura de Internet con respecto a la tecnología y la ética?

A. Crea pautas de sentencia penal.

B. Emite declaraciones relacionadas con la ética sobre el uso de Internet.

C. Edita la Solicitud de comentarios.

D. Mantiene los Diez Mandamientos de la Ética Informática.

36 . Como candidato a CISSP, debe firmar un Código de Ética. ¿Cuál de los siguientes es delCódigo de Ética(ISC)^2 para el CISSP?

A. La información debe compartirse libre y abiertamente; por lo tanto, compartir información confidencial debe ser ético.

B. Piense en las consecuencias sociales del programa que está escribiendo o del sistema que está diseñando.

C. Actuar de manera honorable, honesta, justa, responsable y legal.

D. No participe en experimentos en Internet de manera negligente.

37 . ¿Cuál de los siguientes fue el primer tratado internacional que buscó abordar los delitos informáticos mediante la coordinación de las leyes nacionales y la mejora de las técnicas de investigación y la cooperación internacional?

A. Council of Global Convention on Cybercrime

B. Convenio del Consejo de Europa sobre el delito cibernético

C. Organización de Cooperación y Desarrollo Económicos

D. Organización para la cooperación y el desarrollo en materia de ciberdelincuencia

38 . Lee es un nuevo gerente de seguridad que está a cargo de garantizar que su empresa cumpla con los Principios de Privacidad de la Unión Europea cuando su empresa interactúa con sus socios europeos. ¿El conjunto de principios que trata sobre la transmisión de datos considerados privados se engloba dentro de cuál de las siguientes leyes o regulaciones?

A. Directiva de protección de datos

B. Organización de Cooperación y Desarrollo Económicos

C. Factura privada federal

D. Ley de protección de la privacidad

39 . Brandy no pudo entender cómo Sam obtuvo acceso no autorizado a su sistema, ya que tiene poca experiencia en computadoras. ¿Cuál de los siguientes es el ataque más probable que utilizó Sam?

A. Ataque de diccionario

B. Ataque de surf de hombro

C. Ataque de canal encubierto

D. Ataque cronometrado

40 . Jane ha sido encargada de garantizar que la privacidad de la información médica personal de los clientes esté adecuadamente protegida antes de intercambiarla con un nuevo socio europeo. ¿Qué requisitos de seguridad de datos debe cumplir?

A. HIPAA

B. NIST SP 800-66

C. Puerto seguro

D. Principios de privacidad de la Unión Europea

41 . A Sue se le ha encomendado la tarea de implementar una serie de controles de seguridad, incluido el software antivirus y antispam, para proteger el sistema de correo electrónico de la empresa. ¿Qué tipo de enfoque está adoptando su empresa para manejar el riesgo que representa el sistema?

A. Mitigación de riesgos

B. Aceptación de riesgos

C. Evitación de riesgos

D. Transferencia de riesgo

42 . Se deben considerar varios factores al asignar valores a los activos. ¿Cuál de los siguientes no se utiliza para determinar el valor de un activo?

A. El valor del activo en el mercado externo

B. El nivel de seguro requerido para cubrir el activo.

C. Los costos iniciales y salientes de compra, licencia y soporte del activo.

D. El valor del activo para las operaciones de producción de la organización.

43 . El marco de arquitectura de Zachman se utiliza a menudo para configurar una arquitectura de seguridad empresarial. ¿Cuál de las siguientes opciones no describe correctamente el marco de Zachman?

A. Un modelo bidimensional que utiliza interrogantes de comunicación que se cruzan con diferentes niveles.

B. Un modelo orientado a la seguridad que da instrucciones de forma modular

C. Se utiliza para construir una arquitectura empresarial robusta frente a una arquitectura de seguridad técnica

D. Utiliza seis perspectivas para describir una infraestructura de información holística

44 . Se le ha dicho a John que informe a la junta directiva con un marco de arquitectura empresarial independiente del proveedor que ayudará a la empresa a reducir la fragmentación que resulta de la desalineación de los procesos de TI y de negocios. ¿Cuál de los siguientes marcos debería sugerir?

A. DoDAF

B. CMMI

C. ISO / IEC 42010

D. TOGAF

45 . La Biblioteca de Infraestructura de Tecnología de la Información (ITIL) consta de cinco juegos de libros instructivos. ¿Cuál de los siguientes se considera el conjunto básico y se centra en la planificación general de los servicios de TI previstos?

