Domain 2 - Asset Security

Test ID: 175720741

Pregunta #1 de 41

Id. de pregunta: 1113915

En la programación orientada a objetos (OOP), ¿qué define las funciones que un objeto puede llevar a cabo?

- ✗ **A)** atributo
- ✓ **B)** método
- ✗ **C)** clase
- ✗ **D)** Mensaje

explicación

En la programación orientada a objetos (OOP), el método define las funciones que un objeto puede llevar a cabo.

En OOP, cada objeto pertenece a una clase. Cada clase contiene varios atributos. Cada objeto dentro de una clase puede asumir los atributos de la clase a la que pertenece. Los objetos se comunican entre sí mediante mensajes. Estos mensajes indican a los objetos que lleven a cabo ciertas operaciones.

En un sistema orientado a objetos, la situación en la que los objetos con un nombre común responden de manera diferente a un conjunto común de operaciones se denomina polimorfismo. La herencia se produce cuando todos los métodos de una clase se pasan a una subclase.

Smalltalk, Simula 67 y C++ son lenguajes orientados a objetos.

La fase OOP del ciclo de vida del desarrollo de software orientado a objetos se describe como enfatizando el empleo de objetos y métodos, en lugar de tipos o transformaciones como en otros enfoques de software

Objetivo:
Seguridad de activos

Subobsecución:
Determinar los controles de seguridad de los datos

Referencias:

Cissp Cert Guide (3ª edición), Capítulo 2: Seguridad de activos, Bases de datos

Pregunta #2 de 41

Id. de pregunta: 1114684

El nuevo plan de seguridad para su organización indica que todos los datos de los servidores deben clasificarse para garantizar que se implementan los controles de acceso adecuados. ¿Qué ocurre con la clasificación de la información?

un. El propietario de los datos debe determinar la clasificación de la información de un activo.

B. La clasificación de datos se refiere a la asignación de etiquetas de seguridad a los activos de información.

c. Un custodio de datos debe determinar la clasificación de un activo de información.

d. Las dos clases principales de clasificación de datos se refieren a instituciones gubernamentales y militares y organizaciones del sector privado.

E. Las dos clases principales del esquema de clasificación de datos se aplican a organizaciones sin fines de lucro e instituciones financieras.

- ✗ **A)** opción b
- ✗ **B)** opción c
- ✗ **C)** opción A
- ✗ **D)** Opciones C y E Solamente
- ✗ **E)** todas las opciones
- ✗ **F)** opción e
- ✓ **G)** opciones a, b y d solamente
- ✗ **H)** Opción d

explicación

La clasificación de datos se refiere a la asignación de etiquetas de seguridad a los activos de información. Al clasificar los datos, los profesionales de la seguridad deben tener en cuenta la confidencialidad, integridad y disponibilidad de los datos. El propietario de los datos debe determinar la clasificación de la información de un activo. La clasificación de datos es el método más importante utilizado para garantizar la integridad de los datos. Es responsabilidad del propietario de los datos decidir el nivel de clasificación que requiere la información. Una vez que el propietario de los datos determina los niveles de clasificación, el custodio de datos implementa realmente el esquema de clasificación de la información. Uno de los propósitos de la clasificación de la información es definir los parámetros necesarios para las etiquetas de seguridad. Después de ser clasificado, es difícil desclasificar la información. La administración es responsable en última instancia de la clasificación de los datos. Los siguientes pasos son necesarios para clasificar la información:

- Especifique los criterios de clasificación.
- Clasificar los datos.
- Especifique los controles.
- Dar a conocer los controles de clasificación.

Las siguientes situaciones son la distribución externa adecuada de la información clasificada:

- Cumplimiento de una orden judicial
- Tras la aprobación de alto nivel después de un acuerdo de confidencialidad
- Contratos de contratación pública para un proyecto gubernamental

Existen dos sistemas de clasificación de datos: el sector privado y el gobierno y el ejército. Las empresas generalmente se preocupan más por la integridad y disponibilidad de los datos, mientras que el gobierno y el ejército están más preocupados por la confidencialidad.

Los tipos de clasificación de datos del sector privado son los siguientes:

- Confidencial: Los datos clasificados como confidenciales están destinados a ser uso dentro de la organización, independientemente de si son comerciales o militares. Esta es la única categoría común entre los sistemas de clasificación comercial y militar. La información confidencial requiere autorización para cada acceso y está disponible para aquellos empleados de la organización cuyo trabajo se relaciona con el tema. Los datos confidenciales están exentos de la Ley de Libertad de Información (FOIA). Algunos ejemplos son los secretos comerciales, los códigos de programación o la información sanitaria.
- Privada: La información privada es personal para los empleados de una empresa, por lo que también debe protegerse. Un ejemplo es el salario de los empleados.
- Confidencial: La información confidencial requiere una protección especial contra la modificación o eliminación no autorizada. En otras palabras, hay que garantizar la integridad y la confidencialidad. Los ejemplos incluyen información financiera, ganancias o detalles del proyecto.
- Público: La divulgación de información pública no causaría ningún problema a la empresa. Un ejemplo son los anuncios de nuevos proyectos.

Los tipos de clasificación de datos gubernamentales y militares incluyen: alto secreto, secreto, confidencial, sensible pero no clasificado y no clasificado.

Objetivo:
Seguridad de activos

Subobsecución:
Identificar y clasificar la información y los activos

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 2: Seguridad de activos, datos y clasificación de activos

---

Pregunta #3 de 41

Id. de pregunta: 1114688

Debe implementar hardware que proporcione alta disponibilidad. ¿Qué soluciones de contingencia de hardware ofrecen esto?

a. RAID

b. Copias de seguridad en cinta

c. bóveda

d. Replicación de disco

- ✗ **A)** Opción B y C
- ✗ **B)** Opción d
- ✗ **C)** opciones A y B
- ✓ **D)** Opciones A y D
- ✗ **E)** opción b
- ✗ **F)** opción A
- ✗ **G)** Opciones B y D
- ✗ **H)** opción c

explicación

Tanto raid como replicación en disco ofrecen alta disponibilidad.

La matriz redundante de discos independientes (RAID) proporciona redundancia para las unidades de disco duro. Un volumen RAID que incluye varias unidades se considera como una unidad para aplicaciones y otros dispositivos. En la mayoría de las implementaciones raid, los datos permanecen disponibles si falla una unidad dentro del volumen.

La replicación de disco es el proceso de replicar los datos de un disco en otro disco. Si se produce un error en el disco principal, el disco que contiene los datos replicados puede hacerse cargo.

Las copias de seguridad en cinta no tienen una alta disponibilidad. Deben restaurarse, lo que podría tardar mucho tiempo dependiendo de la cantidad de datos que se van a restaurar. Las copias de seguridad en cinta también tienen los siguientes problemas:

Transferencia de datos lenta durante la copia de seguridad y restauración

Se amplía la utilización del espacio en disco del servidor

La posibilidad de que sea necesario realizar alguna reentrada de datos después de un bloqueo Vaulting realiza copias de seguridad electrónicas de los datos y los transmite a ubicaciones de almacenamiento fuera del sitio. Estas copias de seguridad deben restaurarse de forma similar a las copias de seguridad en cinta.

El equilibrio de carga, la replicación de discos y la agrupación en clústeres proporcionan una solución de contingencia de servidor que ofrece alta disponibilidad. Las instalaciones fuera del sitio también pueden ofrecer soluciones de

contingencia de servidor con una disponibilidad menor que el equilibrio de carga, la replicación de disco o la agrupación en clústeres.

Objetivo:
Seguridad de activos

Subobsecución:
Determinar los controles de seguridad de los datos

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 2: Raid de seguridad de activos

---

Pregunta #4 de 41

Id. de pregunta: 1104926

Ha decidido implementar una estrategia de copia de seguridad completa o incremental. Una copia de seguridad completa se realizará cada domingo. Se realizará una copia de seguridad incremental los otros días de la semana. ¿Qué hace una copia de seguridad incremental?

- ✗ **A)** Hace una copia de seguridad de todos los archivos.
- ✗ **B)** Realiza una copia de seguridad de todos los archivos nuevos y los archivos que han cambiado desde la última copia de seguridad completa sin restablecer el bit de archivo.
- ✓ **C)** Realiza una copia de seguridad de todos los archivos nuevos y los archivos que han cambiado desde la última copia de seguridad completa o incremental y restablece el bit de archivo.
- ✗ **D)** Hace una copia de seguridad de todos los archivos en un formato comprimido.

explicación

Una copia de seguridad incremental realiza una copia de seguridad de todos los archivos y archivos nuevos que han cambiado desde la última copia de seguridad completa o incremental y restablece el bit de archivo. Al restaurar los datos, primero se debe restaurar la copia de seguridad completa, seguida de cada copia de seguridad incremental en orden. Las copias de seguridad incrementales se basan unas en otras. Por ejemplo, la segunda copia de seguridad incremental contiene los cambios realizados desde la primera copia de seguridad incremental. Una restauración que implique copias de seguridad incrementales requeriría restaurar primero la copia de seguridad completa más reciente y, a continuación, restaurar en orden las copias de seguridad incrementales que se produjeron desde la última copia de seguridad completa.

Una copia de seguridad completa realiza una copia de seguridad de todos los archivos cada vez que se ejecuta. Debido a la cantidad de datos de los que se realiza una copia de seguridad, las copias de seguridad completas pueden tardar mucho tiempo en completarse. Una copia de seguridad completa se utiliza como línea de base para cualquier estrategia de copia de seguridad y es más adecuada cuando se usa el archivado fuera del sitio.

Una copia de seguridad completa comprimida realiza una copia de seguridad de todos los archivos en formato comprimido.

Una copia de seguridad diferencial realiza una copia de seguridad de todos los archivos nuevos y los archivos que han cambiado desde la última copia de seguridad completa sin restablecer el bit de archivo. Al restaurar los datos, primero se debe restaurar la copia de seguridad completa, seguida de la copia de seguridad diferencial más reciente. Las copias de seguridad diferenciales no dependen unas de otras. Por ejemplo, cada copia de seguridad diferencial contiene los cambios realizados desde la última copia de seguridad completa. Por lo tanto, las copias de seguridad diferenciales pueden tardar mucho más tiempo que las copias de seguridad incrementales. Sin embargo, una restauración diferencial requiere sólo dos archivos de copia de seguridad: la copia de seguridad completa y la copia de seguridad diferencial más reciente.

Un sistema de copia de seguridad continua es aquel que realiza copias de seguridad de forma regular para garantizar que los datos se puedan restaurar a un punto en el tiempo determinado. SQL Server 2000 es una aplicación que proporciona esta característica.

Si no se utiliza un plan de copia de seguridad continua, los cambios de datos que se produzcan desde la última copia de seguridad se deben volver a crear una vez completada la restauración.

