Domain 1 - Security and Risk Management

Test ID: 160498066

Pregunta #1 de 137

Id. de pregunta: 1111689

Como administrador de seguridad de su organización, está revisando los resultados de la auditoría para evaluar si se mantienen las líneas de base de seguridad de su organización. ¿En qué fase del ciclo de vida de la gestión de la seguridad está participando?

✗ **A)** instrumento

✗ **B)** Planificar y organizar

✓ **C)** Supervisar y evaluar

✗ **D)** Operar y mantener

explicación

Participa en la fase supervisar y evaluar del ciclo de vida de la administración de seguridad. Esta fase incluye los siguientes componentes:

- Revise los registros, los resultados de la auditoría, las métricas y los acuerdos de nivel de servicio.
- Evaluar los logros.
- Completar las reuniones trimestrales del comité directivo.
- Desarrollar pasos de mejora para la integración en la fase planificar y organizar.
- La revisión de las auditorías no forma parte de ninguna de las otras fases.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender y aplicar los conceptos de gestión de riesgos

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Ciclo de vida del programa de seguridad y gestión de riesgos

Pregunta #2 de 137

Id. de pregunta: 1192906

Al configurar una nueva red, decide utilizar enrutadores y cifrado para mejorar la seguridad. ¿De qué tipo de control técnico es este un ejemplo?

✗ **A)** disuasivo

✗ **B)** compensativo

✗ **C)** detective

✗ **D)** directiva

✗ **E)** recuperación

✓ **F)** preventivo

✗ **G)** correctivo

explicación

Los enrutadores y el cifrado son ejemplos de controles técnicos preventivos. Un control técnico es un control que restringe el acceso. Un control preventivo evita brechas de seguridad. Los routers y el cifrado también son controles técnicos compensativos.

Los controles técnicos preventivos se configuran con mayor frecuencia mediante listas de control de acceso (ACL) integradas en el sistema operativo. Protegen el sistema operativo del acceso, la modificación y la manipulación no autorizados. Protegen la integridad y disponibilidad del sistema al limitar el número de usuarios y procesos a los que se permite acceder al sistema o a la red.

Un control técnico de recuperación puede restaurar las capacidades del sistema. Las copias de seguridad de datos se incluyen en esta categoría.

Un control técnico detective puede detectar cuándo se produce una violación de seguridad. Los registros de auditoría y los sistemas de detección de intrusiones (IDS) se incluyen en esta categoría.

Un control técnico disuasorio es aquel que desalienta las brechas de seguridad. Un firewall es el mejor ejemplo de este tipo de control.

Un control técnico correctivo es aquel que corrige cualquier problema que surja debido a las brechas de seguridad. El software antivirus y las imágenes de servidor también se incluyen en esta categoría.

Un control técnico compensativo es aquel que se considera una alternativa a otros controles.

Hay tres categorías de control de acceso: controles técnicos, administrativos y físicos. Se ha establecido un control técnico para restringir el acceso. Los controles técnicos funcionan para proteger el acceso al sistema, la arquitectura y el acceso a la red, las zonas de control, la auditoría y el cifrado y los protocolos. Un administrativo se desarrolla para dictar cómo se implementan las políticas de seguridad para cumplir con los objetivos de seguridad de la empresa. Los controles administrativos incluyen políticas y procedimientos, controles de personal, estructura de supervisión, capacitación en seguridad y pruebas. Un control físico se implementa para proteger el acceso físico a un objeto, como un edificio, una sala o un equipo. Los controles físicos incluyen insignias, cerraduras, guardias, segregación de red, seguridad perimetral, controles informáticos, separación de áreas de trabajo, copias de seguridad y cableado.

Las tres categorías de control de acceso proporcionan siete funcionalidades o propósitos diferentes:

- Preventivo - Un control preventivo previene brechas de seguridad y evita riesgos.
- Detective - Un control detective detecta las brechas de seguridad a medida que ocurren.
- Correctivo : un control correctivo restaura el control e intenta corregir cualquier daño infligido durante una infracción de seguridad.
- Disuasión - Un control disuasorio disuade posibles violaciones.
- Recuperación: un control de recuperación restaura los recursos.
- Compensativo: un control compensativo proporciona un control alternativo si otro control puede ser demasiado costoso. Por lo general, todos los controles se consideran compensativos.
- Directiva - Un control de directiva proporciona controles obligatorios basados en regulaciones o requisitos ambientales.

Cada categoría de control incluye controles que proporcionan funciones diferentes. Por ejemplo, una insignia de seguridad es tanto un control físico preventivo como un control físico compensativo. La supervisión y supervisión es tanto un control administrativo detectivesco como un control administrativo compensativo.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender y aplicar los conceptos de gestión de riesgos

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 1: Seguridad y Gestión de Riesgos, Preventiva

---

Pregunta #3 de 137

Id. de pregunta: 1104794

Trabaja para una empresa que se encuentra en los Estados Unidos. Se le ha pedido que se asegure de que se siguen los requisitos de puerto seguro para garantizar la privacidad de los datos. ¿En qué ubicación se exigen estos requisitos?

✗ **A)** Organización de las Naciones Unidas
✗ **B)** Estados Unidos
✓ **C)** Europa
✗ **D)** Asia

explicación

Los requisitos de puerto seguro son obligatorios en Europa. Europa tiene regulaciones que protegen la información de privacidad que son mucho más estrictas que los Estados Unidos y otros países o regiones.

Ninguna de las otras ubicaciones enumeradas exige los requisitos de puerto seguro.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender los problemas legales y reglamentarios relacionados con la seguridad de la información en un entorno global

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Unión Europea

---

Pregunta #4 de 137

Id. de pregunta: 1104826

La administración le ha solicitado que implemente controles que tomen medidas correctivas contra las amenazas. ¿Qué entidad es un ejemplo de este tipo de control?

- ✓ **A)** planificación de la continuidad del negocio
- ✗ **B)** Backups
- ✗ **C)** separación de funciones
- ✗ **D)** pistas de auditoría

explicación

La planificación de la continuidad del negocio es un ejemplo de control correctivo. Los controles correctivos son controles que toman medidas correctivas contra las amenazas.

Las pistas de auditoría son un ejemplo de controles detectivesco. Los controles detectivesco son controles que detectan amenazas.

Las copias de seguridad son un ejemplo de recuperación y controles compensativos. Los controles de recuperación son controles que se recuperan de un incidente o error. Los controles compensativos son controles que proporcionan una medida alternativa de control. Para restaurar un sistema y sus archivos de datos después de un error del sistema, debe implementar los procedimientos de recuperación. Los procedimientos de recuperación podrían incluir los pasos adecuados para reconstruir un sistema desde el principio y aplicar los parches y configuraciones necesarios.

La separación de funciones es un ejemplo de control preventivo.

Los controles de las directivas son controles que dicen a los usuarios lo que se espera de ellos y lo que se considera inapropiado. Los controles de recuperación son controles que describen las acciones que se deben realizar para restaurar un sistema a su estado normal después de que se produzca un desastre.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Identificar, analizar y priorizar los requerimientos de Continuidad del Negocio (BC, Business Continuity)

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Planificación de continuidad y el Plan de Continuidad del Negocio (BCP)

Pregunta #5 de 137

Id. de pregunta: 1113898

¿Cuál es la definición correcta de un agregador de datos?

- ✗ **A)** una empresa que regula la información personal
- ✗ **B)** una empresa que analiza información personal
- ✗ **C)** una empresa que protege la información personal
- ✓ **D)** una empresa que compila, almacena y vende información personal

explicación

Un agregador de datos es una empresa que compila, almacena y vende información personal. A menudo estas empresas compilan perfiles de esta información.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender los problemas legales y reglamentarios relacionados con la seguridad de la información en un entorno global

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 1: Seguridad y Gestión de Riesgos, Privacidad

---

Pregunta #6 de 137

Id. de pregunta: 1192901

Haga clic en cada uno de los encabezados del escenario para expandir o contraer su contenido. Debe leer todo el escenario para responder a la pregunta.

fondo

Usted es un profesional de la seguridad contratado recientemente por una empresa que cotiza en bolsa para ayudar a administrar la seguridad de la organización. La compañía tiene una oficina principal en Atlanta, GA, y sucursales en todo el sureste de los Estados Unidos. El departamento de TI tiene un pequeño personal alojado en la oficina de Atlanta.

Temas actuales

El año pasado, una tormenta invernal cerró las operaciones en la mayoría de sus oficinas. Si bien ninguna de sus instalaciones fue destruida y las operaciones normales se restauraron en 24 horas, a la administración le preocupa que no exista un plan de recuperación ante desastres. Se le ha pedido que prepare un plan para cubrir este tipo de interrupción.

Actualmente, su organización mantiene varias bases de datos grandes de contenido digital que son vitales para las operaciones de su organización. Se utilizan diferentes controles para administrar este contenido. La administración le ha pedido que implemente una solución para controlar la apertura, edición, impresión o copia de estos datos de una manera más centralizada.

En los próximos seis meses, su empresa planea mover todos los servidores y granjas de servidores a un centro de datos centralizado. El centro de datos ocupará el tercer piso de un edificio de seis pisos que actualmente está en construcción. La administración le ha pedido que se asegure de que el acceso al centro de datos esté estrictamente controlado. Durante ese mismo tiempo, es probable que su organización compre un competidor para fusionarse con su organización existente.

Recientemente, uno de los servidores de la intranet fue víctima de un ataque de denegación de servicio (DoS). El departamento de TI tardó más de 24 horas en volver a poner en funcionamiento el servidor. Durante ese tiempo, el personal de la oficina principal no pudo acceder a la importante información sobre recursos humanos disponible en el servidor de la intranet afectado.

La semana pasada, descubrió que se utilizaron varias cuentas de usuario en un intento de piratear su red. Afortunadamente, las cuentas fueron bloqueadas debido a intentos de inicio de sesión no válidos. Revise los registros y determine que tres de las cuentas se crearon para el personal que ya no está empleado por su organización.

Después de presionar durante años, ha recibido permiso de la administración para diseñar e implementar un programa integral de concienciación de seguridad en toda la organización.

¿Cuál es la clasificación del ataque que se ha producido contra el servidor de la intranet?

- ✗ **A)** delitos informáticos incidentales
- ✓ **B)** delitos dirigidos por computadoras

✗ **C)** delitos informáticos de prevalencia

✗ **D)** delitos asistidos por computadora

explicación

El ataque que se ha producido contra el servidor de intranet es un delito dirigido al equipo. El servidor de la intranet es víctima de un ataque de denegación de servicio (DoS). Un delito dirigido a la computadora se produce cuando una computadora es víctima de un ataque donde el único propósito es dañar la computadora o su propietario.

Un delito asistido por ordenador se produce cuando un ordenador es la herramienta que se utiliza para llevar a cabo el delito. Un ejemplo de muchos de los ataques actuales de robo de identidad que tienen lugar hoy en día. Los ordenadores facilitan mucho la realización de este tipo de ataques, y a menudo se utiliza un ordenador como medio para obtener la información de identidad.

Un delito informático incidental se produce cuando un equipo está involucrado sin ser la víctima o atacantes. En la mayoría de los casos, las computadoras solo se utilizan para almacenar información y se incautan para proporcionar pruebas o un rastro de cómo se llevó a cabo el delito.

Un delito de prevalencia informática se produce porque las computadoras son ampliamente utilizadas. Un ejemplo de este delito es la piratería de software.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Desarrollar, documentar e implementar políticas, estándares, procedimientos y directrices de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Cuestiones Legales y Regulatorias

Delitos informáticos, http://www.lectlaw.com/files/cri14.htm

Pregunta #7 de 137

Id. de pregunta: 1192898

Está diseñando las directivas de administración de usuarios para su organización. ¿Qué es típicamente parte de estas políticas?

✗ **A)** clasificación de la información

✓ **B)** despido de empleados

✗ **C)** autenticación

✗ **D)** uso aceptable

explicación

Los procedimientos de despido de empleados suelen formar parte de las políticas de gestión de usuarios de una empresa, que también incluyen procedimientos para tratar con nuevos empleados y empleados transferidos.