A. Operación del servicio

B. Diseño de servicios

C. Transición del servicio

D. Estrategia de servicio

46 . Sarah y su equipo de seguridad han llevado a cabo muchas pruebas de vulnerabilidad a lo largo de los años para localizar las debilidades y vulnerabilidades dentro de los sistemas de la red. El CISO le ha pedido que supervise el desarrollo de un modelo de amenazas para la red. ¿Cuál de las siguientes opciones describe mejor qué es este modelo y para qué se utilizaría?

R. Un modelo de amenaza puede ayudar a evaluar la probabilidad, el daño potencial y la prioridad de los ataques, y así ayudar a minimizar o erradicar las amenazas.

B. Un modelo de amenaza combina el resultado de las diversas pruebas de vulnerabilidad y las pruebas de penetración realizadas para comprender la postura de seguridad de la red en su conjunto.

C. Un modelo de amenaza es un modelo basado en riesgos que se utiliza para calcular las probabilidades de los diversos riesgos identificados durante las pruebas de vulnerabilidad.

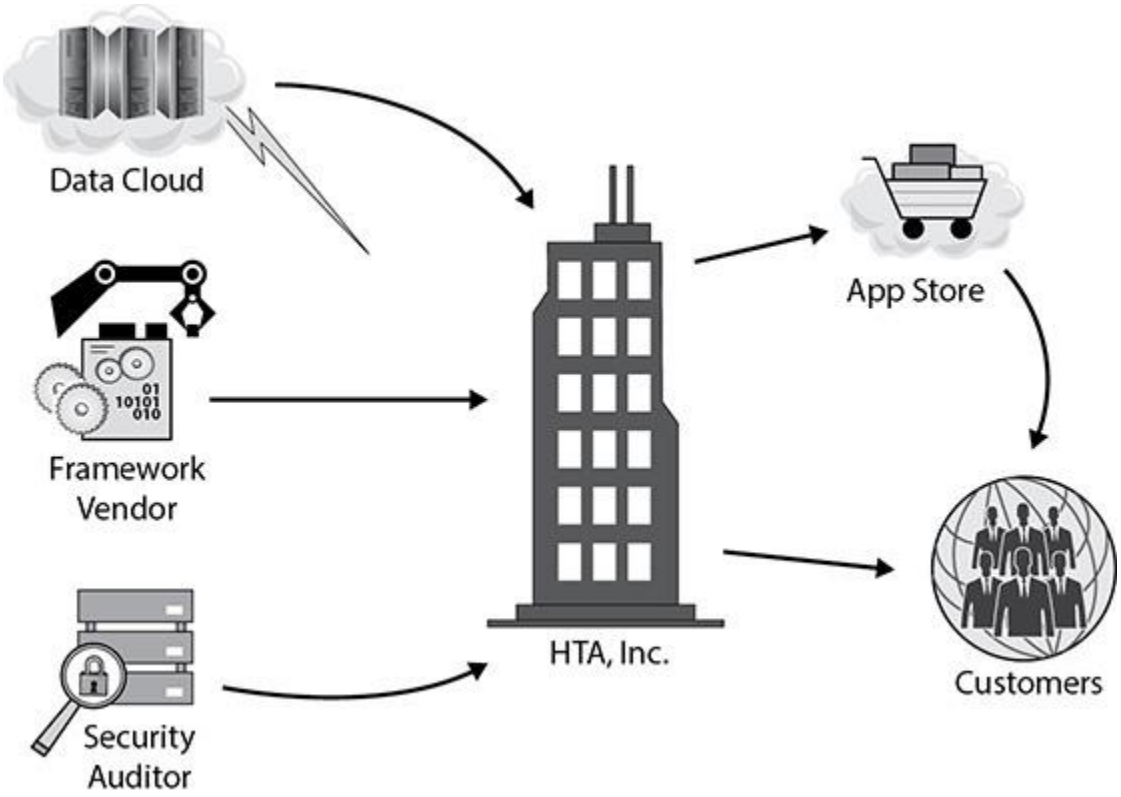
D. Se utiliza un modelo de amenaza en las prácticas de desarrollo de software para descubrir errores de programación.

El siguiente escenario se aplica a las preguntas 47 a 51.

Health Tracking Apps, Inc. (HTA) es una corporación con sede en EE. UU. Que desarrolla y vende aplicaciones que sus clientes pueden usar para rastrear varios aspectos de su propia salud, desde sus regímenes diarios de ejercicio hasta varios resultados de pruebas médicas y estadísticas comparativas a lo largo del tiempo. Estas aplicaciones utilizan almacenamiento basado en la nube para que los clientes puedan acceder a sus datos desde múltiples plataformas, incluidos dispositivos móviles inteligentes y sistemas de escritorio. Los clientes también pueden compartir fácilmente los datos que generan las aplicaciones con sus entrenadores personales y proveedores de atención médica si así lo desean, mediante suscripción.

