CISSP Dominio 2 - Seguridad de Activos

Este dominio incluye preguntas de los siguientes temas:

• Ciclo de vida de la información

• Clasificación y protección de la información

• Propiedad de la información

• Protección de la privacidad

• Retención de información

• Controles de seguridad de datos

• Requisitos de manejo de datos

Si bien el Dominio 1 prepara el escenario para la base de cómo se deben construir y administrar los programas de seguridad, el objetivo de los programas de seguridad es proteger completamente los activos identificados como críticos para la empresa. Para hacer esto de manera eficaz, y especialmente rentable, es necesario comprender la naturaleza de lo que debe protegerse, por qué debe protegerse y cómo protegerlo. El dominio 2 se centra en comprender qué activos de información deben protegerse y por qué, y cómo categorizar su valor para la priorización de los controles de seguridad que se implementarán a lo largo del ciclo de vida de cada activo.

Elija la mejor respuesta a estas preguntas

1 . Como jefe de ventas, Jim es el propietario de los datos del departamento de ventas. ¿Cuál de las siguientes opciones no es responsabilidad de Jim como propietario de los datos?

A. Asignación de clasificaciones de información

B. Dictar cómo se deben proteger los datos

C. Verificación de la disponibilidad de datos

D. Determinar cuánto tiempo se van a retener los datos

2 . La asignación de niveles de clasificación de datos puede ayudar con todo lo siguiente excepto:

A. La agrupación de información clasificada con seguridad jerárquica y restrictiva

B. Asegurarse de que los datos no sensibles no estén protegidos por controles innecesarios

C. Extraer datos de una base de datos

D. Reducir los costos de proteger los datos

3 . Susan, una abogada, ha sido contratada para ocupar un nuevo puesto en Widgets, Inc .: directora de privacidad (CPO). ¿Cuál es la función principal de su nuevo rol?

A. Garantizar la protección de los datos de los socios

B. Garantizar la precisión y protección de la información financiera de la empresa

C. Asegurar que las políticas de seguridad se definan y se cumplan

D. Garantizar la protección de los datos de clientes, empresas y empleados

4 . Jared juega un papel en el sistema de clasificación de datos de su empresa. En esta función, debe tener el debido cuidado al acceder a los datos y asegurarse de que los datos se utilicen solo de acuerdo con la política permitida, respetando las reglas establecidas para la clasificación de los datos. Él no determina, mantiene ni evalúa los controles, entonces, ¿cuál es el papel de Jared?

A. Propietario de los datos

B. Custodio de datos

C. Usuario de datos

D. Auditor de sistemas de información

5 . Michael está encargado de desarrollar un programa de clasificación de datos para su empresa. ¿Cuál de las siguientes cosas debería hacer primero?

A. Comprender los diferentes niveles de protección que se deben brindar.

B. Especifique los criterios de clasificación de datos.

C. Identificar a los custodios de los datos.

D. Determinar los mecanismos de protección para cada nivel de clasificación.

6 . ¿Cuál de los siguientes NO es un factor para determinar la sensibilidad de los datos?

A. Quién debería tener acceso a los datos

B. El valor de los datos

C. Cómo se utilizarán los datos

D. El nivel de daño que se podría causar si los datos estuvieran expuestos.

7 . ¿Cuál es la principal responsabilidad de seguridad de un propietario de datos?

A. Determinar cómo se deben conservar los datos

B. Determinación de la clasificación de datos

C. Determinación del valor de los datos

D. Determinar cómo se utilizarán los datos

8 . ¿Cuál es la técnica más valiosa para determinar si se debe implementar un control de seguridad específico?

A. Análisis de riesgo

B. Análisis de costo / beneficio

C. Resultados de ALE

D. Identificar las vulnerabilidades y amenazas que causan el riesgo.

9 . ¿Cuál de las siguientes es la etapa MENOS importante en la gestión del ciclo de vida de la información?

A. Especificación y clasificación de datos

B. Supervisión y auditoría continuas del acceso a los datos

C. Archivo de datos

D. Migración de bases de datos

10 . ¿Cuáles de los siguientes son métodos efectivos para prevenir la remanencia de datos en dispositivos de estado sólido (SSD)?

I. Claro

ii. Purga

iii. Desmagnetización

iv. Destrucción

A. i, ii

B. i, iii, iv

C. iv

D. Todo lo anterior

11 . El requisito de borrado es el final del ciclo de vida de los medios si los medios contienen información confidencial. ¿Cuál de las siguientes opciones describe mejor la purga?