La clasificación de la información suele estar cubierta por una política de información. Una empresa suele tener un mínimo de dos clasificaciones para la información: pública y privada. La mayoría de las compañías definen la información pública como información que puede ser revelada a cualquier persona, y la información propietaria como información que solo se puede compartir con los empleados que han firmado un acuerdo de confidencialidad. La directiva de seguridad de una empresa normalmente contiene procedimientos de autenticación estándar. Las directivas de uso aceptable, que indican la manera en que los empleados pueden usar los recursos de la empresa, forman parte de la directiva de uso del equipo de una empresa.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Determinar los requisitos de cumplimiento

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Políticas de incorporación de empleados de gestión de riesgos y seguridad

---

Pregunta #8 de 137

Id. de pregunta: 1111653

Debe asegurarse de que su organización cumple con los principios europeos de privacidad. ¿Qué declaración NO es uno de los principios?

- ✗ **A)** El motivo de la recopilación de datos debe indicarse cuando se recopilan los datos.
- ✗ **B)** No se deben recopilar datos que no sean necesarios.
- ✓ **C)** Los datos pueden ser utilizados para otros fines que no sean los específicamente establecidos en la recopilación.
- ✗ **D)** Los datos solo deben conservarse mientras sean necesarios para realizar una tarea declarada.

explicación

Los datos no se pueden utilizar para otros fines que no sean los específicamente indicados en la recopilación.

Los Principios Europeos de Privacidad son los siguientes:

- El motivo de la recopilación de datos debe indicarse cuando se recopilan los datos.
- Los datos no se pueden utilizar para otros fines que no sean los específicamente indicados en la recopilación.
- No se deben recopilar datos que no sean necesarios.
- Los datos solo deben conservarse mientras sean necesarios para realizar una tarea declarada.
- Solo las personas que están obligadas a realizar una tarea declarada deben tener acceso a los datos.
- Las personas responsables de almacenar de forma segura los datos no deben permitir la filtración involuntaria de datos.
- Las personas tienen derecho a recibir un informe sobre la información que se tiene sobre ellas.
- La transmisión de datos de información personal a lugares donde no se puede garantizar una protección de datos personales equivalente está prohibida.
- Las personas tienen derecho a corregir los errores contenidos en sus datos personales.

Los principios de notificación, elección, acceso, seguridad y aplicación se refieren a la privacidad.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender los problemas legales y reglamentarios relacionados con la seguridad de la información en un entorno global

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Unión Europea

---

Pregunta #9 de 137

Id. de pregunta: 1111668

El equipo de continuidad del negocio está entrevistando a los usuarios para recopilar información sobre las unidades de negocio y sus funciones. ¿Qué parte del plan de continuidad del negocio incluye este análisis?

✗ **A)** plan de recuperación ante desastres
✗ **B)** plan de emergencia para ocupantes (OEP)
✗ **C)** plan de contingencia
✓ **D)** análisis de impacto en el negocio (BIA)

explicación

El análisis de impacto empresarial (BIA) incluye entrevistas para recopilar información sobre las unidades de negocio y sus funciones.

Se crea un plan de recuperación ante desastres para garantizar que su empresa pueda reanudar sus operaciones de manera oportuna. Las entrevistas no se incluyen como parte de su desarrollo.

Se crea un plan de contingencia para detallar cómo se llevarán a cabo todas las funciones comerciales en caso de una interrupción o desastre. Debe abordar los riesgos residuales. Las entrevistas no se incluyen como parte de su desarrollo.

Se crea un plan de emergencia para ocupantes (OEP, por sus, para garantizar que las lesiones y la pérdida de vidas se minimicen cuando se produce una interrupción o un desastre). También se centra en los daños a la propiedad. Las entrevistas no se incluyen como parte de su desarrollo.

Se crea un BIA para identificar las funciones vitales y priorizarlas en función de la necesidad. Se identifican las vulnerabilidades y amenazas, y se calculan los riesgos. Es una metodología comúnmente utilizada en la planificación de la continuidad del negocio. Su objetivo principal es ayudar a las unidades de negocio a comprender cómo un evento afectará a las funciones corporativas, sin la recomendación de una solución adecuada. El propósito de la BIA es crear un documento para entender qué impacto tendría un evento disruptivo en el negocio.

Uno de los primeros pasos en el BIA es identificar las unidades de negocio. La etapa de recopilación de información de la BIA incluye decidir qué técnicas utilizar (encuestas o entrevistas), seleccionar a las personas que planea entrevistar y personalizar la técnica para recopilar la información adecuada. La etapa analítica de la BIA incluye el análisis de la información recopilada, la determinación de las funciones críticas del negocio, el impacto económico máximo tolerable (MTD) de la interrupción y la priorización de la restauración de las funciones críticas del negocio. Esto conduce al establecimiento de un objetivo de tiempo de recuperación (RTO) para cada unidad o elemento. La etapa de documentación incluye la documentación de los hallazgos y la presentación de informes a la administración. Un BIA incluye los siguientes pasos:

- Analizar las amenazas asociadas a cada área funcional
- Determinación del riesgo asociado con cada amenaza
- Identificación de las principales áreas funcionales de la información

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Identificar, analizar y priorizar los requerimientos de Continuidad del Negocio (BC, Business Continuity)

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Análisis de Impacto en el Negocio (BIA)

Pregunta #10 de 137

Id. de pregunta: 1104874

¿Qué tipo de control es un ejemplo de un control detective?

- ✓ **A)** circuito cerrado de televisión (CCTV)
- ✗ **B)** cortafuegos
- ✗ **C)** tarjeta inteligente
- ✗ **D)** cerco

explicación

El circuito cerrado de televisión (CCTV) es un tipo de control detectivesco que es utilizado por los guardias para evitar el acceso no autorizado a la instalación. Los CCTVs aumentan la visibilidad al permitir que los guardias supervisen diferentes zonas de la instalación desde una ubicación centralizada y tomen medidas correctivas para evitar el acceso no autorizado o la violación de la seguridad.

Las vallas y las tarjetas inteligentes son ejemplos de controles preventivos que bloquean el acceso no autorizado a las instalaciones. La valla y los guardias no son controles detectivescos.

Un firewall es un control técnico preventivo que regula el tráfico de red entre diferentes zonas de acuerdo con la directiva de seguridad de red de una organización. Un firewall impide el acceso no autorizado a la red.

Los controles de seguridad se pueden clasificar en preventivos, detectives, correctivos, disuasorios, de recuperación y compensación. Cada uno de estos controles se puede clasificar en controles físicos, administrativos y técnicos.

Se implementa un control preventivo para evitar una brecha de seguridad o una interrupción de los servicios críticos antes de que puedan ocurrir. Ejemplos de controles preventivos físicos son las iluminaciones, los sistemas biométricos, las vallas, los sistemas de insignias, las puertas de mantrap y el personal de seguridad. Ejemplos de controles preventivos administrativos son las políticas de seguridad, la supervisión y supervisión, la rotación de puestos de trabajo, la clasificación de la información y los procedimientos de personal. Algunos ejemplos de controles técnicos preventivos son los enrutadores, las listas de control de acceso, el cifrado, el software antivirus, los firewalls y las tarjetas inteligentes.

Un control detective detecta la intrusión a medida que se produce. Ejemplos de controles físicos de detectives incluyen guardias de seguridad, detectores de movimiento, CCTVs y alarmas. Ejemplos de controles de detección administrativa incluyen monitoreo y supervisión, rotación de trabajos, investigaciones de antecedentes, pruebas y capacitación en conciencia de seguridad. Los registros de auditoría, los IDs, el software antivirus y los firewalls son ejemplos de controles técnicos de detectives.

Los controles correctivos son las contramedidas utilizadas para corregir eventos indeseables que han ocurrido. Algunos ejemplos son los sistemas antivirus y de detección de intrusiones (IDS).

Un control disuasorio se utiliza para disuadir una infracción de seguridad. Ejemplos de controles disuasorios físicos son las vallas, las cerraduras, los sistemas de insignias, las puertas de mantrap, los CCTVs, las alarmas y el personal de seguridad. Ejemplos de controles administrativos disuasorios son la supervisión y supervisión, la capacitación en

materia de concienciación sobre la seguridad y los procedimientos del personal. Ejemplos de controles técnicos disuasorios son el cifrado y los cortafuegos.

Los controles de recuperación se utilizan para restablecer los recursos y servicios perdidos. Una copia de seguridad es un ejemplo de un control físico de recuperación. Un ejemplo de un control técnico de recuperación es una copia de seguridad de datos.

Los controles de compensación se incluyen en la categoría de control administrativo compensatorio. Ejemplos de controles compensatorios incluyen monitoreo, supervisión y procedimientos de personal.

Al usar CCTV, debe considerar el área que desea observar. La profundidad de campo hace referencia a la parte del entorno que está en foco cuando se muestra en el monitor. La profundidad de campo varía dependiendo del tamaño de la abertura de la lente, la distancia del objeto en el que se enfoca y la distancia focal de la lente. La profundidad de campo aumenta a medida que disminuye el tamaño de la abertura de la lente, aumenta la distancia del sujeto o disminuye la distancia focal de la lente. Si desea cubrir un área grande y no enfocar en elementos específicos, lo mejor es usar una lente gran angular y una abertura de lente pequeña. Las lentes Zoom llevarán a cabo la funcionalidad de enfoque automáticamente. Se debe utilizar una lente de iris automático en entornos donde la luz cambia, como un ajuste al aire libre.

La mayoría de los sistemas cctv actuales utilizan dispositivos acoplados a carga. Estos dispositivos reciben la entrada a través de las lentes y las convierten en una señal electrónica. Capturan señales en el rango infrarrojo. Proporcionan imágenes de mejor calidad que otros tipos.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender y aplicar los conceptos de gestión de riesgos

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 1: Seguridad y Gestión de Riesgos, Detective

---

Pregunta #11 de 137

Id. de pregunta: 1111642

Como responsable de seguridad de su organización, actualmente está completando auditorías para asegurarse de que la configuración de seguridad cumple con las líneas de base establecidas. ¿En qué fase del ciclo de vida de la gestión de la seguridad está participando?

✗ **A)** Supervisar y evaluar

✗ **B)** Planificar y organizar

✓ **C)** Operar y mantener

✗ **D)** instrumento

explicación

Está involucrado en la fase operar y mantener del ciclo de vida de administración de seguridad. Esta fase incluye los siguientes componentes:

- Asegúrese de que se cumplen todas las líneas base.
- Completar auditorías internas y externas.
- Complete las tareas descritas en los blueprints.
- Administre los acuerdos de nivel de servicio como se describe en los blueprints.

Completar las auditorías no forma parte de ninguna de las otras fases.

El oficial de seguridad de la información es responsable de la administración diaria de la seguridad.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
evaluar y aplicar los principios de gobierno de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y gestión de riesgos, Ciclo de vida del programa de seguridad

---

Pregunta #12 de 137

Id. de pregunta: 1104765

Se le ha pedido que diseñe un programa de seguridad. ¿Qué enfoque debe utilizar?

✗ **A)** enfoque ascendente
✓ **B)** enfoque de arriba hacia abajo
✗ **C)** enfoque jerárquico
✗ **D)** enfoque intermedio

explicación

Al diseñar un programa de seguridad, debe utilizar un enfoque descendente. Esto garantiza que todas las iniciativas provenan de la alta dirección y se aloen camino a través de la dirección intermedia hasta el resto del personal. Si un programa de seguridad no utiliza este enfoque, probablemente se producirá un error.

Un enfoque ascendente se produce cuando el departamento de TI tiene que implementar un programa de seguridad sin el inicio o el soporte de la alta dirección. Este enfoque es menos eficaz que el enfoque descendente.

Las otras dos opciones no son válidas.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
evaluar y aplicar los principios de gobierno de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y gestión de riesgos, enfoque de arriba hacia abajo frente a bottom-up

---

Pregunta #13 de 137

Id. de pregunta: 1104780

El sitio web de su organización sigue las directrices del Proyecto de preferencias de privacidad (Platform for Privacy Preferences Project) para la privacidad del usuario en su sitio web público. ¿Qué organización desarrolló P3P?

- ✓ **A)** World Wide Web Consortium (W3C)
- ✗ **B)** Unión Europea
- ✗ **C)** Placa de arquitectura de Internet (IAB)
- ✗ **D)** Asociación de protección de software (SPA)

explicación

El World Wide Web Consortium (W3C) desarrolló el Proyecto de Plataforma de Preferencias de Privacidad (P3P) para la privacidad del usuario en los sitios Web. Cada sitio que adopte P3P tendrá su propia declaración de privacidad que los usuarios deben leer. W3C permite a los sitios Web expresar sus prácticas de privacidad en un formato estándar que puede ser recuperado automáticamente e interpretado fácilmente por los agentes de usuario. Permite a los usuarios estar informados de las prácticas del sitio en formato legible por humanos. Automatiza la toma de decisiones en función de las prácticas de privacidad del sitio cuando es apropiado.