Objetivo:
Seguridad de activos

Subobsecución:
Determinar los controles de seguridad de los datos

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 2: Seguridad de activos, tipos y esquemas de copia de seguridad de datos

---

Pregunta #5 de 41

Id. de pregunta: 1104915

Su organización tiene varias bases de datos. Cada base de datos se usa para un propósito específico dentro de su organización. La administración ha decidido combinar las bases de datos en una sola base de datos grande para el análisis de datos. ¿Cómo se llama este proceso?

- ✗ **A)** metadatos
- ✗ **B)** minería de datos

✓ **C)** almacenamiento de datos

✗ **D)** particionado

explicación

El almacenamiento de datos es el proceso de combinar bases de datos en una sola base de datos grande para su análisis.

La creación de particiones es el proceso que divide una base de datos en partes para proporcionar una mayor seguridad.

Los metadatos son los datos que se obtienen al analizar un almacén de datos. Básicamente, los datos entran en un almacén de datos y los metadatos (datos sobre los datos) salen.

La minería de datos es el proceso de usar herramientas para analizar los datos del almacén de datos para descubrir tendencias y relaciones.

Objetivo:
Seguridad de activos

Subobsecución:
Determinar los controles de seguridad de los datos

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 2: Seguridad de activos, almacenes de datos y minería de datos

---

Pregunta #6 de 41

Id. de pregunta: 1104895

Está revisando los métodos de control de acceso utilizados por una organización. A la organización le preocupa el costo del control de acceso. ¿Qué aspecto de la información que se está salvaguardando afectará más a este costo?

✗ **A)** costo de reemplazo de información

✗ **B)** redundancia de información

✗ **C)** tipo de información

✓ **D)** valor de la información

explicación

El valor de la información afectará más al costo del control de acceso. La información que tiene un alto valor para la empresa debe ser protegida. Esto afecta a la confidencialidad de la información. El costo efectivo máximo del control de acceso se determina en función del valor de la información.

El tipo de información afectará al diseño del control de acceso. Si bien puede afectar el costo, no es el factor más importante que lo afecta.

La redundancia de información afectará al diseño del control de acceso. La redundancia de la información garantiza que se conserve más de una copia de los datos importantes. Las copias redundantes pueden estar en un CD-ROM, en otro disco duro o en un medio de copia de seguridad. Por lo general, la redundancia de la información no afecta en gran medida al costo del control de acceso porque las copias redundantes conservan los mismos permisos de control de acceso que las copias originales.

El costo de reemplazo de información afectará el costo de su control de acceso, pero no es el factor que más lo afectará. El costo de reemplazo de información debe incluir el costo de reemplazar el equipo, así como el tiempo de mano de obra que tomaría volver a poner la información en línea.

Objetivo:
Seguridad de activos

Subobsecución:
Identificar y clasificar la información y los activos

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 2: Seguridad de activos, datos y clasificación de activos

---

Pregunta #7 de 41

Id. de pregunta: 1113913

Se le ha pedido que proporcione orientación de ámbito y adaptación para los controles de seguridad de una organización. ¿Cuál de las siguientes pautas NO es cierta con respecto a este proceso?

- ✓ **A)** El ámbito y la adaptación están estrechamente vinculados a las listas de control de acceso.
- ✗ **B)** El alcance y la adaptación permiten a una organización reducir su enfoque.
- ✗ **C)** La adaptación de los controles de seguridad a las necesidades de la organización.
- ✗ **D)** El ámbito proporciona instrucciones a una organización sobre cómo aplicar e implementar controles de seguridad.

explicación

NO es cierto afirmar que el ámbito y la adaptación están estrechamente vinculados a las listas de control de acceso. El ámbito y la adaptación están estrechamente vinculados a las líneas de base de seguridad, no a las listas de control de acceso.

El ámbito proporciona instrucciones a una organización sobre cómo aplicar e implementar controles de seguridad. La adaptación de los controles de seguridad a las necesidades de la organización. El alcance y la adaptación permitirán a una organización reducir su enfoque para identificar y abordar los riesgos apropiados.

Objetivo:
Seguridad de activos

Subobsecución:
Determinar los controles de seguridad de los datos

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 2: Seguridad de activos, alcance y adaptación

Adaptación de controles de seguridad, http://www.hackingtheuniverse.com/infosec/nist-computer-security/security-control-implementation/tailoring-security-controls

---

Pregunta #8 de 41

Id. de pregunta: 1104899

¿Qué instrucción define más correctamente un sistema de administración de bases de datos (DBMS)?

- ✗ **A)** un repositorio central de elementos de datos y sus respectivas relaciones
- ✓ **B)** Un conjunto de programas de software que proporcionan acceso a los datos e implementan permisos en los componentes de datos
- ✗ **C)** un programa de software que permite el diseño y la implementación de bases de datos
- ✗ **D)** Una interfaz de programación de aplicaciones utilizada para proporcionar conectividad entre la base de datos y las aplicaciones

explicación

Un DBMS de sistema de administración de bases de datos (DBMS) hace referencia a un conjunto de programas de software que mantiene y proporciona acceso controlado a los componentes de datos almacenados en filas y columnas de una tabla. La colección de tablas interrelacionadas se conoce como base de datos. Un administrador de base de datos administra una base de datos y supervisa las limitaciones aplicadas a los componentes de datos mediante mecanismos de seguridad de base de datos, como vistas de base de datos y listas de control de acceso. Los usuarios acceden a la base de datos a través de un software cliente mediante un lenguaje de consulta estructurado para obtener la salida de datos. Una base de datos puede utilizar el lenguaje de definición de datos (DDL), el lenguaje de manipulación de datos (DML) y el lenguaje de consulta (QL) para extraer datos según las instrucciones del usuario.

Un DBMS no está relacionado con el diseño y la implementación de la base de datos. Un diseño e implementación de DBMS son las instrucciones incrustadas durante el ciclo de vida de desarrollo de la base de datos. Un DBMS permite a un administrador de bases de datos administrar eficazmente la información de una base de datos. Un administrador de base de datos puede proporcionar permisos granulares a diferentes usuarios de los cuales algunos usuarios pueden ser capaces de leer los componentes de datos y otros pueden tener los privilegios para modificar los datos e implementar el control de acceso.

Un repositorio central de los componentes de datos y sus interrelaciones se conoce como un diccionario de datos y no como un DBMS. Un diccionario de datos es una base de datos para desarrolladores de sistemas.

Una interfaz de programación de aplicaciones (API) proporciona conectividad remota o local entre los sistemas de bases de datos y las aplicaciones web. Una API, como Conectividad abierta de bases de datos (ODBC), puede actuar como una interfaz entre la base de datos y los componentes de datos almacenados en otras aplicaciones.

Objetivo:
Seguridad de activos

Subobsecución:
Identificar y clasificar la información y los activos

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 2: Seguridad de activos, arquitectura y modelos DBMS

Pregunta #9 de 41

Id. de pregunta: 1113914

Ha implementado las tres bases de datos que usa su organización para asegurarse de que se debe ejecutar una transacción completa para garantizar la integridad de los datos. Si una parte de una transacción no se puede completar, no se realiza toda la transacción. ¿Qué mecanismo de seguridad de base de datos está utilizando?

- ✗ **A)** agregación
- ✗ **B)** concurrencia
- ✓ **C)** confirmación en dos fases
- ✗ **D)** guardar puntos

explicación

Está utilizando la confirmación en dos fases. Una confirmación en dos fases garantiza que se ejecuta toda la transacción para garantizar la integridad de los datos. Si una parte de una transacción no se puede completar, no se realiza toda la transacción.

La simultaneidad garantiza que la información más actualizada se muestre a los usuarios de la base de datos. Para garantizar la simultaneidad, los bloqueos a menudo se implementan en el nivel de página, tabla, fila o campo para garantizar que las actualizaciones se produzcan de una en una.

Los puntos de guardado garantizan que la base de datos pueda volver a un estado anterior si se produce un error del sistema. Un punto de guardado normalmente guardará parte de la actualización de datos. Los puntos de guardado son un mecanismo de seguridad para garantizar la integridad de los datos.

La agregación se produce cuando un usuario puede tomar información de diferentes orígenes y combinarla para predecir con precisión que el usuario no tiene la autorización para ver directamente.

Objetivo:
Seguridad de activos

Subobsecución:
Determinar los controles de seguridad de los datos

Referencias:

Cissp Cert Guide (3ª edición), Capítulo 2: Seguridad de activos, Bases de datos

---

Pregunta #10 de 41

Pregunta con id.: 1104900

Un usuario de su organización ha estado difundiendo información de nóminas sobre varios compañeros de trabajo. Aunque no se le ha dado acceso directo a estos datos, pudo determinar esta información sobre la base de algunas vistas de la base de datos a las que tiene acceso. ¿Qué término se utiliza para la condición que se ha producido?

- ✗ **A)** guardar punto
- ✗ **B)** poliinstanciación
- ✗ **C)** compactación de datos
- ✓ **D)** agregación

explicación

La condición que se ha producido es la agregación. La agregación es un proceso en el que un usuario recopila y combina información de varias fuentes para obtener información completa. Las partes individuales de la información están en la sensibilidad correcta, pero la información combinada no lo es. Un usuario puede combinar la información disponible con un privilegio inferior, deduciendo así la información en un nivel de privilegios más alto.

Una amenaza similar surge en los ataques de inferencia, donde el sujeto deduce la información completa sobre un objeto a partir de los bits de información recopilados a través de la agregación. Por lo tanto, la inferencia es la

capacidad de un sujeto para derivar información implícita. Un mecanismo de protección para limitar la inferencia de información en las consultas de bases de datos estadísticas es especificar un tamaño mínimo del conjunto de consultas, pero prohibir la consulta de todos los registros de la base de datos, pero uno.

La condición que se ha producido no es un punto de guardado. Un punto de guardado no es una característica de seguridad de base de datos, sino una característica de integridad y disponibilidad de datos. Los puntos de guardado se utilizan para garantizar que una base de datos pueda volver a un punto antes de que el sistema se bloqueara y poner a disposición los datos antes del error de la base de datos. Los puntos de guardado se pueden iniciar mediante un intervalo de tiempo programado o en la actividad realizada por un usuario durante el procesamiento de datos.

La condición que se ha producido no es la poliinstanciación. La poliinstanciación, también conocida como contaminación de datos, se utiliza para ocultar información clasificada que existe en una base de datos y para engañar a los intrusos. La poliinstanciación garantiza que los usuarios con un nivel de acceso inferior no puedan acceder a los datos categorizados ni modificarlos para obtener un nivel de acceso superior en una base de datos de varios niveles. La poliinstanciación se puede utilizar para reducir las infracciones de inferencia de datos. Cuando se implementa la poliinstanciación, se crean dos objetos utilizando las mismas claves principales. Un objeto se rellena con información incorrecta y se considera no clasificado, y el otro objeto contiene la información clasificada original. Cuando un usuario con privilegios de nivel inferior intenta acceder al objeto, se dirige al usuario al objeto que contiene información incorrecta. La poliinstanciación se refiere a la misma clave principal que existe en diferentes niveles de clasificación en la misma base de datos.