A. Cambiar la polarización de los átomos en los medios.

B. Es inaceptable que los medios se reutilicen en el mismo entorno físico para los mismos fines.

C. Los datos que se encontraban anteriormente en los medios se vuelven irrecuperables sobrescribiéndolos con un patrón.

D. La información se vuelve irrecuperable, incluso con un esfuerzo extraordinario.

12 . Sam planea establecer un servicio de telefonía móvil utilizando la información personal que le ha robado a su antiguo jefe. ¿Qué tipo de robo de identidad es este?

A. Phishing

B. Nombre verdadero

C. Pharming

D. Adquisición de cuenta

13 . ¿Cuáles de las siguientes son categorías militares comunes de clasificación de datos?

A. Alto secreto, secreto, clasificado, sin clasificar

B. Alto secreto, secreto, confidencial, privado

C. Alto secreto, secreto, confidencial, sin clasificar

D. Clasificados, no clasificados, públicos

14 . Joan necesita documentar un esquema de clasificación de datos para su organización. ¿Qué criterios debería utilizar para guiar sus decisiones?

A. El valor de los datos y la antigüedad de los datos

B. Responsabilidades legales basadas en regulaciones ISO

C. ¿Quién será responsable de proteger los datos y cómo

D. Cómo se manejaría una violación de datos adversa

15 . ¿Cuál de los siguientes medios de eliminación de datos hace que los datos sean irrecuperables incluso con un esfuerzo extraordinario, como con la física forense en un laboratorio?

A. Eliminación de los datos

B. Higienización de los medios

C. Purga mediante sobrescritura

D. Ninguno de los anteriores

16 . Al clasificar la información, su sensibilidad se refiere a:

A. La magnitud del daño o la pérdida que sufriría una organización si la información se perdiera o no estuviera disponible.

B. La magnitud del daño o la pérdida que sufriría una organización si la información se revelara a personas no autorizadas.

C. Las formas en que una organización protege su información de terceros

D. Las formas en que una organización protege su información del abuso interno.

17 . Al clasificar la información, su criticidad se refiere a:

A. La magnitud del daño o la pérdida que sufriría una organización si la información se perdiera o no estuviera disponible.

B. La magnitud del daño o la pérdida que sufriría una organización si la información se revelara a personas no autorizadas.

C. Las formas en que una organización protege su información de terceros

D. Las formas en que una organización protege su información del abuso interno.

18 . ¿Cuáles de los siguientes niveles de clasificación se utilizan con más frecuencia en la industria comercial?

A. Confidencial, Secreto, Máximo Secreto

B. Sin clasificar, sensible pero sin clasificar

C. Privado, patentado, sensible

D. Sin restricciones, solo para uso gubernamental

19 . ¿Cuál de los siguientes niveles de clasificación se usa con más frecuencia en entornos militares?

A. Confidencial, Secreto, Máximo Secreto

B. Sin clasificar, sensible pero sin clasificar

C. Privado, patentado, sensible

D. Sin restricciones, solo para uso gubernamental

20 . ¿Cuál de las siguientes afirmaciones es verdadera con respecto a los requisitos de retención de datos?

R. Los requisitos legales para la retención de datos son uniformes en todos los sectores comerciales regulados y deben seguirse para reducir el riesgo de litigios penales.

B. Para cumplir con las diversas regulaciones de retención de datos, es mejor conservar todos los datos hasta el máximo de los requisitos legales.

C. Retener la mayor cantidad de datos posible hace que responder a las órdenes de descubrimiento electrónico (e-discovery) sea más fácil y sencillo.

D. Una política bien documentada para la retención de datos es un componente mínimo pero necesario del cumplimiento normativo.

21 . ¿Por qué el tema de la remanencia de datos a veces es problemático?

R. Las políticas de retención de datos no suelen especificar cuándo se deben eliminar los datos.

B. Con la mayoría de los sistemas de archivos, la eliminación de datos no garantiza que no se puedan recuperar.

C. Con la mayoría de los sistemas de archivos modernos, sobrescribir accidentalmente una pequeña parte de un archivo hace que los restos restantes sean irrecuperables.

D. La destrucción física es la única forma de garantizar que los datos no se puedan recuperar, y esto suele ser demasiado caro.

22 . ¿Para cuál de los siguientes medios físicos la desmagnetización es un medio relativamente económico y eficaz de erradicar datos?