El Internet Architecture Board (IAB) coordina el diseño, la ingeniería y la administración de Internet. Supervisa el Grupo de Trabajo de Ingeniería de Internet (IETF). La IAB emite directrices de uso de Internet relacionadas con la ética.

La Unión Europea (UE) ha desarrollado sus propios Principios de la UE sobre privacidad, que enumeran seis áreas que abordan el uso y la transmisión de información que es de naturaleza sensible.

La Asociación de Protección de Software (SPA) se ocupa principalmente de la piratería de software.

Objetivo:

Seguridad y gestión de riesgos

Subobsecución:

Determinar los requisitos de cumplimiento

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 1: Seguridad y Gestión de Riesgos, Cumplimiento

P3P: El proyecto de la plataforma para las preferencias de privacidad, http://www.w3.org/P3P/

Pregunta #14 de 137

Id. de pregunta: 1104799

¿Qué afirmación es cierta de un refugio de datos?

- ✗ **A)** Un país conocido como un paraíso de datos no tiene leyes en absoluto.
- ✗ **B)** Un refugio de datos es un término alternativo para la agrupación en clústeres de servidores.
- ✗ **C)** Un refugio de datos no puede ser ni un ordenador ni una red.
- ✓ **D)** Un refugio de datos no tiene leyes o leyes mal aplicadas para la protección de la información.

explicación

Un refugio de datos se refiere a un país u otro lugar sin leyes o leyes mal aplicadas para la protección de la información. El término paraíso de datos fue acuñado por Bruce Sterling en 1989. Un refugio de datos implica una concentración de datos ilícitos en servidores informáticos. Estos datos ilícitos están más allá de la ley de protección de derechos de autor.

Un refugio de datos también puede ser un sistema informático o una red que proporciona protección de la información a través de métodos, como el cifrado. Un refugio de datos se encuentra en un lugar que está fuera de la jurisdicción de las leyes. Estos países no tienen tratados de extradición. Por lo tanto, los delincuentes no pueden ser presentados ante un tribunal de justicia.

Muchos paraísos de datos tienen leyes. Sin embargo, generalmente no tienen leyes de protección de la información.

La agrupación en clústeres de servidores hace referencia a una granja de servidores. No está relacionado con los refugios de datos.

Sealand, un micro-principado en Europa, es un ejemplo de un refugio de datos. Sealand casi no tiene leyes para la protección de datos. Una empresa llamada HavenCo en Sealand proporciona el refugio de datos para fines de alojamiento de datos internacionales.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender los problemas legales y reglamentarios relacionados con la seguridad de la información en un entorno global

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Unión Europea

Asilo de datos, http://www.worldwidewords.org/turnsofphrase/tp-dat2.htm

---

Pregunta #15 de 137

Id. de pregunta: 1111687

¿Qué opción NO es un elemento de control físico detectivesco?

✗ **A)** Cctv
✗ **B)** sensores
✓ **C)** generador de movimiento
✗ **D)** detector de movimiento de patrón de onda

explicación

Los generadores de movimiento no son controles físicos detectives desplegados para asegurar una instalación. Un generador de movimiento no es una categoría válida de controles físicos detectivesco.

Los controles físicos del detective incluyen los siguientes elementos:

- Sensores: supervisa los eventos y envía las anomalías detectadas al software de monitoreo centralizado
- Detectores de movimiento, como el detector de movimiento de patrón de onda, el detector de capacitancia y el detector de audio: detecta cambios en un entorno en función de diferentes parámetros, como el movimiento de un sujeto, los patrones de onda, etc.
- Televisores de circuito cerrado (CCTVs): Monitoree las diferentes áreas de la instalación desde una ubicación centralizada para ayudar al personal de seguridad
- Alarmas: Notifique inmediatamente a las autoridades competentes sobre eventos anormales

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender y aplicar los conceptos de gestión de riesgos

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 1: Seguridad y Gestión de Riesgos, Tipos de Control

---

Pregunta #16 de 137

Id. de pregunta: 1104801

En los últimos años, muchas empresas han cometido fraude al proporcionar a sabiendas informes financieros inexactos a los accionistas y al público. ¿Qué ley se escribió para abordar esta situación?

- ✗ **A)** HIPAA
- ✗ **B)** GLBA
- ✓ **C)** Sox
- ✗ **D)** Basilea II

explicación

La Ley Sarbanes-Oxley (SOX) de 2002 se redactó para impedir que las empresas de los Estados Unidos cometieran fraude al proporcionar a sabiendas informes financieros inexactos a los accionistas y al público. Se ocupa principalmente de las prácticas contables corporativas. El artículo 404 de esta ley se refiere específicamente a la tecnología de la información.

La Ley Gramm-Leach-Bliley (GLBA) de 1999 fue escrita para garantizar que las instituciones financieras desarrollen avisos de privacidad y permitan a sus clientes evitar que las instituciones financieras compartan información con terceros.

La Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA, por sus contra, por sus contralo, por susta- fue escrita para evitar que las organizaciones médicas (incluidas las compañías de seguros de salud, hospitales y consultorios médicos) compartan información médica del paciente sin consentimiento. Se ocupa principalmente de la seguridad, integridad y privacidad de la información del paciente.

El Acuerdo de Basilea II se basa en tres pilares principales: requisitos mínimos de capital, supervisión y disciplina de mercado. Estos pilares se aplican a las instituciones financieras.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender los problemas legales y reglamentarios relacionados con la seguridad de la información en un entorno

global

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Ley Sarbanes-Oxley (SOX)

Pregunta #17 de 137

Id. de pregunta: 1104833

¿Qué tipo de aplicación sirve como núcleo para las operaciones empresariales de una organización?

- ✗ **A)** una aplicación de confianza
- ✗ **B)** una aplicación obligatoria
- ✗ **C)** una aplicación urgente
- ✓ **D)** una aplicación crítica

explicación

Una aplicación crítica sirve como un núcleo para las operaciones comerciales de una organización y debe permanecer operativa todo el tiempo para la operación continua de una organización y la generación de ingresos.

La recuperación ante desastres y la planificación de la continuidad del negocio implican la identificación de sistemas críticos y funciones empresariales que se pueden implementar en toda la organización en caso de que se produzca un error o un desastre.

Confiable, obligatorio y urgente son términos genéricos y no se aplican a las aplicaciones que son vitales para las operaciones comerciales de una organización.

Para garantizar un funcionamiento continuo y sin problemas, debe emplearse un mecanismo de copia de seguridad para dichos sistemas y áreas funcionales. Esto garantizará la disponibilidad de la infraestructura necesaria para realizar las tareas vitales para las operaciones comerciales de una organización.

Es importante que una organización realice un análisis inicial del impacto en el negocio para determinar las aplicaciones clave y las funciones empresariales, las interdependencias del departamento, el tiempo de inactividad máximo tolerable para los activos críticos y las contramedidas correspondientes que se implementarán. Esto permitirá a una empresa reanudar las operaciones comerciales de manera efectiva en caso de un desastre.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Identificar, analizar y priorizar los requerimientos de Continuidad del Negocio (BC, Business Continuity)

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Análisis de Impacto en el Negocio (BIA)

Pregunta #18 de 137

Id. de pregunta: 1104781

¿Qué afirmación es cierta de Tripwire?

- ✗ **A)** Actúa como un sistema de control de acceso centralizado para el mantenimiento de cuentas de usuario.
- ✗ **B)** Por lo general, es utilizado por los hackers para realizar intrusiones.
- ✗ **C)** Aumenta el rendimiento de los sistemas.
- ✓ **D)** Supervisa el cambio en la configuración de línea base de un sistema.

explicación

El propósito principal de Tripwire es monitorear la configuración de línea base de un sistema y los cambios realizados en él. Los cambios o modificaciones en el sistema operativo y en los programas de aplicación se supervisan manteniendo un valor de suma de comprobación de los programas y examinando periódicamente los valores.

Tripwire supervisa las alteraciones no autorizadas en el conjunto de software de infraestructura y no se puede utilizar para mejorar el rendimiento del sistema.

Tripwire es una herramienta de mejora de la seguridad y no es utilizado por los hackers para realizar intrusiones. Los hackers pueden usar herramientas, como l0phtrack, John el destripador y Nessus, para descifrar las contraseñas almacenadas en Windows NT, descifrar las contraseñas de UNIX y realizar el ataque de reconocimiento.

Tripwire no actúa como un sistema de control de acceso centralizado para administrar las cuentas de usuario. Para administrar las cuentas de usuario, se implementan los servicios de autenticación, autorización y contabilidad (AAA).

Una funcionalidad adicional de tripwire es la funcionalidad antivirus que garantiza la integridad de los datos y genera alertas para los administradores en caso de cambio en el sistema operativo y las aplicaciones.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Determinar los requisitos de cumplimiento

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Integridad

TripWire, http://www.onlamp.com/pub/a/onlamp/excerpt/incidentres_07/index2.html

Pregunta #19 de 137

Id. de pregunta: 1114675

¿Qué declaraciones con respecto a la política de seguridad son correctas?

un. Una política de seguridad establece los objetivos de seguridad generales de una organización.

B. Una directiva de seguridad establece los objetivos de rendimiento de una organización.

c. Una política de seguridad establece la autoridad y las responsabilidades de las personas y es de naturaleza estratégica.

d. Una política de seguridad establece la autoridad y las responsabilidades de los individuos y es de naturaleza táctica.

E. Una política de seguridad se desarrolla después de la implementación de los procedimientos operativos estándar.

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

explicación

Una política de seguridad define los objetivos de seguridad generales de una organización, establece la autoridad y las responsabilidades de los individuos y es de naturaleza estratégica.

Una directiva de seguridad no establece los objetivos de rendimiento de una organización.

Una política de seguridad no es de naturaleza táctica. Los objetivos tácticos de la política de seguridad son de corto a mediano plazo, mientras que los objetivos estratégicos de la política son a largo plazo. Toda una política de seguridad debe ser siempre de naturaleza estratégica para garantizar que se aborden las cuestiones a largo plazo.

Se debe desarrollar una política de seguridad antes de que se desarrollen los procedimientos y directrices. La directiva de seguridad debe utilizarse para diseñar correctamente los procedimientos y directrices.

Una directiva de seguridad solicita procedimientos para aplicar la directiva de seguridad y las ramificaciones del incumplimiento. Una directiva de seguridad rige el fondo del programa de seguridad, los requisitos de auditoría y las reglas para la aplicación. La administración superior de la organización es responsable de crear la directiva de

seguridad para la organización. Obtener la aprobación de la administración es el primer paso en el desarrollo de una política de seguridad.

Las tres categorías de directivas de seguridad son organizativas, específicas de un problema y específicas del sistema:

- Política de seguridad de la organización: Esta directiva es formulada por la administración y define el procedimiento utilizado para configurar el programa de seguridad y sus objetivos. Identifica las principales áreas funcionales de la información y define todos los términos relevantes. La administración asigna los roles y responsabilidades y define el procedimiento para aplicar la directiva de seguridad. Una política de seguridad se desarrolla antes de la implementación de los procedimientos operativos estándar o directrices. Las políticas organizativas se desarrollan estratégicamente para el logro a largo plazo de los objetivos de seguridad.
- Directiva específica del problema: una directiva de seguridad específica del problema implica una evaluación detallada de los problemas de seguridad y aborda problemas de seguridad específicos. Una directiva de seguridad específica del problema garantiza que todos los empleados entiendan estos problemas de seguridad y cumplan con las directivas de seguridad definidas para abordar estos problemas de seguridad.
- Directiva específica del sistema: una directiva específica del sistema describe las reglas para la protección de los sistemas de procesamiento de información, como bases de datos, equipos, etc. Una política específica del sistema es de naturaleza estratégica y está diseñada con un enfoque a largo plazo. Restringe el uso de software a funciones aprobadas por la administración y define aún más las políticas y directrices para la configuración del sistema, la implementación de cortafuegos, los sistemas de detección de intrusiones y los analizadores de redes y virus.

Una política eficaz de seguridad de la información debería incluir la separación de funciones. Debe ser fácilmente entendida y apoyada por todos los empleados de la organización.