La condición que se ha producido no es barrido. El barrido, también conocido como exploración, implica buscar información sin conocer su formato. El barrido es buscar los residuos de datos en un sistema para obtener conocimiento no autorizado de los datos confidenciales.

Objetivo:
Seguridad de activos

Subobsecución:
Identificar y clasificar la información y los activos

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 2: Seguridad de activos, amenazas de base de datos

---

Pregunta #11 de 41

Id. de pregunta: 1104898

A la administración le preocupa que los atacantes intenten acceder a la información de la base de datos. Le han pedido que implemente la protección de la base de datos utilizando datos falsos con la esperanza de que los datos falsos engañen a los atacantes. ¿Qué técnica se solicita?

✗ **A)** front-end de confianza

✓ **B)** ruido y perturbación

✗ **C)** particionado

✗ **D)** supresión celular

explicación

Se está solicitando la técnica de ruido y perturbación. Esta técnica consiste en insertar información falsa aleatoria junto con registros válidos de la base de datos para engañar a los atacantes y proteger la confidencialidad e integridad de la base de datos. Esto altera los datos, pero permite a los usuarios acceder a la información relevante de la base de datos. Esta técnica también crea suficiente confusión para evitar que el atacante indique la diferencia entre información válida y no válida.

No se solicita la creación de particiones. La creación de particiones es otra técnica de protección para la seguridad de la base de datos. La partición implica dividir la base de datos en muchas partes y dificultar que un intruso recopile y combine información confidencial y deduzca hechos relevantes.

No se solicita la supresión de celdas. La supresión de celdas es la técnica utilizada para proteger la información confidencial almacenada en las bases de datos ocultando las celdas de la base de datos que se pueden utilizar para divulgar información confidencial.

No se solicita un front-end de confianza. Un front-end de confianza hace referencia a proporcionar seguridad a la base de datos mediante la incorporación de características de seguridad en la funcionalidad del software cliente front-end que se usa para emitir instrucciones al servidor back-end mediante un lenguaje de consulta estructurado. El software cliente front-end de confianza actúa como una interfaz para el sistema de base de datos back-end y proporciona la salida resultante en función de las instrucciones de entrada emitidas por el usuario.

Objetivo:
Seguridad de activos

Subobsecución:
Identificar y clasificar la información y los activos

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 2: Seguridad de activos, vistas de base de datos

---

Pregunta #12 de 41

Id. de pregunta: 1104911

¿Cuál de las siguientes opciones NO debería afectar a las políticas de retención de activos?

- ✗ **A)** leyes y reglamentos
- ✓ **B)** calidad de activos o datos
- ✗ **C)** Antigüedad de activos o datos
- ✗ **D)** activo o tipo de datos

explicación

La calidad de los activos o datos no debe afectar a las políticas de retención de activos.

Las directivas de retención de activos se ven afectadas por la antigüedad de los activos o datos y el activo o el tipo de datos. Además, las políticas pueden verse afectadas por las leyes y regulaciones aplicables. Si se coloca una retención legal en un activo o datos, el activo o los datos deben conservarse al menos hasta que se levante la retención legal.

Objetivo:
Seguridad de activos

Subobsecución:
Garantizar una retención adecuada de activos

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 2: Seguridad de activos, retención de activos

---

Pregunta #13 de 41

Id. de pregunta: 1132507

Su empresa implementa varias bases de datos. Le preocupa la seguridad de los datos de las bases de datos. ¿Qué instrucción es correcta para la seguridad de la base de datos?

- ✗ **A)** Las variables de enlace proporcionan control de acceso mediante la implementación de restricciones granulares.
- ✓ **B)** El lenguaje de control de datos (DCL) implementa la seguridad a través del control de acceso y las restricciones granulares.
- ✗ **C)** El lenguaje de manipulación de datos (DML) implementa el control de acceso a través de la autorización.
- ✗ **D)** El lenguaje de identificación de datos implementa la seguridad en los componentes de datos.

explicación

El lenguaje de control de datos (DCL) administra el control de acceso a los registros de una base de datos. DCL define los permisos de usuario granulares para varios objetos de datos e implementa la seguridad de la base de datos. Algunos ejemplos de comandos de lenguaje de control de base de datos son conceder, denegar e implementar permisos granulares para diferentes usuarios y grupos. Por ejemplo, Juan podría tener acceso de lectura al archivo A y Matt podría tener el acceso de lectura y actualización al mismo archivo. La seguridad granular se basa en la necesidad de conocer y privilegios mínimos. Normalmente, las responsabilidades de trabajo y los roles de los usuarios determinan su acceso a varios componentes de datos.

El idioma de identificación de datos es una opción no válida porque no es un lenguaje válido del sistema de administración de bases de datos.

El lenguaje de manipulación de datos (DML) no proporciona control de acceso a través de la autorización. DML hace referencia a un conjunto de lenguajes informáticos utilizados por los usuarios de bases de datos para recuperar, insertar, eliminar y actualizar datos en una base de datos. DML proporciona a los usuarios la capacidad de almacenar, recuperar y manipular los datos de acuerdo con las instrucciones emitidas.

Las variables de enlace no proporcionan control de acceso. Las variables de enlace se utilizan para mejorar el rendimiento de la base de datos al permitir que una sola instrucción ejecute varias variables. Las variables de enlace son marcadores de posición para los valores enviados a un servidor de bases de datos en una consulta SQL. Permiten la reutilización de instrucciones SQL emitidas previamente mediante la ejecución de un conjunto preparado de instrucciones con los parámetros proporcionados en tiempo de ejecución. Las variables de enlace no implementan la seguridad en un sistema de administración de bases de datos.

Objetivo:
Seguridad de activos

Subobsecución:
Determinar los controles de seguridad de los datos

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 2,Seguridad de activos, Bases de datos

Lenguaje de control de datos, http://databases.about.com/od/Advanced-SQL-Topics/a/Data-Control-Language-Dcl.htm

Lenguaje de manipulación de datos, http://databases.about.com/od/sql/a/sqlfundamentals_3.htm

---

Pregunta #14 de 41

Id. de pregunta: 1104923

¿Qué protocolo NO utiliza el almacenamiento conectado en red?

✗ **A)** Smb

✗ **B)** CIFS

✗ **C)** Nfs

✓ **D)** NTFS

explicación

Sistema de archivos de nueva tecnología (NTFS) es el sistema de archivos utilizado por los equipos con Windows Server. No es un protocolo.

Network File System (NFS), Common Internet File System (CIFS) y Server Message Block (SMB) son protocolos utilizados por el almacenamiento conectado en red (NAS).

Objetivo:
Seguridad de activos

Subobsecución:
Determinar los controles de seguridad de los datos

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 2: Seguridad de activos, NAS

Almacenamiento de información conectado en red,
http://compnetworking.about.com/od/itinformationtechnology/l/aa070101a.htm

---

Pregunta #15 de 41

Id. de pregunta: 1104904

Está considerando la sensibilidad y la criticidad de los datos de su organización. ¿Cuál de las siguientes afirmaciones NO es verdadera?

✗ **A)** La sensibilidad determina la libertad con la que se pueden manejar los datos.

✓ **B)** Los datos que son confidenciales también deben considerarse críticos.

✗ **C)** La criticidad mide la importancia de los datos.

✗ **D)** Una vez que se documenta la sensibilidad y la criticidad de los datos, la organización debe trabajar para crear un sistema de clasificación de datos.

explicación

No es cierto que los datos confidenciales también deban considerarse datos críticos. Los datos considerados sensibles no necesariamente pueden considerarse críticos. La sensibilidad y la criticidad no están relacionadas.

La sensibilidad determina la libertad con la que se pueden manejar los datos. La criticidad mide la importancia de los datos. Una vez que se documenta la sensibilidad y la criticidad de los datos, la organización debe trabajar para crear un sistema de clasificación de datos.

Objetivo:
Seguridad de activos

Subobsecución:
Identificar y clasificar la información y los activos

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 2: Sensibilidad y criticidad de la seguridad de los activos

---

Pregunta #16 de 41

Id. de pregunta: 1114687

¿Qué instrucciones NO son válidas con respecto a los comandos SQL?

un. Una instrucción ADD se utiliza para agregar nuevas filas a una tabla.

B. Una instrucción DELETE se utiliza para eliminar filas de una tabla.

c. Se utiliza una instrucción REPLACE para reemplazar filas en una tabla.

d. Se utiliza una instrucción SELECT para recuperar filas de una tabla.

E. Una instrucción GRANT se utiliza para conceder permisos a un usuario.

- ✓ **A)** Sólo las opciones A y C
- ✗ **B)** Opción d
- ✗ **C)** opción b
- ✗ **D)** todas las opciones
- ✗ **E)** opción e
- ✗ **F)** opción A
- ✗ **G)** opciones b, d y e solamente
- ✗ **H)** opción c

explicación

Las instrucciones relativas a una instrucción ADD y una instrucción REPLACE NO son válidas con respecto a los comandos SQL.

SELECT, DELETE y GRANT son comandos SQL válidos. La instrucción SELECT se utiliza para recuperar filas de una tabla, la instrucción DELETE se utiliza para eliminar filas de una tabla y la instrucción GRANT se utiliza para conceder permisos a un usuario.

Las instrucciones REPLACE y ADD no son instrucciones SQL válidas. La instrucción UPDATE se utiliza para reemplazar o actualizar filas en una tabla. Se utiliza una instrucción INSERT para agregar filas a una tabla.

Objetivo:
Seguridad de activos

Subobsecución:
Determinar los controles de seguridad de los datos

Referencias:

Red Hat Database: Guía y referencia sql, http://www.redhat.com/docs/manuals/database/RHDB-7.1.3-Manual/sql/sql-commands.html

---

Pregunta #17 de 41

Id. de pregunta: 1104928

Su empresa tiene una solución de copia de seguridad que realiza una copia de seguridad completa cada sábado por la noche y una copia de seguridad incremental todas las demás noches. Un sistema vital se estrella el lunes por la mañana. ¿Cuántas copias de seguridad se necesitarán restaurar?

- ✓ **A)** Dos
- ✗ **B)** Tres
- ✗ **C)** Cuatro
- ✗ **D)** Uno

explicación

Debido a que el sistema se bloquea el lunes por la mañana, deberá restaurar dos copias de seguridad: la copia de seguridad completa del sábado por la noche y la copia de seguridad incremental del domingo por la noche. Cuando se incluyen copias de seguridad incrementales en el plan de copia de seguridad, deberá restaurar la copia de seguridad completa y todas las copias de seguridad incrementales que se han realizado desde la copia de seguridad completa. Dado que el error se produjo el lunes por la mañana, solo es necesario restaurar la copia de seguridad completa del sábado y la copia de seguridad incremental del domingo.