Los productos de HTA están disponibles en varios idiomas, incluidos inglés, francés, español, alemán e italiano. Todo el software de HTA es desarrollado por un personal dedicado dentro de los Estados Unidos, aunque HTA ocasionalmente contrata pasantes de la universidad local para ayudar con las traducciones de idiomas para sus diversas interfaces de usuario.

El siguiente diagrama de relación entre entidades ilustra las dependencias del modelo de negocio de HTA:



47 . ¿Se le exigirá a HTA que cumpla con el Reglamento general de protección de datos (RGPD)? Si es así, ¿por qué? Si no es así, ¿por qué?

1. Tal vez, porque los registros de recursos humanos de HTA podrían contener datos de privacidad protegidos sobre ciudadanos europeos si alguno de los pasantes de HTA son estudiantes que estudian en el extranjero.

2. No, porque el RGPD se aplica solo a las empresas con sede en Europa.

3. Sí, en la medida en que los datos privados almacenados por HTA incluyen los de cualquier cliente europeo.

4. No, porque los datos privados sobre ciudadanos europeos que contienen los registros de clientes y RR.HH. de HTA se almacenan en los Estados Unidos.

A. Declaración 2 solamente

B. Declaración 4 solamente

C. Ambas declaraciones 1 y 3

D. Solo estado 3

48 . Los datos del cliente de HTA se violan a través de una vulnerabilidad en su interfaz de programación de aplicaciones (API). Se descubre que esta vulnerabilidad es el resultado de una falla de seguridad recientemente anunciada en el marco de Java subyacente que HTA usa para el desarrollo de sus aplicaciones. ¿Cuál de las siguientes opciones describe mejor la raíz de este problema?

A. HTA no logró gestionar los riesgos asociados con su cadena de suministro.

B. HTA no aplicó un parche crítico de manera oportuna.

C. HTA almacenó datos críticos / sensibles en una nube.

D. HTA eligió un lenguaje y un marco de riesgo para su desarrollo.

49 . HTA almacena los datos privados de sus clientes en una nube de terceros. ¿Cuál es el medio principal a través del cual HTA puede garantizar que su proveedor de servicios en la nube mantenga el cumplimiento de las regulaciones, incluido el GDPR, si es necesario, al que está sujeto HTA?

A. Hacer cumplir un acuerdo a nivel empresarial (ELA) que especifique cómo el proveedor de servicios debe realizar las actividades de aseguramiento.

B. Hacer cumplir un acuerdo de nivel de servicio (SLA) que especifica sanciones contractuales por incumplimiento del proveedor de servicios.

C. Realice una inspección in situ de las instalaciones del proveedor de servicios para asegurarse de que cumplan con las normas.

D. Revise el programa de seguridad del proveedor de servicios.

50 . Muchos de los empleados de HTA tienen acceso directo o indirecto a los datos privados de sus clientes. HTA debe asegurarse de que los empleados recién contratados conozcan todas las políticas y procedimientos de seguridad que se les aplican, tengan solo el acceso necesario a través de las cuentas creadas para ellos y hayan firmado un acuerdo para no divulgar los datos de manera inapropiada. ¿Cuál de los siguientes términos describe este proceso?

A. Debida diligencia

B. Seguridad del personal

C. Acuerdo de no divulgación (NDA)

D. Incorporación

51 . HTA tiene un programa de concientización diseñado para educar a todos los empleados sobre los problemas relevantes para la seguridad que se les aplican, según su función. Los miembros del personal de TI reciben instrucciones específicas de que es importante estar al tanto de las nuevas vulnerabilidades a medida que se descubren, no solo en los sistemas operativos que usa HTA, sino también en las aplicaciones y marcos que los desarrolladores usan para construir su software. El programa de concientización también enfatiza la importancia de una rápida mitigación por parte del personal de TI. Como se indica en la pregunta 48, los datos del cliente de HTA se han violado a través de una vulnerabilidad en su API, una vulnerabilidad que se descubrió como resultado de una falla de seguridad anunciada recientemente en el marco de trabajo subyacente de Java que HTA usa para el desarrollo de sus aplicaciones. ¿Cuál de las siguientes opciones contribuyó con mayor probabilidad a la infracción con respecto al programa de concienciación sobre seguridad?

R. HTA no ha realizado revisiones periódicas del contenido del programa de concientización sobre seguridad.

B. La evaluación de la eficacia del programa ha sido insuficiente.

C. Los empleados no están debidamente capacitados.

D. El programa de concientización sobre seguridad no fue relevante para la violación.