La descripción de las tecnologías específicas necesarias para aplicar la seguridad de la información no se incluye en la directiva de seguridad.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Desarrollar, documentar e implementar políticas, estándares, procedimientos y directrices de seguridad

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 1: Seguridad y Gestión de Riesgos, Políticas

---

Pregunta #20 de 137

Id. de pregunta: 1104809

¿Qué afirmación es cierta en el derecho administrativo?

✗ **A)** Según el derecho administrativo, los altos funcionarios de una empresa no son responsables.

✗ **B)** El derecho administrativo se establece sobre la base del consenso común de empresas específicas.

✓ **C)** El derecho administrativo hace hincapié en el desempeño y la conducta de las organizaciones.

✗ **D)** El derecho reglamentario es diferente del derecho administrativo.

explicación

El derecho administrativo define las normas reguladoras para el desempeño y la conducta de las empresas. El derecho administrativo a menudo se llama derecho regulatorio. Este tipo de ley incluye estándares considerados de desempeño o conducta esperados por las agencias gubernamentales de compañías, industrias y ciertos funcionarios.

El gobierno crea las normas para el derecho administrativo. Estas normas actúan como medidas para controlar el rendimiento y la conducta de las empresas y sus empleados. Por ejemplo, las leyes administrativas regulan que todas las empresas deben tener sistemas de detección y extinción de incendios. La violación de las leyes administrativas puede dar lugar a sanciones severas.

Las leyes administrativas también se conocen como leyes reguladoras.

Los altos funcionarios de una empresa son responsables de mantener las normas dictadas por el derecho administrativo. Si una empresa no se adhiere a las normas y procedimientos regulatorios específicos, los altos funcionarios de la empresa son responsables de la negligencia. Se les pueden imponer fuertes sanciones por descuidar las normas que controlan el desempeño y la conducta de la empresa.

El derecho administrativo no se basa en el consenso de unas pocas empresas.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender los problemas legales y reglamentarios relacionados con la seguridad de la información en un entorno global

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Derecho Administrativo/Regulatorio

---

Pregunta #21 de 137

Id. de pregunta: 1111667

Su organización ha decidido externalizar su servicio de correo electrónico. La empresa elegida para este fin ha proporcionado un documento que detalla las funciones de correo electrónico que se proporcionarán durante un período específico, junto con métricas de rendimiento garantizadas. ¿Cómo se llama este documento?

✗ **A)** depósito de garantía de software

✓ **B)** acuerdo de nivel de servicio (SLA)

✗ **C)** acuerdo recíproco

✗ **D)** acuerdo de instalación fuera del sitio

explicación

Un acuerdo de nivel de servicio (SLA) es un acuerdo entre una empresa y un proveedor en el que el proveedor acepta proporcionar ciertas funciones durante un período especificado.

El propósito de un depósito de garantía de software es proporcionar el código fuente de un proveedor de software en caso de que el proveedor salga del negocio. En un depósito de garantía de software, un tercero es responsable de mantener el código fuente y otros materiales aplicables. El contrato de depósito de garantía de software garantiza que tanto el proveedor de software como el cliente estén protegidos.

Un acuerdo recíproco es un acuerdo en el que dos compañías acuerdan proporcionar instalaciones fuera del sitio entre sí en caso de que ocurra un desastre.

Un acuerdo de instalación fuera del sitio es un acuerdo entre una empresa y un proveedor en el que el proveedor se compromete a proporcionar una instalación fuera del sitio en caso de que ocurra un desastre. La siguiente es la clasificación de las instalaciones fuera del sitio, desde la implementación más costosa hasta la implementación menos costosa:

- Sitio caliente
- Sitio cálido
- Sitio frío
- Acuerdo de ayuda mutua

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Identificar, analizar y priorizar los requerimientos de Continuidad del Negocio (BC, Business Continuity)

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y gestión de riesgos, requisitos de nivel de servicio

Pregunta #22 de 137

Id. de pregunta: 1111637

¿A qué afecta principalmente el envío de datos a través de una red insegura, como Internet?

✗ **A)** integridad y autenticidad

✗ **B)** confidencialidad y disponibilidad

✓ **C)** confidencialidad e integridad

✗ **D)** integridad y disponibilidad

explicación

El envío de datos a través de una red insegura, como Internet, afecta a la confidencialidad y la integridad. Es responsabilidad del remitente asegurarse de que existen los controles de seguridad adecuados. Por ejemplo, el remitente de un correo electrónico es responsable del cifrado si se desea seguridad. La confidencialidad y la integridad deben implementarse para garantizar la exactitud de los datos y su accesibilidad al personal autorizado.

La transmisión de datos a través de una red insegura no afecta a la disponibilidad o autenticidad de los datos.

La confidencialidad, la integridad y la disponibilidad son los tres objetivos de seguridad principales para la protección de los activos de información de una organización. Estos tres objetivos también se conocen como la tríada de la CIA. La mayoría de los ataques informáticos resultan en la violación de la tríada de la CIA. Por ejemplo, el robo de una computadora portátil representa una amenaza para todos los principios de la tríada de la CIA.

La confidencialidad es el nivel mínimo de secreto que se mantiene para proteger la información confidencial de la divulgación no autorizada. La confidencialidad se puede implementar a través del cifrado, la clasificación de datos de control de acceso y la conciencia de seguridad. Mantener la confidencialidad de la información evita que una organización ataques, como el shoulder surf y la ingeniería social, que pueden conducir a la divulgación de información confidencial e interrumpir las operaciones comerciales. La falta de controles de seguridad suficientes para mantener la confidencialidad conduce a la divulgación de información.

La integridad garantiza las siguientes condiciones:

- Los datos son precisos y fiables.
- Los datos y el sistema están protegidos contra alteraciones no autorizadas.
- Los ataques y errores del usuario no afectan a la integridad de los datos y del sistema.

Garantizar la integridad de la información implica que la información está protegida contra modificaciones no autorizadas y que los contenidos no han sido alterados.

Los objetivos de integridad incluyen:

- Prevención de la modificación de la información por parte de usuarios no autorizados
- Prevención de la modificación no autorizada o no intencional de la información por parte de usuarios autorizados
- Preservación de la coherencia interna y externa

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender y aplicar los conceptos de confidencialidad, integridad y disponibilidad

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 1: Seguridad y Gestión de Riesgos, confidencialidad, integridad y disponibilidad

---

Pregunta #23 de 137

Id. de pregunta: 1104892

Está diseñando el plan de formación de concienciación sobre seguridad para su organización. Se han identificado varios grupos para recibir capacitación personalizada. ¿Qué grupo requiere capacitación en seguridad para garantizar que los programas producidos por la empresa no contengan problemas de seguridad?

- ✓ **A)** Desarrolladores
- ✗ **B)** Ejecutivos
- ✗ **C)** Administradores
- ✗ **D)** Empleados

explicación

Los desarrolladores deben recibir formación en seguridad para asegurarse de que desarrollan programas que no contienen problemas de seguridad.

Los ejecutivos de la empresa deben recibir capacitación en seguridad que sea parte educación y parte marketing. El componente de educación debe diseñarse para proporcionar a los ejecutivos una visión general de la seguridad de la red, y el componente de marketing debe incluir información diseñada para persuadir a los ejecutivos de que apoyen medidas de seguridad sólidas en una red informática. Se deben proporcionar actualizaciones frecuentes a los administradores para que puedan configurar una red de forma segura. Los empleados deben recibir formación general sobre seguridad de red sobre cuestiones de seguridad como ingeniería social, creación de credenciales de red y directiva de seguridad de la empresa.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Establecer y mantener un programa de concienciación, educación y capacitación en materia de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Niveles Requeridos

---

Pregunta #24 de 137

Id. de pregunta: 1104847

Como auditor de seguridad, está examinando las cuentas de usuario en la red de inicio de sesión único. Descubre que un empleado a largo plazo tiene más permisos de acceso de los que necesita para completar su trabajo. Determinar que este problema se ha producido con el tiempo como resultado de cambiar de trabajo dentro de la organización. ¿Qué término se utiliza para describir la condición que ha ocurrido?

- ✓ **A)** arrastramiento de autorización
- ✗ **B)** fluencia de autenticación
- ✗ **C)** arrastramiento de identidad
- ✗ **D)** fluencia de capacidad

explicación

La fluencia de autorización es el término utilizado para describir cuándo se asignan permisos de acceso adicionales a un usuario como resultado de cambiar de trabajo. Los permisos de usuario deben revisarse de forma periódica para garantizar la aplicación del principio de privilegios mínimos.

Ninguna de las otras opciones es válida.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Contribuir y aplicar las políticas y procedimientos de seguridad del personal

Referencias:

Privilege Creep, https://searchsecurity.techtarget.com/definition/privilege-creep

---

Pregunta #25 de 137

Id. de pregunta: 1192896

Usted ha sido contratado como contratista de seguridad para una pequeña empresa de fabricación. La compañía utiliza actualmente un modelo de control de acceso discrecional (DAC). ¿Qué persona es la principal responsable de determinar el control de acceso en esta empresa?

- ✓ **A)** titular de los datos
- ✗ **B)** administrador de seguridad
- ✗ **C)** usuario de datos
- ✗ **D)** director

explicación

El propietario de los datos es el principal responsable de determinar el control de acceso en esta empresa. Cuando se usa el control de acceso discrecional (DAC), el propietario de los datos permite o deniega el acceso a usuarios o grupos. Una lista de control de acceso (ACL) es la herramienta utilizada en este modelo.

Ninguna de las otras opciones es correcta. Con DAC, el propietario de los datos determina el control de acceso.

Using mandatory access control (MAC), the security label assigned to subjects and objects is primarily responsible for determining access control. This security label is defined for each subject and object based on strict rules. Using role-based access control (RBAC), the security administrator is primarily responsible for determining access control based on the roles defined and the written security policy.

Objective:
Security and Risk Management

Sub-Objective:
Evaluate and apply security governance principles

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, DataOwner

---

Question #26 of 137

Question ID: 1114674

Which statements regarding system security policy are correct?

a. A system security policy is issue specific in nature.

b. A system security policy establishes guidelines for information security.

c. A system security policy does not require the prior approval of management.

d. A system security policy specifies the list of approved hardware and software.

e. A system security policy specifies the steps undertaken for the protection of infrastructure equipment.

- ✗ **A)** option c

- ✗ **B)** options a, b, and c only
- ✗ **C)** option e
- ✗ **D)** option d
- ✗ **E)** option b
- ✓ **F)** options d and e only
- ✗ **G)** option a

Explanation

A system security policy specifies the list of approved hardware and software. It also specifies the steps undertaken for the protection of infrastructure equipment.

A system security policy is NOT issue specific in nature. This function is performed by an issue-specific policy. Issue-specific policies include e-mail privacy policy, virus-checking disk policy, and unfriendly employee termination policy. A system-specific policy is much more technically focused than an issue-specific policy.

A system security policy does NOT establish guidelines for information security. Procedures, standards, and guidelines are written after the development of the security policy and use the security policy as a basis for development.

A system security policy DOES require the prior approval of management.

A system-specific policy defined by management describes the rules governing the protection of information processing systems, such as databases, computers, and other infrastructure equipment. A system-specific policy is strategic and designed with a long-term focus. This policy restricts the use of software to only those approved by management, and further defines policies and guidelines for system configuration, firewalls, intrusion detection systems, and network and virus scanners. A system-specific policy is used to implement those security configuration settings that were determined to provide optimum security to assets. It should include a statement of senior executive support and a definition of the legal and regulatory controls.

An example of a system-specific security policy is a computer policy that defines the acceptable use of computer systems and has approved hardware and software according to the security objectives of an organization.

The other types of security policy are organizational security policies and issue-specific policies:

- Organizational security policy: Formulated by the management, this security policy defines the procedure used to set up a security program and its goals. It identifies the major functional areas of information and defines all relevant terms. The management assigns the roles and responsibilities and defines the procedure used to enforce the security policy. A security policy is developed prior to the implementation of standard operating procedures. The organizational polices are strategically developed for a long term.
- Issue-specific policy: An issue-specific security policy involves the detailed evaluation of security problems and addresses specific security issues. An issue-specific security policy ensures that all employees understand these security issues and will comply with the security policies defined to address these security issues.

Objective:

Security and Risk Management

Sub-Objective:

Develop, document, and implement security policy, standards, procedures, and guidelines

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management,

System-Specific Security Policy

Question #27 of 137

Question ID: 1111649

Which statement is true of trade secret law?

✗ **A)** Trade secret law promotes the use of information between different companies to ensure a homogeneous environment.

✗ **B)** Trade secret law involves protection of either a word or a symbol that is used to represent the company.