Si el bloqueo se hubiera producido el martes por la mañana, habría tenido que restaurar tres copias de seguridad: la copia de seguridad completa del sábado por la noche, la copia de seguridad incremental del domingo por la noche y la copia de seguridad incremental del lunes por la noche.

Si el bloqueo se hubiera producido el miércoles por la mañana, habría necesitado restaurar cuatro copias de seguridad: la copia de seguridad completa del sábado por la noche, la copia de seguridad incremental del domingo por la noche, la copia de seguridad incremental del lunes por la noche y la copia de seguridad incremental del martes por la noche.

Objetivo:
Seguridad de activos

Subobsecución:
Determinar los controles de seguridad de los datos

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 2: Seguridad de activos, tipos y esquemas de copia de seguridad de datos

---

Pregunta #18 de 41

Id. de pregunta: 1111697

¿Qué operación debe realizar para evitar el mal manejo de cintas, CDs, DVDs, disquetes y material impreso?

- ✓ **A)** etiquetado
- ✗ **B)** puesta a cero
- ✗ **C)** almacenamiento de información fuera del sitio
- ✗ **D)** Desmagnetización

explicación

Se requiere un etiquetado adecuado para evitar el mal manejo de la información en los medios de almacenamiento, como cintas y disquetes. Los discos compactos y los disquetes se utilizan para almacenar pequeños conjuntos de datos, mientras que las cintas de copia de seguridad se utilizan para almacenar un gran número de conjuntos de datos. Los medios de almacenamiento que contengan información confidencial deben estar debidamente marcados y etiquetados para garantizar una clasificación adecuada. Los medios de almacenamiento también deben almacenarse en un área protegida. Cada medio debe etiquetarse con los siguientes detalles:

- clasificación
- fecha de creación
- período de retención
- nombre y versión del volumen
- Nombre de la persona que creó la copia de seguridad

La desgaussing no es una técnica de manejo de medios, sino una técnica de desinfección de medios. La desmagnación es el proceso de reducir o eliminar un campo magnético no deseado de un medio de almacenamiento

mediante la aplicación de fuertes fuerzas magnéticas. Los dispositivos de desmagnación generan potentes campos magnéticos opuestos que reducen la densidad de flujo magnético de los medios de almacenamiento a cero. La desmagrasación es el método más preferido para borrar datos de medios magnéticos, como disquetes y cintas magnéticas.

La puesta a cero no es una técnica de manejo de medios, sino una técnica de desinfección de medios. La puesta a cero implica que un medio de almacenamiento se sobrescribe repetidamente con valores nulos, como varios unos y ceros, para la desinfección. La puesta a cero se utiliza generalmente en un entorno de desarrollo de software.

La transferencia de datos a una ubicación fuera del sitio debe realizarse para crear una copia de seguridad de los medios si se produce un desastre en el sitio primario. Los datos transferidos a una ubicación fuera del sitio actúan como una copia de seguridad de los datos. Los medios de almacenamiento deben etiquetarse adecuadamente para evitar un mal manejo.

Objetivo:
Seguridad de activos

Subobjetiva:
Establecer requisitos de información y manejo de activos

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 2: Requisitos de seguridad, información y manejo de activos

---

Pregunta #19 de 41

Id. de pregunta: 1114689

A la administración le preocupa que la pérdida de datos pueda ocurrir en caso de una falla en el disco duro. Se le ha pedido que proporcione un sistema de disco que proteja contra la pérdida de datos si falla una sola unidad en cualquier sistema vital. ¿Qué sistemas de disco debe evaluar?

a. Creación de bandas de disco

b. Creación de reflejo de disco

c. Creación de bandas de disco con paridad

d. Sistema de disco resistente a fallos (FRDS)

- ✗ **A)** Opción d
- ✗ **B)** opción A
- ✗ **C)** todas las opciones
- ✗ **D)** opción b

✗ **E)** opciones a, b y c

✗ **F)** opción c

✓ **G)** opciones b, c y d

explicación

La creación de reflejos de disco, la creación de bandas de disco con paridad y el sistema de disco resistente a errores (FRDS) protegen contra la pérdida de datos si se produce un error en una sola unidad. La creación de reflejo de disco proporciona una copia duplicada de los datos en el disco duro reflejado. La creación de bandas de disco con paridad reconstruye los datos perdidos utilizando la información de paridad en caso de que falle una sola unidad de la matriz. FRDS se utiliza principalmente en servidores de archivos y es similar a RAID.

La creación de bandas de disco no protege contra la pérdida de datos si se produce un error en una sola unidad. Si se produce un error en una unidad en un volumen de creación de bandas de disco, se pierden los datos.

Objetivo:
Seguridad de activos

Subobsecución:
Determinar los controles de seguridad de los datos

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 2: Raid de seguridad de activos

---

Pregunta #20 de 41

Id. de pregunta: 1111694

Usted ha sido contratado como consultor de seguridad para una organización que realiza trabajo por contrato para el Departamento de Defensa de los Estados Unidos (DoD). Debe asegurarse de que todos los datos que forman parte del trabajo del contrato se clasifican correctamente. ¿Cuál es la categoría de clasificación de datos más alta que puede usar?

✗ **A)** sensible

✗ **B)** secreto

✓ **C)** ultrasecreto

✗ **D)** confidencial

explicación

Top Secret es la categoría de clasificación de datos más alta que se puede utilizar al categorizar datos para uso gubernamental o militar. Este sistema tiene cinco niveles principales de clasificación (de menor a mayor):

- Sin clasificar
- sensible
- confidencial
- secreto
- ultrasecreto

Si bien existen otros niveles de clasificación, por lo general operan dentro de estos cinco niveles principales.

Objetivo:
Seguridad de activos

Subobsecución:
Identificar y clasificar la información y los activos

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 2: Seguridad de activos, clasificaciones militares y gubernamentales

---

Pregunta #21 de 41

Id. de pregunta: 1104907

¿Qué método NO se recomienda para eliminar datos de un medio de almacenamiento que se utiliza para almacenar información confidencial?

✗ **A)** Desmagnetización
✓ **B)** formateo
✗ **C)** puesta a cero
✗ **D)** destrucción

explicación

No se recomienda el formato para quitar datos de un medio de almacenamiento que se utiliza para almacenar información confidencial. Formatear o eliminar los datos de un medio de almacenamiento, como un disco duro, no garantiza la eliminación real de los datos, sino que quita los punteros a la ubicación donde residen los datos en el medio de almacenamiento. Los datos residuales en el medio de almacenamiento se conocen como remanencia de datos. El principal problema con la reutilización de medios es la remanencia. Los datos residuales se pueden recuperar mediante procedimientos de recuperación de datos. Esto puede suponer una grave amenaza para la seguridad si la información borrada es de naturaleza confidencial.

La desinfección es el proceso de borrar los medios de almacenamiento para garantizar que sus datos no se puedan recuperar o reutilizar. La desinfección incluye varios métodos, como la reducción a cero, la desgasificación y la destrucción de medios. Todos estos métodos se pueden utilizar para eliminar datos de los medios de almacenamiento,

dependiendo del tipo de medio utilizado. La mayoría de los medios de almacenamiento que tienen una base magnética se pueden desinfectar. Sin embargo, los CDs y DVDs a menudo no pueden ser desgausados. Si este es el caso, la única opción es la destrucción física del CD o DVD.

La puesta a cero implica que un medio de almacenamiento se sobrescribe repetidamente con valores nulos, como varios unos y ceros, para la desinfección. La puesta a cero se utiliza generalmente en un entorno de desarrollo de software.

La desmagnación es el proceso de reducir o eliminar un campo magnético no deseado de un medio de almacenamiento. La desmagnización se refiere a un método de desinfección de medios de almacenamiento mediante el uso de fuerzas magnéticas. Los dispositivos de desmagnación producen potentes campos magnéticos opuestos que reducen la densidad de flujo magnético de los medios de almacenamiento a cero. La desmagnización es el método preferido para borrar datos de medios magnéticos, como disquetes, discos duros y cintas magnéticas.

La destrucción de los medios implica destruir físicamente los medios para hacerlos inutilizables. La seguridad de los medios de almacenamiento puede ser crucial si los datos almacenados son de naturaleza confidencial. Algunos medios de almacenamiento, como los CD-ROM, no se pueden desinfectar debido a la falta de una base magnética. Por lo tanto, se recomienda que los destruya físicamente para evitar la divulgación de información confidencial.

Los controles de viabilidad de los medios se utilizan para proteger la viabilidad de los medios de almacenamiento de datos. Las medidas de control de viabilidad de los medios incluyen el etiquetado o marcado adecuado, la manipulación y el almacenamiento seguros y la eliminación de los medios de almacenamiento.

Objetivo:
Seguridad de activos

Subobsecución:
Proteger la privacidad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 2: Seguridad de activos, desinfección y eliminación de medios

---

Pregunta #22 de 41

Id. de pregunta: 1104909

Debe dar formato a los datos de la base de datos para que se puedan mostrar fácilmente mediante tecnologías web. ¿Qué lenguaje de interfaz debe utilizar?

- ✗ **A)** JDBC
- ✗ **B)** alboroto
- ✗ **C)** OLE DB

✓ **D)** XML

explicación

Debe utilizar el lenguaje de marcado extensible (XML). XML es un lenguaje de interfaz que se utiliza para organizar los datos de modo que las tecnologías web puedan compartirla. Este lenguaje flexible se puede utilizar para organizar los datos en una variedad de formatos mediante etiquetas.

Java Database Connectivity (JBDC) es una interfaz de programación de aplicaciones (API) que permite a una aplicación Java comunicarse con una base de datos. La base de datos de vinculación e incrustación de objetos (OLE DB) es un método para vincular datos de bases de datos diferentes. ActiveX Data Objects (ADO) es una API que permite a los programas ActiveX consultar bases de datos.

Objetivo:
Seguridad de activos

Subobsecución:
Proteger la privacidad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 2: Seguridad de activos, lenguajes de interfaz de base de datos

---

Pregunta #23 de 41

Id. de pregunta: 1104925

Está investigando las implementaciones de RAID para determinar qué nivel de RAID es el mejor para su organización. ¿Qué nivel raid proporciona sólo mejoras de rendimiento y no proporciona tolerancia a errores?

✗ **A)** RAID 3
✗ **B)** espejado de disco
✗ **C)** RAID 5
✓ **D)** creación de bandas de disco
✗ **E)** agrupamiento

explicación

La creación de bandas de disco sólo proporciona mejoras de rendimiento y no proporciona tolerancia a errores. RAID 0 se conoce como creación de bandas de disco. Los datos se dividen en bandas sobre el número de unidades de disco duro de la matriz. Si se produce un error en una sola unidad, no se puede utilizar toda la matriz.

La creación de reflejo de disco proporciona tolerancia a errores. RAID 1 se conoce como duplicación de disco. Los datos se escriben en la primera unidad y se copian inmediatamente en la segunda unidad. Si se produce un error en una sola unidad, los datos están disponibles desde la otra unidad. Cuando se implementa con varias tarjetas controladoras de disco duro, se conoce como duplicación. La duplicación proporciona tolerancia a fallos tanto para los discos duros como para la tarjeta controladora.