A. Discos ópticos (CD / DVD)

B. Cintas de respaldo

C. unidades de memoria USB

D. Unidades de disco duro (HDD)

23 . ¿Cuál de los siguientes enfoques es la forma más eficaz para que una organización reduzca su responsabilidad con respecto a la protección de datos privados?

R. Recopile todos y cada uno de los datos que tengan utilidad comercial, pero asegúrese de que el equipo legal haya revisado y aprobado todas las políticas con respecto a su protección.

B. Nunca recopile ni almacene datos protegidos por privacidad.

C. Limite la cantidad de datos privados recopilados a los permitidos legalmente.

D. Limite la cantidad de datos privados recopilados a los necesarios para las funciones comerciales.

24 . Al proteger los activos de información, ¿cuál de los siguientes controles de seguridad es más efectivo para los datos en movimiento?

A. Requerir cifrado de disco completo para todos los dispositivos con el Estándar de cifrado avanzado (AES)

B. Implementación de cifrado con Transport Layer Security (TLS) o IPSec

C. Implementar el cifrado de toda la memoria con el almacenamiento de claves en los registros de la CPU

D. Exigir el uso de firewalls de próxima generación (NGFW) y / o sistemas de prevención de intrusiones basados en la red (NIPS)

25 . Al proteger los activos de información, ¿cuál de los siguientes controles de seguridad es más eficaz para los datos en reposo?

A. Requerir cifrado de disco completo para todos los dispositivos con el Estándar de cifrado avanzado (AES)

B. Implementación de cifrado con Transport Layer Security (TLS) o IPSec

C. Implementar el cifrado de toda la memoria con el almacenamiento de claves en los registros de la CPU

D. Exigir el uso de firewalls de próxima generación (NGFW) y / o sistemas de prevención de intrusiones basados en la red (NIPS)

26 . ¿Cuál de los siguientes es el control de seguridad MENOS efectivo con respecto a los datos confidenciales almacenados en dispositivos móviles?

A. Realice una copia de seguridad de todos los dispositivos en un repositorio administrado organizacionalmente.

B. Implementar el cifrado de volumen completo en todos los dispositivos móviles.

C. Exigir que todos los dispositivos móviles se puedan borrar de forma remota en caso de robo o extravío.

D. Promulgar una política que prohíba el acceso o el almacenamiento de datos corporativos confidenciales en dispositivos móviles personales.

27 . En la era moderna, ¿siguen siendo los registros en papel una preocupación importante en la protección de los activos de datos empresariales? Si es así, ¿por qué? ¿Si no, porque no?

R. Sí, porque los datos más confidenciales generalmente solo se almacenan en forma impresa

B. Sí, porque las copias impresas todavía se producen comúnmente, son más difíciles de rastrear y, por lo general, no se eliminan correctamente.

C. No, porque la cantidad de datos confidenciales que se imprime es excepcionalmente pequeña en comparación.

D. No, porque los datos confidenciales que se imprimen son los más fáciles de destruir correctamente.

28 . Al seleccionar e implementar estándares de protección de activos de información, el proceso de determinación del alcance se refiere a ¿cuál de los siguientes?

A. Elegir el estándar que más fielmente proporciona el cumplimiento normativo dentro de la industria de su organización

B. Modificar las disposiciones de la norma elegida para que sean más relevantes para el entorno de su organización.

C. La eliminación de la aplicación de las partes de la norma elegida que no son relevantes para el entorno de su organización

D. Tomar decisiones con respecto a las sanciones internas por incumplimiento de la norma elegida.

29 . Al seleccionar e implementar estándares de protección de activos de información, ¿por qué la adaptación es un proceso importante?

A. Porque las sanciones por incumplimiento previstas por la norma elegida pueden ser demasiado severas y poco realistas.

B. Porque algunas de las disposiciones de la norma elegida podrían no aplicarse al entorno de su organización.

C. Porque algunas de las disposiciones de la norma elegida podrían abordar mejor el entorno de su organización si se modifican ligeramente

D. Porque no todos los estándares son adecuados para su organización, por lo que es importante elegir el mejor.

30 . Al implementar la prevención de fugas de datos (DLP), ¿cuál es el primer paso y el más crítico?

A. Examine el flujo de datos confidenciales en su organización para comprender mejor qué es apropiado y qué no debe permitirse.

B. Realice una evaluación de riesgos para determinar cuál será la mejor estrategia de protección de datos para su organización.

C. Evalúe las características de los productos disponibles para determinar cuál se adapta mejor a la infraestructura de su organización.

D. Realizar un inventario de todos los datos de su organización para caracterizar y priorizar su sensibilidad.