✗ **C)** Trade secret law involves protection of an idea's expression.

✓ **D)** Trade secret law protects information that is vital to a company's survival and profitability.

Explanation

Trade secret law protects information that is vital to a company's survival and profitability. Trade secret law preserves the proprietary information pertaining to a company's business. Trade secrets provide a company with a competitive advantage. Special skill and talent is required to develop trade secrets. The Trade Secret Act qualifies company information as a trade secret only if the information fulfills the following conditions:

- The information must not be easily accessible.
- The information must have economic value for the company's competitors.
- The information must be protected by the company using all reasonable means.

The following are examples of company trade secrets:

- customer identities and preferences
- vendors
- product pricing
- marketing strategies
- company finances

- manufacturing processes
- other competitively valuable information

Unlike a copyright, a trade secret does not protect either an idea or an expression. Copyright law protects an idea's expression rather than the idea itself. The ideas are protected by the use of patents, and the corresponding expression is controlled by copyrights.

Trademark refers either to a word or to a symbol that is used to represent a company to the world. Trademarks are protected because each trademark is a unique symbol to represent the company, and the organization has spent time and effort to develop a trademark.

Trade secret law prevents unauthorized disclosure of a company's confidential information and does not ensure a homogeneous environment.

Many companies require their employees to sign nondisclosure agreements (NDAs) to ensure trade secret protection. A resource can be protected by trade secret law if it is not generally known and if it requires special expertise, creativity, or expense and effort to develop it.

Objective:
Security and Risk Management

Sub-Objective:
Understand legal and regulatory issues that pertain to information security in a global

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Trade Secret

---

Question #28 of 137

Question ID: 1104759

You are your organization's security administrator. You need to ensure that your organization's data is accurate and secure. Which security objective should you implement?

✗ **A)** integrity and availability
✓ **B)** confidentiality and integrity
✗ **C)** control and accessibility
✗ **D)** confidentiality and availability

Explanation

Confidentiality and integrity should be implemented to ensure the accuracy of the data and its secrecy. Confidentiality is defined as the minimum level of secrecy that is maintained to protect sensitive information from unauthorized

disclosure. Ensuring the integrity of information implies that the information is protected from unauthorized modification and that the contents have not been altered.

Confidentiality can be implemented through encryption, access control data classification, and security awareness. Confidentiality is the opposite of disclosure. Maintaining the confidentiality of information prevents an organization from attacks, such as shoulder surfing and social engineering. These attacks can lead to disclosure of confidential information and can disrupt business operations. The lack of sufficient security controls to maintain confidentiality leads to disclosure of information.

Control and accessibility is not a category of security objectives. Therefore, this is an invalid option.

Confidentiality, integrity, and availability are the three security objectives considered as core for the protection of the information assets of an organization. These three objectives are called the CIA triad.

Objective:
Security and Risk Management

Subobsecución:
Comprender y aplicar los conceptos de confidencialidad, integridad y disponibilidad

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 1: Seguridad y Gestión de Riesgos, confidencialidad, integridad y disponibilidad

---

Pregunta #29 de 137

Id. de pregunta: 1113905

¿Qué componente de una directiva de uso del equipo debe indicar que no se garantiza que los datos almacenados en el equipo de una empresa permanezcan confidenciales?

- ✗ **A)** propiedad de la información
- ✓ **B)** ninguna expectativa de privacidad
- ✗ **C)** uso aceptable
- ✗ **D)** propiedad del equipo

explicación

Una política de no expectativa de privacidad es el componente de una política de uso de computadora que debe indicar que no se garantiza que los datos almacenados en una computadora de la compañía permanezcan confidenciales. Una política de privacidad sin expectativas también debe indicar que los datos transferidos hacia y desde una red de la empresa no se garantiza que permanezcan confidenciales.

La propiedad del equipo es un componente de una directiva de uso del equipo que indica que los equipos son propiedad de la empresa y deben usarse únicamente para fines de la empresa. La propiedad de la información es un componente de una directiva de uso del equipo que establece que toda la información almacenada en los equipos de la empresa es propiedad de la empresa. El uso aceptable es una directiva de uso de equipos, que establece las condiciones en las que se deben usar los equipos de la empresa.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Contribuir y aplicar las políticas y procedimientos de seguridad del personal

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y gestión de riesgos, problemas de privacidad de los empleados y expectativas de privacidad

Política de uso aceptable, http://www.sans.org/resources/policies/Acceptable_Use_Policy.pdf

---

Pregunta #30 de 137

Id. de pregunta: 1113907

¿Cuál es el propósito del análisis cuantitativo de riesgos?

- ✗ **A)** para generar una lista priorizado de riesgos que podrían afectar negativamente al proyecto
- ✗ **B)** generar un plan de acción en respuesta a cada riesgo identificado
- ✓ **C)** analizar los riesgos ya priorizado de tal manera que cada uno de ellos se dé una calificación numérica
- ✗ **D)** determinar el impacto general que los riesgos específicos plantean para la finalización exitosa del proyecto

explicación

El propósito del análisis cuantitativo de riesgos es analizar los riesgos ya priorizado de tal manera que se le dé a cada uno una calificación numérica. El análisis cuantitativo de riesgos intenta cuantificar la priorización, la probabilidad y el efecto de los riesgos de seguridad. La mayoría de las veces sigue directamente el análisis cualitativo de riesgos.

La generación de un plan de acción en respuesta a cada riesgo identificado es parte de la planificación de las respuestas de riesgo. La generación de una lista priorizado de riesgos y la determinación del impacto general en el proyecto son parte de la identificación de riesgos de seguridad y la realización de análisis cualitativos de riesgos.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender y aplicar los conceptos de gestión de riesgos

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Análisis Cuantitativo de Riesgos

Análisis cuantitativo de riesgos paso a paso, http://www.sans.org/reading_room/whitepapers/auditing/quantitative-risk-analysis-step-by-step_849

Pregunta #31 de 137

Id. de pregunta: 1111681

Está analizando los riesgos para su organización. Debe asegurarse de que la alta dirección proporciona los componentes de gestión de riesgos que necesitaba. Todos los siguientes componentes son proporcionados por la alta dirección, EXCEPTO:

- ✓ **A)** procedimientos de mitigación de riesgos
- ✗ **B)** asignación de recursos
- ✗ **C)** asignación monetaria
- ✗ **D)** nivel de aceptación de riesgos

explicación

Los procedimientos de mitigación de riesgos NO son proporcionados por la alta gerencia. El objetivo de la mitigación de riesgos es definir el nivel aceptable de riesgo que una organización puede tolerar y reducir el riesgo a ese nivel.

Los siguientes componentes de gestión de riesgos son proporcionados por el personal directivo superior:

- nivel de aceptación de riesgos establecido
- asignación de recursos
- asignación de fondos monetarios

La alta dirección tiene la responsabilidad final de salvaguardar la información de la organización. Cuando se trata de seguridad de la información, la administración debe definir el propósito y el alcance del programa de seguridad, delegar la responsabilidad del programa de seguridad y apoyar el programa a medida que se implementa.

El propósito de la gestión de riesgos es reducir el riesgo a un nivel tolerable.

Objetivo:

Seguridad y gestión de riesgos

Subobsecución:

Comprender y aplicar los conceptos de gestión de riesgos

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 1: Seguridad y Gestión de Riesgos, Gestión

---

Pregunta #32 de 137

Id. de pregunta: 1192905

Haga clic en cada uno de los encabezados del escenario para expandir o contraer su contenido. Debe leer todo el escenario para responder a la pregunta.

fondo

Usted es un profesional de la seguridad contratado recientemente por una empresa que cotiza en bolsa para ayudar a administrar la seguridad de la organización. La compañía tiene una oficina principal en Atlanta, GA, y sucursales en todo el sureste de los Estados Unidos. El departamento de TI tiene un pequeño personal alojado en la oficina de Atlanta.

Temas actuales

El año pasado, una tormenta invernal cerró las operaciones en la mayoría de sus oficinas. Si bien ninguna de sus instalaciones fue destruida y las operaciones normales se restauraron en 24 horas, a la administración le preocupa que no exista un plan de recuperación ante desastres. Se le ha pedido que prepare un plan para cubrir este tipo de interrupción.

Actualmente, su organización mantiene varias bases de datos grandes de contenido digital que son vitales para las operaciones de su organización. Se utilizan diferentes controles para administrar este contenido. La administración le ha pedido que implemente una solución para controlar la apertura, edición, impresión o copia de estos datos de una manera más centralizada.

En los próximos seis meses, su empresa planea mover todos los servidores y granjas de servidores a un centro de datos centralizado. El centro de datos ocupará el tercer piso de un edificio de seis pisos que actualmente está en construcción. La administración le ha pedido que se asegure de que el acceso al centro de datos esté estrictamente controlado. Durante ese mismo tiempo, es probable que su organización compre un competidor para fusionarse con su organización existente.

Recientemente, uno de los servidores de la intranet fue víctima de un ataque de denegación de servicio (DoS). El departamento de TI tardó más de 24 horas en volver a poner en funcionamiento el servidor. Durante ese tiempo, el personal de la oficina principal no pudo acceder a la importante información sobre recursos humanos disponible en el servidor de la intranet afectado.

La semana pasada, descubrió que se utilizaron varias cuentas de usuario en un intento de piratear su red. Afortunadamente, las cuentas fueron bloqueadas debido a intentos de inicio de sesión no válidos. Revise los registros y determine que tres de las cuentas se crearon para el personal que ya no está empleado por su organización.

After pushing for years, you have received permission from management to design and implement a comprehensive security awareness program across the entire organization.

What should you implement to address the issue of the attack that locked out accounts?

- ✗ **A)** minimum password age policies
- ✗ **B)** non-disclosure agreements
- ✓ **C)** termination policies
- ✗ **D)** selección de candidatos

explicación

Debe implementar directivas de terminación. Cuando se termina el personal, deben existir directivas que garanticen que se elimina el acceso al sistema para esos usuarios. En su investigación, encontró específicamente cuentas creadas para el personal que ya no está empleado por su organización.

La selección de candidatos es importante cuando se contrata personal.

Los acuerdos de confidencialidad deben ser firmados por el personal cuando son contratados o despedidos. Sin embargo, no habrían tenido ningún efecto en las cuentas de usuario que todavía están en el sistema para el personal despedido.

Las directivas de antigüedad mínima de las contraseñas garantizan que los usuarios cambien sus contraseñas de forma regular. Aunque pueden ayudar a evitar ataques contra las cuentas de usuario, no impedirán la existencia continuada de cuentas de usuario para los empleados despedidos.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Contribuir y aplicar las políticas y procedimientos de seguridad del personal

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Políticas y Procedimientos de Seguridad del Personal

Cómo crear y hacer cumplir los procedimientos de despido de empleados, http://searchsecurity.techtarget.com/answer/How-to-create-and-enforce-employee-termination-procedures

Pregunta #33 de 137

Id. de pregunta: 1104757

¿Qué principio de seguridad identifica los datos confidenciales y garantiza que las entidades no autorizadas no puedan acceder a los datos?

- ✗ **A)** autenticación
- ✗ **B)** integridad
- ✗ **C)** disponibilidad
- ✓ **D)** confidencialidad

explicación

La confidencialidad identifica los datos confidenciales y garantiza que las entidades no autorizadas no puedan acceder a los datos confidenciales. La confidencialidad es lo opuesto a la divulgación.

La disponibilidad garantiza que los datos y los recursos estén disponibles para las entidades autorizadas de manera oportuna.

La integridad garantiza que los datos y los recursos se editen solo de manera aprobada por las entidades autorizadas.

La autenticación es el proceso de identificar a un sujeto que solicita acceso al sistema.

Al considerar la confidencialidad en el sector privado, la información que se considera altamente confidencial debe estar disponible para cualquier persona cuyo trabajo requiera acceso a los datos confidenciales. Se debe requerir autorización para acceder a datos altamente confidenciales cada vez que se accede a los datos.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender y aplicar los conceptos de confidencialidad, integridad y disponibilidad

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 1: Seguridad y Gestión de Riesgos, Confidencialidad

Pregunta #34 de 137

Id. de pregunta: 1104864

¿Qué afirmación es cierta sobre el papel del director de seguridad (OSC) en una organización?

✗ **A)** El papel de la OSC debe incluir todos los demás departamentos para una gestión eficiente de la seguridad.

✗ **B)** Las OSC no deberían ser la única autoridad, y el proceso de toma de decisiones debería incluir personal de otros departamentos.