RAID 3 proporciona tolerancia a fallos. RAID 3 se conoce como creación de bandas a nivel de bytes con paridad. Los datos se dividen en bandas en todas las unidades de disco duro de la matriz, excepto una. Un disco duro está reservado para los datos de paridad. Si una sola unidad falla, los datos en ella se pueden reconstruir utilizando la información de paridad. Este nivel raid no se utiliza comúnmente hoy en día.

RAID 5 proporciona tolerancia a fallos. RAID 5 se conoce como creación de bandas de disco a nivel de bloque con paridad. Los datos se dividen en bandas sobre todos los discos duros de la matriz; los datos de paridad se escriben en todas las unidades. Si se produce un error en una sola unidad, los datos en ella se pueden reconstruir utilizando la información de las otras unidades. Esta es una de las versiones raid más populares.

La agrupación en clústeres no es un nivel RAID. La agrupación en clústeres es una tecnología de servidor que distribuye el procesamiento entre varios servidores. Lógicamente, un clúster de servidores aparece como un servidor en un equipo cliente. La agrupación en clústeres es similar a los servidores redundantes. Sin embargo, con servidores redundantes sólo un servidor procesa realmente las solicitudes. El otro servidor actúa como una copia de seguridad en caso de que se produzca un error en el servidor principal.

RAID 2 es otro nivel de creación de bandas que secciona los datos en el nivel de bits en lugar del nivel de bloque. No se utiliza comúnmente hoy en día.

RAID 4 es una creación de bandas a nivel de bloque con paridad. Los datos se dividen en bandas en todas las unidades de disco duro de la matriz, excepto una. Un disco duro está reservado para los datos de paridad. Si una sola unidad falla, los datos en ella se pueden reconstruir utilizando la información de paridad. Este nivel se utiliza más ampliamente que RAID 3 porque seccionar los datos en el nivel de bloque en lugar de en el nivel de bits.

RAID 6 es el mismo que RAID 5, excepto que proporciona un segundo conjunto de paridad. Los datos se dividen en bandas sobre todos los discos duros de la matriz; también se escriben dos conjuntos de datos de paridad en todas las unidades.

RAID 7 es un nivel raid propietario que agrega almacenamiento en caché a RAID 3 o RAID 4.

RAID 10 es una franja de espejos. Se crean varios espejos y los datos se dividen en bandas en estos espejos. Por ejemplo, el primer dato se escribe en la primera unidad del primer reflejo. A continuación, se copia en la segunda unidad del primer espejo. Este nivel RAID admitirá varios errores de unidad.

RAID 0+1 es un espejo de rayas. Se crean dos conjuntos seccionados y el conjunto se refleja. Por ejemplo, el primer dato se escribe en el primer conjunto seccionado. A continuación, se copia en el segundo conjunto de bandas. Este nivel RAID admitirá varios errores de unidad.

RAID se puede implementar utilizando hardware o software. Hardware RAID utiliza hardware dedicado, como una tarjeta controladora RAID, para controlar el RAID. Software RAID utiliza software, normalmente el sistema operativo, para controlar el RAID. Raid de software es más barato y más fácil de configurar, pero no proporciona las mejoras de rendimiento y la fiabilidad que raid de hardware hace. Software RAID sólo se puede implementar en RAID 0, 1 y 5. Raid de hardware se puede implementar en todos los niveles de RAID, excepto raid 1 duplexing.

En las implementaciones raid de hoy en día, la mayoría de las unidades son intercambiables en caliente, lo que significa que se pueden quitar y volver a insertar mientras el equipo está operativo.

Objetivo:
Seguridad de activos

Subobsecución:
Determinar los controles de seguridad de los datos

Referencias:

Cissp Cert Guide (3ª edición), Capítulo 2: Seguridad de activos, RAID

Pregunta #24 de 41

Id. de pregunta: 1104908

En el contexto de los medios de copia de seguridad, ¿qué se entiende por el término tiempo de retención?

- ✓ **A)** La cantidad de tiempo que se almacena una cinta antes de que se sobrescriban sus datos
- ✗ **B)** La cantidad de tiempo que se utiliza una cinta antes de ser destruida
- ✗ **C)** La cantidad de tiempo que tarda una cinta en realizar una copia de seguridad de los datos
- ✗ **D)** La cantidad de tiempo que tarda una cinta en restaurar los datos

explicación

El tiempo de retención es la cantidad de tiempo que se almacena una cinta antes de que se sobrescriban sus datos. Cuanto mayor sea el tiempo de retención, más conjuntos de medios se necesitarán para fines de copia de seguridad. Un tiempo de retención más largo le dará más flexibilidad para la restauración.

El tiempo de backup es la cantidad de tiempo que tarda una cinta en realizar una copia de seguridad de los datos. Se basa en la velocidad del dispositivo y la cantidad de datos de los que se realiza una copia de seguridad.

La vida útil de una cinta es la cantidad de tiempo que se utiliza una cinta antes de ser destruida. La vida útil de una cinta se basa en la cantidad de tiempo que se utiliza. La mayoría de los proveedores proporcionan una estimación de

la vida útil de los medios de copia de seguridad.

El tiempo de restauración es la cantidad de tiempo que tarda una cinta en restaurar los datos. Se basa en la velocidad del dispositivo, la cantidad de datos que se restauran y el tipo de copias de seguridad utilizadas.

Al seleccionar dispositivos y medios de copia de seguridad, debe tener en cuenta las características físicas o el tipo de unidad. El tipo de unidad incluye el tipo de medio, la capacidad y la velocidad. También debe tener en cuenta el esquema de rotación. El esquema de rotación incluye la frecuencia de las copias de seguridad y el tiempo de retención de la cinta.

Objetivo:
Seguridad de activos

Subobsecución:
Proteger la privacidad

Referencias:

Cissp Cert Guide (3ª edición), Capítulo 2: Seguridad de activos, ciclo de vida de la información

Sistemas de programación de backup y rotación de medios, http://www.pcguide.com/care/bu/sched.htm

---

Pregunta #25 de 41

Id. de pregunta: 1104918

Debe asegurarse de que un conjunto de usuarios pueda acceder a la información relativa a los gastos departamentales. Sin embargo, cada usuario solo debe poder ver los gastos del departamento en el que trabaja. Los altos directivos deben poder ver los gastos de todos los departamentos. ¿Qué característica de seguridad de base de datos proporciona este control de acceso granular?

- ✓ **A)** vista de base de datos
- ✗ **B)** ruido y perturbación
- ✗ **C)** guardar punto
- ✗ **D)** particionado

explicación

La característica de seguridad de base de datos que proporciona este control de acceso granular son las vistas de base de datos. Las vistas de base de datos se utilizan para limitar el acceso de usuarios y grupos a cierta información en función de los privilegios de usuario y la necesidad de saber. Las vistas se pueden usar para restringir la información en función de la pertenencia a grupos, los derechos de usuario y las etiquetas de seguridad. Las vistas

implementan privilegios mínimos y necesidad de conocer y proporcionan restricciones de acceso dependientes del contenido. Las vistas no proporcionan integridad referencial, que se proporciona mediante restricciones o reglas.

Un punto de almacenamiento no proporciona un control de acceso granular. Los puntos de almacenamiento garantizan la integridad y disponibilidad de los datos, pero no son una característica de seguridad de la base de datos. Los puntos de guardado se utilizan para garantizar que una base de datos pueda volver a un punto cuando el sistema se bloquea. Esto garantiza aún más la disponibilidad de los datos antes del error de la base de datos. Los puntos de guardado se pueden iniciar a una hora programada o mediante una acción del usuario durante el procesamiento de datos.

La integridad de la base de datos también se puede proporcionar mediante la implementación de la integridad referencial, donde todas las claves externas hacen referencia a las claves principales existentes para identificar los registros de recursos de una tabla. La integridad referencial requiere que para cualquier atributo de clave externa, la relación a la que se hace referencia debe tener una tupla con el mismo valor para su clave principal.

La creación de particiones no proporciona un control de acceso granular. La creación de particiones es otra técnica de protección para garantizar la seguridad de la base de datos. La creación de particiones implica dividir la base de datos en muchas partes. La partición dificulta que un intruso recopile y combine información confidencial y deduzca hechos relevantes.

El ruido y la perturbación no proporcionan un control de acceso granular. La técnica de ruido y perturbación implementa la inserción de datos falsos para engañar a los atacantes y proteger la confidencialidad e integridad de la base de datos. La técnica de ruido y perturbación consiste en insertar información falsa aleatoria junto con registros válidos de la base de datos. Esta técnica altera los datos, pero permite a los usuarios acceder a la información relevante de la base de datos. Esta técnica crea suficiente confusión para que el atacante extraiga información confidencial.

Las vistas de base de datos son un ejemplo de control de acceso dependiente del contenido en el que el control de acceso se basa en la confidencialidad de la información y los privilegios de usuario concedidos. Esto conduce a una mayor sobrecarga en términos de procesamiento porque los datos se controlan granularmente por el contenido y los privilegios de los usuarios. Las vistas de base de datos pueden limitar el acceso de los usuarios a partes de datos en lugar de a toda la base de datos. Por ejemplo, durante el procesamiento de la base de datos en una organización, un jefe de departamento podría tener acceso solo a los datos de los empleados que pertenecen a ese departamento.

Objetivo:
Seguridad de activos

Subobsecución:
Determinar los controles de seguridad de los datos

Referencias:

Cissp Cert Guide (3ª edición), Capítulo 2: Seguridad de activos, Bases de datos

Pregunta #26 de 41

Id. de pregunta: 1113917

Como profesional de la seguridad, se le ha pedido que determine las directivas de retención adecuadas para medios, hardware, datos y personal. Primero debe documentar las directivas de retención de datos adecuadas. ¿Cuál de las siguientes afirmaciones NO es cierta en el desarrollo de estas políticas?

✗ **A)** Una vez que haya creado las directivas de retención de datos, el personal debe estar capacitado para cumplir con las directivas de retención de datos.

✗ **B)** El personal que esté más familiarizado con cada tipo de datos debe trabajar con usted para determinar la directiva de retención de datos.

✗ **C)** Debe comprender dónde se almacenan los datos y el tipo de datos almacenados.

✓ **D)** Debe trabajar con los custodios de datos para desarrollar la directiva de retención de datos adecuada para cada tipo de datos que posee la organización.

explicación

No debe trabajar con los custodios de datos para desarrollar la directiva de retención de datos adecuada para cada tipo de datos que posee la organización. Debe trabajar con los propietarios de los datos, no con los custodios de datos, para desarrollar la directiva de retención de datos adecuada para cada tipo de datos que posee la organización.