✓ **C)** El papel de las OSC debe ser autónomo e independiente de todos los demás departamentos de la organización.

✗ **D)** El papel de la OSC debe limitarse al departamento de TI.

explicación

La función del oficial jefe de seguridad debe ser autónoma e independiente de todos los demás departamentos de la organización. La OSC debe informar al director de información (CIO), al director de tecnología (CTO) o al director ejecutivo (CEO) solo para obtener la aprobación de la administración para la implementación de la seguridad y para proporcionar comentarios sobre el cumplimiento del proceso de seguridad. En una organización, una función de seguridad de tecnología de la información debe estar dirigida por un oficial jefe de seguridad.

La función de tecnología de la información es responsable de llevar a cabo la implementación de la infraestructura basada en las directivas emitidas por la OSC. Las responsabilidades de seguridad de una OSC incluyen no sólo la función de tecnología de la información, sino que se extienden a todos los departamentos de la organización. Las OSC podrían celebrar una reunión periódica con los directores de diferentes departamentos de la organización y darles a conocer las iniciativas de seguridad que fluyen en un enfoque de arriba hacia abajo de la alta dirección.

Para el proceso de toma de decisiones como parte del programa de seguridad de la información, la OSC es la única autoridad. Las iniciativas de seguridad se extienden a través de los diversos departamentos y la OSC es responsable ante la alta gerencia por el cumplimiento de la seguridad de la información.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender y aplicar los conceptos de gestión de riesgos

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 1: Seguridad y Gestión de Riesgos, Gestión

Director de Seguridad, http://searchsecurity.techtarget.com/gDefinition/0,294236,sid14_gci858563,00.html

---

Pregunta #35 de 137

Id. de pregunta: 1192899

Haga clic en cada uno de los encabezados del escenario para expandir o contraer su contenido. Debe leer todo el escenario para responder a la pregunta.

fondo

Usted es un profesional de la seguridad contratado recientemente por una empresa que cotiza en bolsa para ayudar a administrar la seguridad de la organización. La compañía tiene una oficina principal en Atlanta, GA, y sucursales en todo el sureste de los Estados Unidos. El departamento de TI tiene un pequeño personal alojado en la oficina de Atlanta.

Temas actuales

El año pasado, una tormenta invernal cerró las operaciones en la mayoría de sus oficinas. Si bien ninguna de sus instalaciones fue destruida y las operaciones normales se restauraron en 24 horas, a la administración le preocupa que no exista un plan de recuperación ante desastres. Se le ha pedido que prepare un plan para cubrir este tipo de interrupción.

Actualmente, su organización mantiene varias bases de datos grandes de contenido digital que son vitales para las operaciones de su organización. Se utilizan diferentes controles para administrar este contenido. La administración le ha pedido que implemente una solución para controlar la apertura, edición, impresión o copia de estos datos de una manera más centralizada.

En los próximos seis meses, su empresa planea mover todos los servidores y granjas de servidores a un centro de datos centralizado. El centro de datos ocupará el tercer piso de un edificio de seis pisos que actualmente está en construcción. La administración le ha pedido que se asegure de que el acceso al centro de datos esté estrictamente controlado. Durante ese mismo tiempo, es probable que su organización compre un competidor para fusionarse con su organización existente.

Recientemente, uno de los servidores de la intranet fue víctima de un ataque de denegación de servicio (DoS). El departamento de TI tardó más de 24 horas en volver a poner en funcionamiento el servidor. Durante ese tiempo, el personal de la oficina principal no pudo acceder a la importante información sobre recursos humanos disponible en el servidor de la intranet afectado.

La semana pasada, descubrió que se utilizaron varias cuentas de usuario en un intento de piratear su red. Afortunadamente, las cuentas fueron bloqueadas debido a intentos de inicio de sesión no válidos. Revise los registros y determine que tres de las cuentas se crearon para el personal que ya no está empleado por su organización.

Después de presionar durante años, ha recibido permiso de la administración para diseñar e implementar un programa integral de concienciación de seguridad en toda la organización.

¿Cuál de las siguientes leyes afectará a la organización?

- ✓ **A)** Ley SOX
- ✗ **B)** FISMA de 2002

✗ **C)** GLBA de 1999

✗ **D)** HIPAA

explicación

La Ley Sarbanes-Oxley (SOX) afectará a la organización. La Ley SOX afecta a cualquier empresa que cotiza en bolsa en los Estados Unidos.

La Ley Gramm-Leach-Bliley (GLBA) de 1999 sólo afecta a las instituciones financieras.

La Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA, por susta, por susccciones y responsabilidades) afecta a las organizaciones de atención médica.

La Ley Federal de Gestión de la Seguridad de la Información (FISMA) de 2002 afecta a todas las agencias federales.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Determinar los requisitos de cumplimiento

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Cuestiones Legales y Regulatorias

Ley Sarbanes-Oxley de 2002 - SOX, http://www.investopedia.com/terms/s/sarbanesoxleyact.asp

Comisión Federal de Comercio: Ley Gramm-Leach-Bliley, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act

HHS Home > HIPAA > para profesionales > entidades cubiertas y socios comerciales, http://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html

Nist > Computer Security Division > Computer Security Resource Center > GROUPS > SMA > FISMA, http://csrc.nist.gov/groups/SMA/fisma/overview.html

---

Pregunta #36 de 137

Id. de pregunta: 1192914

La gestión de su empresa se ha vuelto recientemente cada vez más preocupada por la seguridad. Se le ha pedido que proporcione ejemplos de controles que ayudarán a evitar infracciones de seguridad. ¿Qué control es un ejemplo de esto?

✗ **A)** Backups

✗ **B)** rotación de trabajos

✗ **C)** registros de auditoría

✓ **D)** directiva de seguridad

explicación

Una política de seguridad es un ejemplo de control administrativo preventivo. También se considera un control administrativo compensativo. Los controles preventivos son controles que se implementan para evitar brechas de seguridad. Los controles administrativos dictan cómo se implementan las políticas de seguridad para cumplir con los objetivos de seguridad de la empresa. Otros ejemplos de controles administrativos preventivos incluyen políticas de seguridad, separación de funciones, clasificación de la información, procedimientos de personal, pruebas y capacitación en conciencia de seguridad.

Las copias de seguridad son un ejemplo de un control técnico de recuperación y un control técnico compensativo. Los registros de auditoría son un ejemplo de un control técnico detectivesco y un control técnico compensativo. La rotación de puestos de trabajo es un ejemplo de un control administrativo detectivesco y un control administrativo compensativo.

Hay tres categorías de control de acceso: controles técnicos, administrativos y físicos. Se ha establecido un control técnico para restringir el acceso a las redes y los sistemas. Un administrativo se desarrolla para dictar cómo se implementan las políticas de seguridad para cumplir con los objetivos de seguridad de la empresa. Un control físico se implementa para proteger el acceso físico a un objeto, como un edificio, una sala o un equipo. Las tres categorías de control de acceso proporcionan siete funcionalidades o propósitos diferentes:

- Preventivo - Un control preventivo previene brechas de seguridad y evita riesgos.
- Detective - Un control detective detecta las brechas de seguridad a medida que ocurren.
- Correctivo : un control correctivo restaura el control e intenta corregir cualquier daño infligido durante una infracción de seguridad.
- Disuasión - Un control disuasorio disuade posibles violaciones.
- Recuperación: un control de recuperación restaura los recursos.
- Compensativo: un control compensativo proporciona un control alternativo si otro control puede ser demasiado costoso. Por lo general, todos los controles se consideran compensativos.
- Directiva - Un control de directiva proporciona controles obligatorios basados en regulaciones o requisitos ambientales.

Cada categoría de control incluye controles que proporcionan funciones diferentes. Por ejemplo, una insignia de seguridad es tanto un control físico preventivo como un control físico compensativo. La supervisión y supervisión es tanto un control administrativo detectivesco como un control administrativo compensativo.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender y aplicar los conceptos de gestión de riesgos

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 1: Seguridad y Gestión de Riesgos, Preventiva

---

Pregunta #37 de 137

Id. de pregunta: 1113903

Como parte de la nueva iniciativa de seguridad, debe asegurarse de que los usuarios de la organización no instalen software no autorizado. ¿Qué acuerdo de usuario debe incluir esta restricción?

- ✗ **A)** acuerdo de confidencialidad
- ✗ **B)** contrato de licencia de software
- ✗ **C)** contrato de licencia de usuario final
- ✓ **D)** política de uso aceptable

explicación

Una directiva de uso aceptable incluye una restricción que prohíbe a los usuarios de una organización instalar software no autorizado. Este acuerdo también suele incluir información sobre ninguna expectativa de privacidad, lo que significa que el uso de la computadora no es privado.

Un contrato de licencia de software es un acuerdo entre un proveedor de software y un cliente empresarial. El cliente compra un nivel determinado de licencias para una aplicación en particular y acepta limitar el uso dentro de la empresa a ese número. El uso del software debe supervisarse automáticamente para asegurarse de que las licencias de uso no superan el número permitido en el contrato de licencia de software.

Un contrato de licencia de usuario final es un acuerdo entre un proveedor de software y el usuario final. El usuario final es el propietario del equipo.

Un acuerdo de confidencialidad es un acuerdo entre dos partes en el que la información que se comparte no se divulgará a terceros. Un ejemplo de un acuerdo de confidencialidad es el acuerdo electrónico que los candidatos a la certificación "firman" digitalmente antes de tomar un examen de certificación.

Objective:
Security and Risk Management

Sub-Objective:
Develop, document, and implement security policy, standards, procedures, and guidelines

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Directive

Different Types of Software License Agreements, http://www.blogsharp.com/news_9684.html

Question #38 of 137

Question ID: 1111654

Usted trabaja para una agencia federal de los Estados Unidos. El administrador indica que debe identificar los equipos que contienen información confidencial. ¿Qué ley exige esto?

✗ **A)** Ley de espionaje económico de 1996

✗ **B)** Ley HIPAA

✗ **C)** U.S. Communications Assistance for Law Enforcement Act de 1994

✓ **D)** Ley de Seguridad Informática de 1987

explicación

Bajo la Ley de Seguridad Informática de 1987, todas las agencias federales de los Estados Unidos deben identificar las computadoras que contienen información confidencial y desarrollar un plan de seguridad para ellas. Se imparte capacitación periódica sobre la concienciación sobre la seguridad sobre las prácticas aceptables por el gobierno para las personas que operan y administran estos sistemas.

La Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA, por sus, por sus contralo, por sus, por sus contrao, por susta, por suscia) también se conoce como Ley Kennedy-Kassebaum. El énfasis principal de HIPAA está en la simplificación de la administración a través de la mejora de la eficiencia en la prestación de atención médica. Esta simplificación se logra mediante la normalización del intercambio electrónico de datos y la protección de la confidencialidad y la seguridad de los datos sanitarios. Después de la implementación, HIPAA se adelanta a las leyes estatales, a menos que la ley estatal sea más estricta.

La Ley de Asistencia de Comunicaciones para la Aplicación de la Ley de Los Estados Unidos (CALEA, por sus siglas en inglés) de 1994 preserva la capacidad de las agencias de aplicación de la ley para llevar a cabo la vigilancia electrónica. Esto puede requerir la modificación del diseño de equipos y servicios de telecomunicaciones. En los Estados Unidos, CALEA describe cómo los operadores inalámbricos y de línea fijo deben proporcionar información de vigilancia a un centro de monitoreo de la aplicación de la ley para permitir que el centro realice un seguimiento de las actividades.

La Ley de espionaje económico de 1996 estructuró las directrices sobre quién debe investigar un delito. Las agencias de aplicación de la ley de los Estados Unidos, como el Buró Federal de Investigaciones (FBI), investigan los actos de espionaje industrial y corporativo bajo esta ley. Esta ley implica que los bienes protegidos incluyen los bienes no corporales, como la propiedad intelectual. El robo ya no se limita a las restricciones físicas. Investigar y enjuiciar los delitos informáticos se hace más difícil porque las pruebas son en su mayoría intangibles.

Las escuchas telefónicas son un ataque pasivo. Las escuchas telefónicas o escuchas telefónicas se basan en el hecho de que todas las señales de comunicación son vulnerables a la escucha pasiva. Las escuchas telefónicas

implican el uso de un dispositivo de transmisión o grabación para monitorear las conversaciones entre dos individuos o compañías con o sin la aprobación de cualquiera de las partes. Se pueden utilizar las siguientes herramientas para interceptar la comunicación:

- Rastreadores de red
- Dispositivos de escucha telefónica
- Receptores de micrófono
- Escáneres celulares
- Grabadoras

Muchos países consideran que las escuchas telefónicas son ilegales. Las escuchas telefónicas sólo son aceptables si cualquiera de las partes que se comunican da su consentimiento para la escucha pasiva.

Las escuchas telefónicas no prohíben a los agentes del orden utilizar órdenes de registro contra los sospechosos. Los agentes de la ley tienen una orden judicial que permite las escuchas telefónicas a individuos específicos solo para una conversación relevante. La orden judicial especifica el propósito de las escuchas telefónicas y la duración durante la cual la conversación puede ser escuchada de conformidad con las regulaciones de la Ley de Privacidad de 1974. La Ley de Privacidad de 1974 estipula que la divulgación de información personal debe limitarse únicamente a las personas autorizadas. Las escuchas telefónicas juegan un papel importante en la inteligencia militar y extranjera.

Debido a que el desarrollo de nuevas tecnologías generalmente supera a la ley, la aplicación de la ley utiliza las leyes de malversación de fondos, fraude y escuchas telefónicas en muchos casos de delitos informáticos.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender los problemas legales y reglamentarios relacionados con la seguridad de la información en un entorno global

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 1: Security and Risk Management, Computer Security Act of 1987

Pregunta #39 de 137

Id. de pregunta: 1111657

Todos los siguientes son ejemplos de delitos asistidos por computadora, EXCEPTO:

✗ **A)** protestar contra los actos de un gobierno atacando las computadoras del gobierno

✗ **B)** atacar los sistemas financieros para robar dinero

✓ **C)** Instalar un virus en un equipo para destruir los datos del equipo

✗ **D)** Obtener datos confidenciales atacando a los servidores que contienen los datos

explicación

La instalación de un virus en una computadora para destruir los datos en la computadora NO es un ejemplo de delito asistido por computadora. Es un ejemplo de un delito dirigido por computadoras.

Las tres categorías de delitos informáticos son las siguientes:

- delito asistido por computadora - Esta categoría de delito es aquella en la que una computadora se utiliza como una herramienta para llevar a cabo un delito.
- delito dirigido por computadora - Esta categoría de delito es aquella en la que una computadora es víctima del delito.
- delito incidental informático - Esta categoría de delito es aquella en la que un ordenador está involucrado incidentalmente en el delito. El ordenador no es el objetivo del delito y no es la principal herramienta utilizada para llevar a cabo el delito.

Entre los ejemplos de delitos asistidos por computadora se incluyen los siguientes:

- Obtener datos confidenciales atacando a los servidores que contienen los datos
- atacar los sistemas financieros para robar dinero
- protestar contra los actos de un gobierno atacando las computadoras del gobierno

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender los problemas legales y reglamentarios relacionados con la seguridad de la información en un entorno global

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, crimen asistido por computadora

---

Pregunta #40 de 137

Id. de pregunta: 1104852

¿Qué elemento del plan de continuidad del negocio (BCP) existe para aliviar el riesgo de ciertas amenazas proporcionando una compensación monetaria en caso de que se produzcan esas amenazas?

✗ **A)** acuerdo recíproco

✓ **B)** seguro

✗ **C)** análisis de impacto en el negocio (BIA)

✗ **D)** plan de continuidad de operaciones (COOP)

explicación

El seguro existe para aliviar el riesgo de ciertas amenazas proporcionando una compensación monetaria en caso de que ocurran esas amenazas. El seguro generalmente se compra para cubrir la pérdida de activos debido a incendios o robos. Hay tipos específicos de pólizas de seguro que ahora existen para cubrir ciertos eventos catastróficos.

Un análisis de impacto empresarial (BIA) analiza las amenazas a una organización para determinar cómo podría verse afectada la organización. Un acuerdo recíproco es un acuerdo entre dos organizaciones para proporcionar facilidades alternativas entre sí. Se redacta un plan de continuidad de operaciones (COOP) para garantizar que una organización pueda continuar con funciones esenciales en una amplia gama de circunstancias.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender y aplicar los conceptos de gestión de riesgos

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Manejo de Riesgos y Respuesta al Riesgo

---

Pregunta #41 de 137

Id. de pregunta: 1192904

¿Qué área NO es parte de la seguridad física de una instalación de procesamiento de información?

✗ **A)** Cerraduras
✗ **B)** procedimientos de evacuación
✓ **C)** análisis del riesgo
✗ **D)** Cercas

explicación

La seguridad física no incluye el análisis de riesgos. El análisis de riesgos es una herramienta utilizada para identificar las amenazas y vulnerabilidades de los activos de una organización y el impacto potencial de tales vulnerabilidades y amenazas. El análisis de riesgos también identifica el nivel de riesgo correspondiente junto con el análisis de costo o beneficio de las salvaguardias como las contramedidas para mitigar el riesgo a un nivel aceptable.

Las vallas son un ejemplo de controles de seguridad física. La esgrima actúa como una primera línea de defensa para evitar el acceso no autorizado a la instalación de los intrusos.

Los procedimientos de evacuación son procedimientos de emergencia en caso de desastres naturales o manufacturados, como inundaciones, incendios, terremotos y terrorismo. Estos procedimientos proporcionan pautas para la seguridad del personal dentro de la instalación.

Los bloqueos son un ejemplo de controles de seguridad físicos. Una organización puede utilizar bloqueos para evitar el acceso no autorizado o para inducir un retraso en el proceso de una infracción de seguridad. Las cerraduras deben usarse en combinación con otros controles de seguridad para proteger la infraestructura de la instalación y sus recursos críticos.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Contribuir y aplicar las políticas y procedimientos de seguridad del personal

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y gestión de riesgos, amenazas internas frente a amenazas externas

---

Pregunta #42 de 137

Id. de pregunta: 1111647

¿Cuál es la designación de un empleado que es responsable de mantener y proteger la información?

- ✗ **A)** usuario de información
- ✓ **B)** custodio de datos
- ✗ **C)** propietario del sistema
- ✗ **D)** titular de los datos

explicación

El custodio de datos es directamente responsable de mantener y proteger los datos, y es un rol que normalmente se delega en el personal del departamento de TI. Las responsabilidades incluyen la implementación y el mantenimiento de controles de seguridad. El rol del custodio de datos incluye las siguientes tareas:

- Mantenimiento de registros de actividad
- Verificación de la exactitud y fiabilidad de los datos
- Copia de seguridad y restauración de datos regularmente

El propietario de los datos controla el proceso de definición de los niveles de servicio de TI, el suministro de información durante la revisión de los controles y la autorización de la aplicación de controles de seguridad para

proteger los activos de información de la organización. Un propietario de datos suele ser la administración de piezas. Por ejemplo, un gerente de unidad de negocio tiene la responsabilidad principal de proteger los activos de información mediante el ejercicio de la debida diligencia y las prácticas de debido cuidado.

El propietario de un sistema es responsable de mantener y proteger uno o más sistemas de procesamiento de datos. El rol incluye principalmente la integración de las características de seguridad necesarias en las aplicaciones e implica una decisión de compra de las aplicaciones. El propietario del sistema también garantiza que el acceso remoto, la administración de contraseñas y las configuraciones del sistema operativo proporcionen la seguridad necesaria.

Un usuario de información es una persona que utiliza los datos regularmente para cumplir con las responsabilidades del trabajo. Los usuarios deben poder acceder a la información basándose en el concepto de privilegios mínimos y solo en función de la necesidad de conocer para lograr los objetivos de seguridad de la organización.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
evaluar y aplicar los principios de gobierno de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Custodio de Datos

---

Pregunta #43 de 137

Id. de pregunta: 1192908

A la administración le preocupa que no se puedan implementar algunos controles de acceso porque son demasiado costosos de implementar. Se le ha pedido que proporcione alternativas menos costosas a los costosos controles de acceso. ¿Qué tipo de control de acceso proporcionará?

- ✗ **A)** directiva
- ✗ **B)** preventivo
- ✗ **C)** recuperación
- ✗ **D)** disuasivo
- ✓ **E)** compensativo
- ✗ **F)** correctivo
- ✗ **G)** detective

explicación

Proporcionará controles compensativos. Los controles compensativos se utilizan para proporcionar alternativas a otros controles, especialmente si un control de acceso es demasiado caro. Algunos ejemplos de controles compensativos son la necesidad de dos firmas autorizadas para liberar información confidencial, la necesidad de dos llaves para abrir una caja de seguridad, la entrada o salida de un registro de tráfico y el uso de una tarjeta magnética para acceder a un centro de operaciones.

Los controles detectivescos se utilizan para identificar cuándo se han producido violaciones de seguridad. Los controles disuasorios se utilizan para desalentar las infracciones de seguridad. Los controles de recuperación se utilizan para garantizar una recuperación adecuada. Los controles correctivos se utilizan para corregir problemas causados por infracciones de seguridad. Los controles de la directiva son controles obligatorios implementados debido a regulaciones o requisitos ambientales. Los controles preventivos se utilizan para evitar infracciones de seguridad e incluyen políticas de seguridad y formación de concienciación sobre seguridad para detener o disuadir de que se produzca una actividad no autorizada.

Hay tres categorías de control de acceso: controles técnicos, administrativos y físicos. Se ha establecido un control técnico para restringir el acceso. Los controles técnicos funcionan para proteger el acceso al sistema, la arquitectura y el acceso a la red, las zonas de control y la auditoría. Los controles técnicos incluyen tarjetas inteligentes, cifrado y protocolos. Un control administrativo es un control que dicta cómo se implementan las políticas de seguridad para cumplir con los objetivos de seguridad de la empresa. Los controles administrativos incluyen políticas y procedimientos, controles de personal, estructura de supervisión, capacitación en seguridad y pruebas. Un control físico se implementa para proteger el acceso físico a un objeto, como un edificio, una sala o un equipo. Los controles físicos incluyen insignias, cerraduras, guardias, segregación de red, seguridad perimetral, controles informáticos, separación de áreas de trabajo, copias de seguridad y cableado.

Las tres categorías de control de acceso proporcionan siete funcionalidades o propósitos diferentes:

- Preventivo - Un control preventivo previene brechas de seguridad y evita riesgos.
- Detective - Un control detective detecta las brechas de seguridad a medida que ocurren.
- Correctivo : un control correctivo restaura el control e intenta corregir cualquier daño infligido durante una infracción de seguridad.
- Disuasión - Un control disuasorio disuade posibles violaciones.
- Recuperación: un control de recuperación restaura los recursos.
- Compensativo: un control compensativo proporciona un control alternativo si otro control puede ser demasiado costoso. Por lo general, todos los controles se consideran compensativos.
- Directiva - Un control de directiva proporciona controles obligatorios basados en regulaciones o requisitos ambientales.

Cada categoría de control incluye controles que realizan muchas funciones. Por ejemplo, una valla es tanto un control físico disuasorio como un control físico compensativo. La supervisión y supervisión es tanto un control administrativo detectivesco como un control administrativo compensativo.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender y aplicar los conceptos de gestión de riesgos

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 1: Seguridad y Gestión de Riesgos, Compensativo

---

Pregunta #44 de 137

Id. de pregunta: 1113894

Está explicando los permisos de control de acceso a otro administrador. El administrador debe asegurarse de que ciertos usuarios no tienen acceso a una subred determinada a través de un enrutador. El resto de los usuarios deben poder acceder a la subred a través del router. ¿Qué debe usar para proporcionar esta funcionalidad?

✗ **A)** rotación de trabajos
✓ **B)** denegar implícita
✗ **C)** privilegio mínimo
✗ **D)** permitir implícito

explicación

Una denegación implícita puede asegurarse de que ciertos usuarios no tengan acceso a una subred a través de un enrutador. Los usuarios que NO tienen una denegación implícita pueden tener acceso a la subred. La denegación implícita se puede configurar en función de la dirección MAC del equipo u otros factores de este tipo.

El principio de privilegios mínimos concede a los usuarios solo los permisos que necesitan para realizar su trabajo.

La rotación de trabajos protege sus datos al proporcionar redundancia. Al implementar la rotación de trabajos, se asegura de que más de un administrador sepa cómo realizar cada trabajo.