El personal que esté más familiarizado con cada tipo de datos debe trabajar con usted para determinar la directiva de retención de datos. Debe comprender dónde se almacenan los datos y el tipo de datos almacenados. Una vez que haya creado las directivas de retención de datos, el personal debe estar capacitado para cumplir con las directivas de retención de datos.

Objetivo:
Seguridad de activos

Subobjetiva:
Establecer requisitos de información y manejo de activos

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 2: Seguridad de activos, información y retención de activos

Desarrollo de una política electrónica de retención de datos, http://searchdatabackup.techtarget.com/tip/Developing-an-electronic-data-retention-policy

Desarrollo de una política de retención de datos: aspectos a tener en cuenta, http://thinksis.com/blog/infrastructure/storage/developing-data-retention-policy-things-consider

Pregunta #27 de 41

Id. de pregunta: 1104906

¿Qué modelo de base de datos usa tuplas y atributos para almacenar y organizar la información?

- ✗ **A)** modelo jerárquico
- ✗ **B)** modelo orientado a objetos
- ✓ **C)** modelo relacional
- ✗ **D)** modelo de datos distribuido

explicación

Un modelo de base de datos relacional utiliza atributos y tuplas para almacenar y organizar la información que los usuarios pueden extraer para cumplir con sus responsabilidades de trabajo en la base de datos. En una base de datos relacional, las columnas y filas se conocen como atributos y tuplas, respectivamente. La tabla bidimensional en la que se almacenan los datos se conoce como tabla de relaciones base. En una base de datos, el número total de columnas o atributos de una tabla se denomina grado y el número de filas o tuplas se denomina cardinalidad. Los atributos y las tuplas pueden tener algunos valores permitidos específicos en una base de datos, y el conjunto total de valores permitidos que se pueden asignar a los atributos de una base de datos se conoce como un dominio de una relación. El dominio de una relación especifica la interrelación de los componentes de datos.

En una base de datos jerárquica, los datos se organizan en una estructura de árbol lógico en lugar de en filas y columnas. Los registros y los campos están relacionados entre sí en una estructura de árbol primario-secundario. Una estructura de árbol de base de datos jerárquica tiene ramas y cada rama tiene muchas hojas. En una base de datos jerárquica, las hojas son los campos de datos y se accede a los datos a través de rutas de acceso bien definidas. Las bases de datos jerárquicas se utilizan si existen una o varias relaciones.

Una base de datos orientada a objetos se utiliza para administrar varios tipos de datos, como imágenes, audio, vídeo y documentos. Los diferentes tipos de datos, denominados objetos, se utilizan para crear componentes de datos dinámicos. La principal diferencia entre los modelos de base de datos relacionales y orientados a objetos es que en una base de datos orientada a objetos, los objetos se pueden crear dinámicamente según los requisitos y las instrucciones ejecutadas. En una base de datos relacional, la aplicación utiliza procedimientos para extraer los datos.

Un modelo de base de datos distribuida hace referencia a varias bases de datos que están situadas en ubicaciones remotas y están conectadas lógicamente. En un modelo de base de datos distribuida, la transición de una base de datos a otra se mantiene transparente para los usuarios. Las bases de datos conectadas lógicamente aparecen como una sola base de datos para los usuarios. El modelo de base de datos distribuida permite que diferentes bases de datos situadas en ubicaciones remotas sean administradas individualmente por diferentes administradores de bases de datos. Una base de datos distribuida tiene características de escalabilidad, como equilibrio de carga y tolerancia a errores.

Objetivo:

Seguridad de activos

Subobsecución:

Proteger la privacidad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 2: Seguridad de activos, arquitectura y modelos DBMS

Pregunta #28 de 41

Id. de pregunta: 1104934

¿Qué define el nivel mínimo de seguridad?

- ✗ **A)** normas
- ✗ **B)** Procedimientos
- ✗ **C)** directrices
- ✓ **D)** Instantáneas

explicación

Una línea base define el nivel mínimo de seguridad y rendimiento de un sistema en una organización. Una línea de base también se utiliza como punto de referencia para futuros cambios. Cualquier cambio realizado en el sistema debe coincidir con la línea de base de seguridad mínima definida. Una línea de base de seguridad se define mediante la adopción de estándares en una organización.

Las directrices son las acciones que se sugieren cuando las normas no son aplicables en una situación particular. Las directrices se aplican cuando no se puede aplicar un estándar determinado para el cumplimiento de la seguridad. Se pueden definir directrices para la seguridad física, el personal o la tecnología en forma de prácticas recomendadas de seguridad.

Los estándares son las reglas obligatorias que rigen el nivel aceptable de seguridad para el hardware y el software. Las normas también incluyen el comportamiento regulado de los empleados. Las normas son aplicables y son las actividades y acciones que deben seguirse. Los estándares se pueden definir internamente en una organización o externamente como regulaciones.

Los procedimientos son las instrucciones detalladas utilizadas para lograr una tarea o un objetivo. Los procedimientos se consideran en el nivel más bajo de un programa de seguridad de la información porque están estrechamente relacionados con problemas de configuración e instalación. Los procedimientos definen cómo se implementará la directiva de seguridad en una organización a través de pasos repetibles. Por ejemplo, un procedimiento de copia de seguridad especifica los pasos que un custodio de datos debe seguir al realizar una copia de seguridad de datos

críticos para garantizar la integridad de la información empresarial. Se debe exigir al personal que siga los procedimientos para garantizar que las políticas de seguridad se apliquen plenamente.

La seguridad de los procedimientos garantiza la integridad de los datos.

Objetivo:
Seguridad de activos

Subobjetiva:
Establecer requisitos de información y manejo de activos

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 2: Seguridad de activos, líneas de base

---

Pregunta #29 de 41

Id. de pregunta: 1104927

Su empresa tiene una solución de copia de seguridad que realiza una copia de seguridad completa cada sábado por la noche y una copia de seguridad diferencial todas las demás noches. Un sistema vital se estrella el martes por la mañana. ¿Cuántas copias de seguridad se necesitarán restaurar?

✗ **A)** Tres
✗ **B)** Uno
✓ **C)** Dos
✗ **D)** Cuatro

explicación

Tendría que restaurar dos copias de seguridad si el sistema se bloquea el martes por la mañana. Las dos copias de seguridad que se deben restaurar son la copia de seguridad completa del sábado por la noche y la copia de seguridad diferencial del lunes por la noche. Cuando se usan copias de seguridad diferenciales en el plan de copia de seguridad, solo es necesario restaurar la copia de seguridad completa y la copia de seguridad diferencial más reciente.

Si el error se hubiera producido el domingo por la mañana, solo sería necesario restaurar la copia de seguridad completa. Si el error se produce cualquier otro día de la semana, sería necesario restaurar la copia de seguridad completa y la copia de seguridad diferencial más reciente.

Independientemente de si implementa una solución de copia de seguridad completa/diferencial o completa/incremental, siempre se necesita una copia de seguridad completa como copia de seguridad inicial de la solución.

Objetivo:

Seguridad de activos

Subobsecución:

Determinar los controles de seguridad de los datos

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 2: Seguridad de activos, tipos y esquemas de copia de seguridad de datos

---

Pregunta #30 de 41

Id. de pregunta: 1114685

Está desarrollando una nueva base de datos para su organización. La base de datos se utilizará para realizar un seguimiento del inventario de almacén. Debe asegurarse de que cada elemento de inventario se identifica de forma única en las tablas de base de datos. ¿Qué clave o claves debe utilizar?

a. Tupla

b. Extranjeros

c. primaria

d. atributo

e. célula

- ✗ **A)** opción c
- ✗ **B)** Opción d
- ✗ **C)** opción b
- ✗ **D)** opción e
- ✗ **E)** Sólo las opciones A y B
- ✗ **F)** opción A
- ✓ **G)** Sólo opciones B y C
- ✗ **H)** Sólo las opciones A y D

explicación

Debe utilizar claves principales y externas. Las claves principales y externas identifican de forma única un registro en una base de datos. Una clave principal identifica de forma única una fila de una tabla. Cuando un usuario solicita un acceso a un recurso, la base de datos realiza un seguimiento de la información mediante su clave principal única. Se selecciona una clave principal de un conjunto de claves candidatas.

Una clave externa hace referencia a un valor que existe en un atributo de una tabla y coincide con el valor de la clave principal de otra tabla. Es posible que el valor de clave externa no sea el valor de clave principal de su propia tabla, pero el valor de clave externa debe coincidir con el valor de clave principal de otra tabla.

Las filas y columnas de una base de datos relacional se conocen como tuplas y atributos, respectivamente. Las filas y columnas forman una tabla o un registro que contiene información. Un modelo de base de datos relacional utiliza atributos y tuplas para almacenar y organizar la información que pueden extraer los usuarios para cumplir con sus responsabilidades de trabajo en la base de datos. La tabla bidimensional en la que se almacenan los datos se conoce como relación base. En una base de datos, el número total de atributos de una tabla se conoce como grado y el número de tuplas se conoce como cardinalidad.

Una celda está en intersección de una fila y una columna. Algunas celdas pueden ser claves principales o externas, pero no todas las celdas lo son.

Una clave candidata identifica de forma única las filas y puede ser una combinación de más de un atributo para determinar la unicidad. Una relación base puede tener varias claves candidatas. La clave principal se define como una clave candidata. Una clave candidata es importante porque identifica tuplas individuales en una relación. Aunque realmente existe una relación dentro de la base de datos, una vista es una relación virtual que no se almacena en la base de datos.

Objetivo:
Seguridad de activos

Subobsecución:
Identificar y clasificar la información y los activos

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 2: Seguridad de activos, arquitectura y modelos DBMS

Pregunta #31 de 41

Id. de pregunta: 1113916

¿Qué instrucción describe correctamente las variables bind en lenguaje de consulta estructurado (SQL)?

- ✗ **A)** Las variables de enlace se utilizan para reemplazar valores en comandos SQL.
- ✗ **B)** Las variables de enlace implementan la seguridad de la base de datos.
- ✗ **C)** Las variables de enlace se utilizan para normalizar una base de datos.
- ✓ **D)** Las variables de enlace se utilizan para mejorar el rendimiento de la base de datos.

explicación

La variable Bind se utiliza para mejorar el rendimiento de la base de datos al permitir que una sola instrucción ejecute varias variables. Las variables de enlace son marcadores de posición para los valores enviados a un servidor de bases de datos en una consulta SQL. Las variables de enlace permiten la reutilización de instrucciones SQL emitidas anteriormente mediante la ejecución de un conjunto preparado de instrucciones con los parámetros proporcionados en tiempo de ejecución.

Las variables de enlace no implementan la seguridad en un sistema de administración de bases de datos. La seguridad de la base de datos se implementa mediante el lenguaje de control de datos (DCL).

Las variables de enlace no se utilizan para normalizar una base de datos. La normalización de bases de datos es un proceso de eliminación de datos duplicados de una base de datos. La normalización garantiza que los atributos de una tabla dependan únicamente de la clave principal.

Las variables de enlace no se utilizan para reemplazar los valores de los comandos SQL. Las variables de sustitución se utilizan para reemplazar los valores de los comandos de SQL PLUS.

Objetivo:
Seguridad de activos

Subobsecución:
Determinar los controles de seguridad de los datos

Referencias:

Cissp Cert Guide (3ª edición), Capítulo 2: Seguridad de activos, Bases de datos

Descripción de las variables de enlace en Oracle, http://www.techworld.com/applications/features/index.cfm?featureid=371

Pregunta #32 de 41

Id. de pregunta: 1104933

¿Cuál es la función principal de los medios de almacenamiento portátiles, como Zip, Jaz y unidades flash?

- ✓ **A)** para intercambiar datos
- ✗ **B)** Para modificar datos
- ✗ **C)** Para borrar datos
- ✗ **D)** para clasificar los datos

explicación

La función principal de los medios de almacenamiento portátiles, como las unidades Zip, las unidades Jaz, las unidades flash, las cajas SyQuest y Bernoulli, es facilitar el intercambio de datos entre una organización para

satisfacer los requisitos empresariales. Los medios de almacenamiento portátiles suelen ser los preferidos para los procesos de intercambio de datos debido a su naturaleza portátil y alta capacidad.

Borrar los datos de un medio de almacenamiento, como un disco duro, en realidad no elimina los datos, sino que sólo quita los punteros a la ubicación donde residen los datos en el medio de almacenamiento. Los datos borrados se pueden recuperar mediante el uso de procedimientos de recuperación de datos. La desinfección es el proceso de borrar los datos de los medios de almacenamiento para garantizar que los datos no se puedan recuperar y no se puedan reutilizar.

La modificación de los datos implica realizar cambios en la información. La modificación de datos puede ser autorizada o no autorizada por naturaleza.

La clasificación de datos implica asignar un nivel a los datos confidenciales e implementar contramedidas para mantener la confidencialidad, integridad y disponibilidad de los datos.

Por ejemplo, las organizaciones pueden clasificar los datos en confidenciales, privados, confidenciales y públicos. Esta clasificación se puede utilizar para implementar controles de seguridad.

Las directivas de seguridad de las operaciones para todos los tipos de medios de almacenamiento portátiles deben estar en su lugar para garantizar que los datos contenidos en estas unidades no se vean comprometidos. Las auditorías deben realizarse periódicamente para garantizar que se siguen las políticas de seguridad de las operaciones para los medios de almacenamiento portátiles. Esto garantizará que los empleados no retiren los medios de almacenamiento portátiles de sus instalaciones a menos que estén autorizados para hacerlo.

Objetivo:
Seguridad de activos

Subobjetiva:
Establecer requisitos de información y manejo de activos

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 2: Seguridad de activos, almacenamiento de datos y archivado

---

Pregunta #33 de 41

Id. de pregunta: 1104901

Debe asegurarse de que un conjunto de usuarios pueda acceder a la información relativa a los gastos departamentales. Sin embargo, cada usuario solo debe poder ver los gastos del departamento en el que trabaja. Los altos directivos deben poder ver los gastos de todos los departamentos. ¿Qué característica de seguridad de base de datos proporciona este control de acceso granular?

✗ **A)** guardar punto

✗ **B)** ruido y perturbación

✗ **C)** particionado

✓ **D)** vista de base de datos

explicación

La característica de seguridad de base de datos que proporciona este control de acceso granular son las vistas de base de datos. Las vistas de base de datos se utilizan para limitar el acceso de usuarios y grupos a cierta información en función de los privilegios de usuario y la necesidad de saber. Las vistas se pueden usar para restringir la información en función de la pertenencia a grupos, los derechos de usuario y las etiquetas de seguridad. Las vistas implementan privilegios mínimos y necesidad de conocer y proporcionan restricciones de acceso dependientes del contenido. Las vistas no proporcionan integridad referencial, que se proporciona mediante restricciones o reglas.

Un punto de almacenamiento no proporciona un control de acceso granular. Los puntos de almacenamiento garantizan la integridad y disponibilidad de los datos, pero no son una característica de seguridad de la base de datos. Los puntos de guardado se utilizan para garantizar que una base de datos pueda volver a un punto cuando el sistema se bloquea. Esto garantiza aún más la disponibilidad de los datos antes del error de la base de datos. Los puntos de guardado se pueden iniciar a una hora programada o mediante una acción del usuario durante el procesamiento de datos. La integridad de la base de datos también se puede proporcionar mediante la implementación de la integridad referencial, donde todas las claves externas hacen referencia a las claves principales existentes para identificar los registros de recursos de una tabla. La integridad referencial requiere que para cualquier atributo de clave externa, la relación a la que se hace referencia debe tener una tupla con el mismo valor para su clave principal.

La creación de particiones no proporciona un control de acceso granular. La creación de particiones es otra técnica de protección para garantizar la seguridad de la base de datos. La creación de particiones implica dividir la base de datos en muchas partes. La partición dificulta que un intruso recopile y combine información confidencial y deduzca hechos relevantes.

El ruido y la perturbación no proporcionan un control de acceso granular. La técnica de ruido y perturbación implementa la inserción de datos falsos para engañar a los atacantes y proteger la confidencialidad e integridad de la base de datos. La técnica de ruido y perturbación consiste en insertar información falsa aleatoria junto con registros válidos de la base de datos. Esta técnica altera los datos, pero permite a los usuarios acceder a la información relevante de la base de datos. Esta técnica crea suficiente confusión para que el atacante extraiga información confidencial.

Las vistas de base de datos son un ejemplo de control de acceso dependiente del contenido en el que el control de acceso se basa en la confidencialidad de la información y los privilegios de usuario concedidos. Esto conduce a una mayor sobrecarga en términos de procesamiento porque los datos se controlan granularmente por el contenido y los privilegios de los usuarios. Las vistas de base de datos pueden limitar el acceso de los usuarios a partes de datos en lugar de a toda la base de datos. Por ejemplo, durante el procesamiento de la base de datos en una organización, un jefe de departamento podría tener acceso solo a los datos de los empleados que pertenecen a ese departamento.

Objetivo:

Seguridad de activos

Subobsecución:

Identificar y clasificar la información y los activos

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 2: Seguridad de activos, vistas de base de datos

---

Pregunta #34 de 41

Id. de pregunta: 1104897

¿Qué suele formar parte de una política de información?

- ✗ **A)** autenticación
- ✗ **B)** uso aceptable
- ✗ **C)** procedimiento de terminación de empleados
- ✓ **D)** clasificación de la información

explicación

La clasificación de la información suele formar parte de una política de información. Una empresa generalmente tiene al menos dos clasificaciones de información: pública y propietaria. La información pública puede ser revelada al público, y la información de propiedad solo puede ser compartida con individuos que han firmado un acuerdo de confidencialidad. Algunas empresas también utilizan la clasificación restringida. Sólo un pequeño grupo de personas dentro de una empresa puede obtener acceso a información restringida. La piedra angular de una política de información bien definida es limitar el acceso individual a esa información que el individuo "necesita saber" para realizar las funciones requeridas.

La autenticación suele formar parte de la directiva de seguridad de una empresa. El uso aceptable suele formar parte de la directiva de uso del equipo de una empresa. Una política de uso aceptable normalmente estipula que los empleados de la empresa utilizan computadoras y otros equipos sólo con el fin de completar los proyectos de la empresa.

Un procedimiento de despido de empleados suele ser parte de las políticas de gestión de una empresa, que también incluyen procedimientos de nuevos empleados y empleados transferidos. Los procedimientos de terminación deben incluir la desactivación de la cuenta de acceso a la red de un usuario a más tardar al final del último día de la relación del empleado con la empresa.

Debido a que una red es vulnerable a los ataques de los empleados que están siendo despedidos, la mayoría de las empresas no proporcionan aviso previo a los empleados despedidos. También es una práctica común proporcionar una escolta para el empleado despedido desde el momento en que se le informa de la terminación hasta el momento

en que abandona las instalaciones de la empresa. Esta práctica limita la posibilidad de que la persona dañe el equipo de la empresa o dañe a otro personal. En el caso de una terminación hostil, es esencial que el acceso al sistema se elimine lo antes posible después de la terminación.

Objetivo:
Seguridad de activos

Subobsecución:
Identificar y clasificar la información y los activos

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 2: Seguridad de activos, datos y clasificación de activos

---

Pregunta #35 de 41

Id. de pregunta: 1104916

¿Cuál es el proceso de combinar varias bases de datos para formar una sola base de datos?

- ✗ **A)** mina de datos
- ✗ **B)** knowledge base
- ✓ **C)** almacén de datos
- ✗ **D)** metadatos

explicación

Un almacén de datos es el proceso de combinar varias bases de datos para formar una sola base de datos grande. Un almacén de datos es una recopilación de datos orientada a temas, integrada, con variantes de tiempo y no volátiles en apoyo del proceso de toma de decisiones de la administración. Los datos combinados se pueden utilizar para la recuperación de información y el análisis de datos. Este mecanismo permite a los usuarios consultar un único repositorio de información en lugar de varias bases de datos.

El almacenamiento de datos no solo aborda el archiving de información, sino que también se centra en presentar la información de una manera útil y comprensible a los usuarios de bases de datos. Esto se hace mediante la combinación de componentes de datos relacionados para proporcionar una imagen amplia de la información. Los almacenes de datos incluyen mecanismos que garantizan la recopilación, administración y uso adecuados de los datos. Un almacén de datos normalmente implementa controles para evitar que los metadatos sean utilizados de forma interactiva por usuarios no autorizados. Los datos se concilian a medida que se mueven entre el entorno de operaciones y el almacén de datos. Se supervisan todas las operaciones de purga de datos que se producen. La arquitectura de la información de almacenamiento de datos administra la recopilación de datos, pero no administra el archivado de datos.

Los metadatos son la información útil extraída de la base de datos existente mediante técnicas de minería de datos. Los metadatos proporcionan una visión de las relaciones de datos. Los metadatos son el resultado de nuevas correlaciones entre los componentes de datos. Este resultado se basa en las instrucciones del usuario.

Las técnicas de minería de datos se utilizan para extraer nueva información de la información existente. Las técnicas de minería de datos son útiles en áreas, como una oficina de crédito donde se monitorea el historial de crédito de un individuo antes de la aprobación de un préstamo. Es importante tener en cuenta que un almacén de datos combina varias bases de datos pero no admite la interrelación de los componentes de datos.

Knowledge base hace referencia a la recopilación de hechos, reglas y procedimientos y no está relacionada con el almacenamiento de datos.

Objetivo:
Seguridad de activos

Subobsecución:
Determinar los controles de seguridad de los datos

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 2: Seguridad de activos, almacenes de datos y minería de datos

---

Pregunta #36 de 41

Id. de pregunta: 1104913

¿Qué lenguaje de interfaz de base de datos reemplaza a conectividad abierta de bases de datos (ODBC) y sólo puede ser utilizado por los clientes de Microsoft Windows?

- ✓ **A)** OLE DB
- ✗ **B)** XML
- ✗ **C)** alboroto
- ✗ **D)** JDBC

explicación

Base de datos de vinculación e incrustación de objetos (OLE DB) es el lenguaje de interfaz de base de datos que reemplaza a ODBC y sólo lo pueden utilizar los clientes de Microsoft Windows. OLE es el modelo de objetos común (COM) que admite el intercambio de objetos entre programas. Un COM permite que dos componentes de software se comuniquen entre sí independientemente de sus sistemas operativos e idiomas de implementación.

ActiveX Data Objects (ADO) es un conjunto de interfaces ODBC que permiten a las aplicaciones cliente tener acceso a sistemas de base de datos back-end. Un desarrollador utilizará ADO para tener acceso a los servidores OLE DB. ADO

puede ser utilizado por muchos tipos diferentes de clientes.

Java Database Connectivity (JDBC) permite que una aplicación Java se comunique con una base de datos a través de ODBC o directamente. En lugar de utilizar ODBC, utiliza aplicaciones de base de datos Java.

El lenguaje de marcado extensible (XML) estructura los datos para que se puedan compartir fácilmente a través de Internet. Los exploradores web están diseñados para interpretar las etiquetas XML.

Objetivo:
Seguridad de activos

Subobsecución:
Determinar los controles de seguridad de los datos

Referencias:

Cissp Cert Guide (3ª edición),capítulo 2: Seguridad de activos, OLE DB

Pregunta #37 de 41

Id. de pregunta: 1192922

Algunos empleados de la organización deben tener acceso al equipo de prueba de comunicación como parte de su trabajo. Actualmente, todo este tipo de equipo se encuentra en un cajón de archivador desbloqueado. ¿Qué declaración se aplica BEST a este tipo de equipos?

✗ **A)** Su uso debería estar prohibido.
✗ **B)** El equipo se puede utilizar para controlar virus informáticos.
✗ **C)** Su uso debe restringirse a la alta dirección.
✓ **D)** Su uso debe ser controlado y monitoreado.

explicación

El equipo de prueba de comunicación se utiliza normalmente con fines experimentales antes de cualquier modificación en el entorno de producción. Su propósito principal es evitar la interrupción de las operaciones críticas del negocio debido a modificaciones. Algunos equipos de prueba de comunicación, como los rastreadores de red, se pueden utilizar para supervisar el tráfico de red.

Es una buena práctica controlar, supervisar, y autorizar estrictamente el acceso al equipo de prueba de la comunicación porque dicho equipo se puede utilizar incorrectamente para capturar el tráfico de red o para realizar actividades no autorizadas. Los controles de seguridad que se aplican a la infraestructura normal normalmente no se aplican al equipo de prueba en igual medida porque el equipo no está en un entorno de producción.

El acceso al equipo de prueba de comunicaciones debe estar debidamente autorizado y aprobado por la alta dirección, pero la alta dirección no utiliza realmente el equipo de prueba. El uso real del equipo de prueba de comunicación, como los rastreadores de red, generalmente se deja en manos del personal de TI.

El equipo de prueba de comunicación no se puede utilizar para controlar código malintencionado, como virus informáticos.

Objetivo:
Seguridad de activos

Subobjetiva:
Establecer requisitos de información y manejo de activos

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 2: Requisitos de seguridad, información y manejo de activos

---

Pregunta #38 de 41

Id. de pregunta: 1104894

¿Qué política define la sensibilidad de los datos de una empresa?

- ✗ **A)** una directiva de uso
- ✗ **B)** una directiva de copia de seguridad
- ✓ **C)** una política de información
- ✗ **D)** una directiva de seguridad

explicación

Una política de información define la sensibilidad de los datos de una empresa y los procedimientos adecuados para el almacenamiento, la transmisión, la eliminación y el marcado de los datos de una empresa. La piedra angular de la política de información de una empresa, al igual que con todas las políticas relacionadas con la seguridad, es conceder solo el acceso que se requiere para permitir que determinadas personas cumplan con sus responsabilidades.

Una política de información bien desarrollada se basará en la información sobre la separación de funciones para establecer diferentes niveles de acceso por función de grupo o responsabilidad individual. A las personas se les otorgará acceso solo a la información para la que tengan una "necesidad de saber" para lograr los objetivos de su posición. Una política de información es la directiva de la alta dirección para crear un programa de seguridad informática. Un ejemplo de una directiva de información es una decisión relativa al uso de la máquina de fax de la organización. Una directiva de información es una documentación de las decisiones de seguridad informática.

Una directiva de copia de seguridad define los procedimientos que se deben usar para realizar copias de seguridad de la información almacenada en la red de una empresa. Una directiva de seguridad define los medios técnicos que se utilizan para proteger los datos de una red. Una directiva de uso, a veces denominada directiva de uso aceptable, define la manera en que los empleados pueden usar el equipo y los recursos de red de una empresa, como el ancho de banda, el acceso a Internet y los servicios de correo electrónico.

Las políticas contienen condiciones de rendimiento esperado y consecuencias del incumplimiento. Una directiva de control de acceso detalla las directrices sobre los derechos, privilegios y restricciones para el uso de equipos y activos de la empresa.

Objetivo:
Seguridad de activos

Subobsecución:
Identificar y clasificar la información y los activos

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 2: Seguridad de activos, Política de datos

---

Pregunta #39 de 41

Id. de pregunta: 1104910

Está estableciendo los requisitos de manejo de medios, incluidos los procedimientos adecuados para marcar, etiquetar, almacenar y destruir los datos almacenados en medios digitales. Actualmente, le preocupa la capacidad de cualquier medio de almacenamiento que pueda utilizar. ¿Qué debe considerar como parte de este aspecto del medio de almacenamiento?

- ✗ **A)** con qué facilidad durará un medio determinado antes de que se deteriore
- ✓ **B)** El volumen de registros que puede almacenar en el medio
- ✗ **C)** cuánto tiempo soportará la industria varias opciones de medios
- ✗ **D)** Qué tan transportables deben ser los registros almacenados

explicación

La capacidad de cualquier medio de almacenamiento que utilice es el volumen de registros que puede almacenar en el medio.

La durabilidad es la facilidad con la que un determinado medio durará antes de que se deteriore. La longevidad es cuánto tiempo la industria apoyará varias opciones de medios. La portabilidad es lo transportables que deben ser los registros almacenados.

Objetivo:
Seguridad de activos

Subobsecución:
Garantizar una retención adecuada de activos

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 2: Seguridad de activos, marcado, etiquetado y almacenamiento

Directrices de administración de registros electrónicos,
http://www.mnhs.org/preserve/records/electronicrecords/erdigital.php

---

Pregunta #40 de 41

Id. de pregunta: 1114686

Debe asegurarse de que se mantiene un inventario completo de los activos de su organización. ¿Qué componentes son necesarios en el inventario de gestión de activos?

a. Versiones de firmware

b. Versiones del sistema operativo

c. Versiones de la aplicación

d. Dispositivos de hardware instalados

- ✗ **A)** opciones A y B
- ✗ **B)** Opción d
- ✗ **C)** opción b
- ✗ **D)** Opciones C y D
- ✗ **E)** opción c
- ✓ **F)** todas las opciones
- ✗ **G)** opción A

explicación

Todas las opciones son correctas. La administración de activos debe incluir un inventario completo de hardware y software. Esto incluye la versión del firmware, las versiones del sistema operativo y las versiones de la aplicación. Se debe inventariar todo el hardware y software de red, incluidos los servidores, los clientes y los dispositivos de red.

Tener un inventario completo de administración de activos garantizará que las actualizaciones de seguridad necesarias se administren de manera controlada. Sin un inventario completo, es posible que las actualizaciones de seguridad no

se implementen en los activos que las requieran, lo que da lugar a posibles infracciones de seguridad.

Los activos se consideran los activos físicos y financieros que son propiedad de la empresa. Ejemplos de activos comerciales que podrían perderse o dañarse durante un desastre son:

- Ingresos perdidos durante el incidente
- Costos de recuperación continuos
- Multas y sanciones en las que incurra el evento.
- Ventaja competitiva, credibilidad o buena voluntad dañada por el incidente

Objetivo:
Seguridad de activos

Subobsecución:
Determinar y mantener la información y la propiedad de los activos

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 2: Seguridad de activos, Gestión de activos

---

Pregunta #41 de 41

Id. de pregunta: 1111696

¿Qué instrucción describe mejor la normalización de datos?

✓ **A)** La normalización de datos garantiza que los atributos de una tabla de base de datos dependen de la clave principal.

✗ **B)** La normalización de datos ayuda a implementar la poliinstanciación.

✗ **C)** La normalización de datos implementa la fragmentación de datos y proporciona un acceso más rápido.

✗ **D)** La normalización de datos mejora la eficacia y el rendimiento de una base de datos.

explicación

La normalización de datos garantiza que los atributos de una tabla de base de datos dependan únicamente de la clave principal. La normalización es necesaria para evitar que aparezca información repetitiva en una base de datos. Esto hace que la base de datos sea coherente y fácil de mantener. La normalización es el proceso de eliminar datos redundantes de un sistema de administración de bases de datos relacionales y almacenar los datos en una única ubicación. La normalización proporciona vínculos a los componentes de datos siempre que sea necesario.

Los problemas relacionados con la normalización de una base de datos son los siguientes:

- Segregación de grupos relacionados en tablas separadas.
- Eliminar datos redundantes de todas las tablas de una base de datos.
- Asegurarse de que solo hay una clave principal por tabla y de que se puede hacer referencia a todos los atributos mediante esta clave principal.

El proceso de normalización debe llevarse a cabo con cuidado porque dividir los datos en varias tablas puede romper la coherencia en la recuperación de información de la base de datos y provocar una degradación del rendimiento. La desnormalización de la base de datos es el proceso de agregar la información redundante a las tablas para optimizar la coherencia y el rendimiento de la base de datos. La desnormalización de datos es diametralmente opuesta al proceso de normalización de datos. El propósito de la desnormalización de datos es aumentar la eficiencia del procesamiento.

La poliinstanciación es un método utilizado para garantizar que los usuarios con un nivel de acceso inferior no puedan acceder y modificar los datos categorizados para un nivel superior de acceso en una base de datos de varios niveles. Cuando se implementa la poliinstanciación, se crean dos objetos utilizando las mismas claves principales. Un objeto se rellena con información incorrecta y se considera no clasificado, y el otro objeto contiene la información clasificada original. Cuando un usuario con privilegios de nivel inferior intenta acceder al objeto, se dirige al usuario al objeto que contiene información incorrecta. La poliinstanciación se utiliza para ocultar información clasificada que existe en una base de datos y para engañar a los intrusos.

Objetivo:
Seguridad de activos

Subobsecución:
Determinar los controles de seguridad de los datos

Referencias:

Cissp Cert Guide (3ª edición), Capítulo 2: Seguridad de activos, Bases de datos