Un permiso implícito permite a los usuarios con nombre específico tener acceso a un archivo determinado. Este permiso no impide que los usuarios tengan acceso a un determinado archivo.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender y aplicar los conceptos de confidencialidad, integridad y disponibilidad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y gestión de riesgos, postura por defecto

Listas de acceso del Cisco IOS: 10 cosas que usted debe saber, http://www.techrepublic.com/article/cisco-ios-access-lists-10-things-you-should-know/5731134

Pregunta #45 de 137

Id. de pregunta: 1104820

¿Qué se define en una política de uso aceptable?

- ✓ **A)** Cómo se permite a los usuarios emplear el hardware de la empresa
- ✗ **B)** El método que los administradores deben utilizar para realizar una copia de seguridad de los datos de red
- ✗ **C)** la sensibilidad de los datos de la empresa
- ✗ **D)** qué usuarios requieren acceso a determinados datos de la empresa

explicación

Una directiva de uso aceptable define cómo se permite a los usuarios emplear el hardware de la empresa. Por ejemplo, una directiva de uso aceptable, que a veces se conoce como directiva de uso, podría responder a las siguientes preguntas: ¿Se permite a los empleados almacenar archivos personales en los equipos de la empresa? ¿Se permite a los empleados jugar juegos de red en los descansos? ¿Se permite a los empleados "navegar por la Web" después de horas?

Una directiva de información define la confidencialidad de los datos de una empresa. En parte, una política de seguridad define la separación de tareas, que determina quién necesita acceso a cierta información de la empresa. Una directiva de copia de seguridad define el procedimiento que los administradores deben usar para realizar una copia de seguridad de la información de la empresa.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Desarrollar, documentar e implementar políticas, estándares, procedimientos y directrices de seguridad

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 1: Seguridad y Gestión de Riesgos, Directiva

Política de uso aceptable,http://www.sans.org/resources/policies/Acceptable_Use_Policy.pdf

---

Pregunta #46 de 137

Id. de pregunta: 1192920

Haga clic en cada uno de los encabezados del escenario para expandir o contraer su contenido. Debe leer todo el escenario para responder a la pregunta.

fondo

Usted es un profesional de la seguridad contratado recientemente por una empresa que cotiza en bolsa para ayudar a administrar la seguridad de la organización. La compañía tiene una oficina principal en Atlanta, GA, y sucursales en todo el sureste de los Estados Unidos. El departamento de TI tiene un pequeño personal alojado en la oficina de Atlanta.

Temas actuales

El año pasado, una tormenta invernal cerró las operaciones en la mayoría de sus oficinas. Si bien ninguna de sus instalaciones fue destruida y las operaciones normales se restauraron en 24 horas, a la administración le preocupa que no exista un plan de recuperación ante desastres. Se le ha pedido que prepare un plan para cubrir este tipo de interrupción.

Actualmente, su organización mantiene varias bases de datos grandes de contenido digital que son vitales para las operaciones de su organización. Se utilizan diferentes controles para administrar este contenido. La administración le ha pedido que implemente una solución para controlar la apertura, edición, impresión o copia de estos datos de una manera más centralizada.

En los próximos seis meses, su empresa planea mover todos los servidores y granjas de servidores a un centro de datos centralizado. El centro de datos ocupará el tercer piso de un edificio de seis pisos que actualmente está en construcción. La administración le ha pedido que se asegure de que el acceso al centro de datos esté estrictamente controlado. Durante ese mismo tiempo, es probable que su organización compre un competidor para fusionarse con su organización existente.

Recientemente, uno de los servidores de la intranet fue víctima de un ataque de denegación de servicio (DoS). El departamento de TI tardó más de 24 horas en volver a poner en funcionamiento el servidor. Durante ese tiempo, el personal de la oficina principal no pudo acceder a la importante información sobre recursos humanos disponible en el servidor de la intranet afectado.

La semana pasada, descubrió que se utilizaron varias cuentas de usuario en un intento de piratear su red. Afortunadamente, las cuentas fueron bloqueadas debido a intentos de inicio de sesión no válidos. Revise los registros y determine que tres de las cuentas se crearon para el personal que ya no está empleado por su organización.

Después de presionar durante años, ha recibido permiso de la administración para diseñar e implementar un programa integral de concienciación de seguridad en toda la organización.

¿Cuál de los siguientes factores debe considerar durante la fusión? (Elija todo lo que se aplique).)

✓ **A)** requisitos mínimos de seguridad

- ✓ **B)** gobierno de terceros
- ✓ **C)** hardware
- ✓ **D)** servicios

explicación

Durante la fusión, debe considerar todas las opciones dadas.

Durante cualquier fusión o adquisición, debe considerar:

- Hardware, software y servicios
- Gobierno de terceros
- Requisitos mínimos de seguridad
- Requerimientos mínimos de nivel de servicio

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Aplicar conceptos de gestión basada en el riesgo a la cadena de suministro

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y gestión de riesgos, Riesgos de seguridad en la cadena de suministro

Consideraciones de seguridad en el proceso de fusión/adquisición, https://www.sans.org/reading-room/whitepapers/casestudies/security-considerations-merger-acquisition-process-667

Pregunta #47 de 137

Id. de pregunta: 1114682

¿Qué acciones debe tomar primero en caso de un incendio en la instalación?

un. Evacuar la instalación.

B. Informe al administrador de la instalación.

c. Póngase en contacto con el departamento de bomberos.

d. Apagar los sistemas informáticos.

E. Consulte la documentación de respuesta a emergencias.

- ✗ **A)** Opción d

✗ **B)** opción e

✗ **C)** opción b

✓ **D)** Opciones A y D

✗ **E)** opciones A y B

✗ **F)** Opciones C y E

✗ **G)** opción A

✗ **H)** opción c

explicación

En caso de incendio, la evacuación de la instalación debe ser el primer paso. Si es posible, los sistemas informáticos y la energía eléctrica deben apagarse para evitar cualquier pérdida o daño a los sistemas críticos. Algunos sistemas de detección y prevención de incendios incluyen mecanismos de apagado automático para sistemas informáticos y energía eléctrica en caso de que se detecte un incendio.

Informar al gerente de la instalación y ponerse en contacto con el departamento de bomberos son los siguientes pasos a seguir después de evacuar la instalación y apagar los sistemas.

Los empleados deben ser capacitados sobre cómo actuar en una situación de emergencia. En el caso de cualquier emergencia, nadie tiene el tiempo para consultar el manual de procedimientos.

La respuesta de emergencia y los procedimientos son los siguientes:

- Procedimiento de evacuación
- Apagado del sistema
- Entrenamiento y ejercicios
- Pruebas periódicas del equipo
- Integración con planes de desastres
- Documentos de fácil acceso para diversas emergencias

La Asociación Nacional de Protección contra Incendios (NFPA) define los factores de riesgo a tener en cuenta al diseñar la protección contra incendios y seguridad para entornos informáticos. Debe utilizar los siguientes factores al evaluar el impacto del daño y la interrupción resultantes de un incendio, en este orden de prioridad:

- Los aspectos de seguridad de la vida de la función
- La amenaza de incendio de la instalación a los ocupantes o propiedad del área de computación
- La pérdida económica sufrida por la pérdida de la función informática o la pérdida de registros almacenados
- La pérdida económica sufrida por la pérdida del valor del equipo

Como en todas las evaluaciones de riesgo, la seguridad de la vida es siempre la prioridad número uno. La distancia de la instalación de una estación de bomberos no es un factor de riesgo según lo definido por la NFPA.

La NFPA recomienda que solo los registros esenciales mínimos absolutos, las existencias de papel, las tintas, los medios de grabación no utilizados u otros combustibles se almacenen en la sala de computadoras. Debido a la

amenaza de incendio, estos combustibles no deben almacenarse en la sala de computadoras o bajo pisos elevados, incluido el cableado viejo y sin usar. Los cables abandonados que se almacenan debajo del piso pueden interferir con el flujo de aire y los sistemas de extinción. Los cables no utilizados deben retirarse de la habitación. Las tapetecas y los almacenes de discos deben estar protegidos por un sistema de extinción y separados de la sala de computadoras por una construcción de paredes resistente al fuego, con una calificación de al menos una hora.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender y aplicar los conceptos de gestión de riesgos

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Incendios

---

Pregunta #48 de 137

Id. de pregunta: 1104796

¿Qué tipo de ley rige el pago de indemnizaciones y multas sin condenar a los infractores a la cárcel?

- ✗ **A)** derecho penal
- ✓ **B)** derecho civil
- ✗ **C)** ley de derechos de autor
- ✗ **D)** Derecho administrativo

explicación

La ley civil o extracontractual rige el pago de indemnizaciones y multas sin condenar a los infractores a la cárcel. Los delincuentes son personas que han engañado a personas o empresas y han causado daños o pérdidas. El jurado en el tribunal de justicia decide sobre la responsabilidad de la persona y determina las medidas correctivas. La responsabilidad de los altos funcionarios de la organización en relación con la protección de los sistemas de información de las organizaciones es perseguible con arreglo al derecho civil.

El derecho penal se aplica a los delincuentes que violan las leyes gubernamentales destinadas a proteger al público. El castigo común en un caso penal es una sentencia de cárcel para el individuo.

La ley de derecho de autor otorga el derecho a controlar la distribución o la reproducción de su obra a un autor. El trabajo puede incluir los escritos de un autor, las pinturas de un artista, los códigos de un programador, etc.

Una ley administrativa o reglamentaria garantiza que las empresas y los particulares se adhieran a las normas reglamentarias prescritas por el gobierno. Por ejemplo, una ley administrativa garantiza que un edificio tenga un

sistema de detección y extinción de incendios. Si la compañía no cumple con las leyes reglamentarias legales, los altos funcionarios de la compañía son responsables por negligencia y pueden ser penalizados.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender los problemas legales y reglamentarios relacionados con la seguridad de la información en un entorno global

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Principales Sistemas Legales

---

Pregunta #49 de 137

Id. de pregunta: 1111644

Durante una auditoría de seguridad reciente, los auditores señalan que el administrador de red también actúa como administrador de seguridad de la empresa. Sugieren que los deberes del administrador de seguridad se den a otra persona. ¿Qué tarea NO se debe transferir al nuevo administrador de seguridad?

- ✗ **A)** creación de perfiles de usuario
- ✗ **B)** implementación de control de acceso
- ✓ **C)** implementación de actualización de software
- ✗ **D)** implementación de revisiones de seguridad
- ✗ **E)** creación de contraseña de usuario inicial

explicación

La implementación de la actualización de software no debe transferirse al administrador de seguridad.

Al administrador de seguridad se le deben asignar todas las tareas relacionadas con la seguridad, incluidas las siguientes:

- Implementación y mantenimiento de dispositivos de seguridad y software, incluidos los parches de seguridad
- Implementación de la evaluación de la seguridad
- Creación y mantenimiento de perfiles de usuario
- Implementación y mantenimiento del control de acceso
- Configuración y mantenimiento de etiquetas de seguridad en un entorno de control de acceso obligatorio (MAC)
- Creación inicial de contraseñas
- Revisión del registro de auditoría

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
evaluar y aplicar los principios de gobierno de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Administrador de Seguridad

---

Pregunta #50 de 137

Id. de pregunta: 1111638

¿Cuál es la designación de un empleado que es responsable de mantener y proteger la información?

- ✗ **A)** propietario del sistema
- ✗ **B)** titular de los datos
- ✓ **C)** custodio de datos
- ✗ **D)** usuario de información

explicación

El custodio de datos es directamente responsable de mantener y proteger los datos, y es un rol que normalmente se delega en el personal del departamento de TI. Las responsabilidades incluyen la implementación y el mantenimiento de controles de seguridad. El rol del custodio de datos incluye las siguientes tareas:

- Mantenimiento de registros de actividad
- Verificación de la exactitud y fiabilidad de los datos
- Copia de seguridad y restauración de datos regularmente

El propietario de los datos controla el proceso de definición de los niveles de servicio de TI, el suministro de información durante la revisión de los controles y la autorización de la aplicación de controles de seguridad para proteger los activos de información de la organización. Un propietario de datos suele ser la administración de piezas. Por ejemplo, un gerente de unidad de negocio tiene la responsabilidad principal de proteger los activos de información mediante el ejercicio de la debida diligencia y las prácticas de debido cuidado.

El propietario de un sistema es responsable de mantener y proteger uno o más sistemas de procesamiento de datos. El rol incluye principalmente la integración de las características de seguridad necesarias en las aplicaciones e implica una decisión de compra de las aplicaciones. El propietario del sistema también garantiza que el acceso remoto, la administración de contraseñas y las configuraciones del sistema operativo proporcionen la seguridad necesaria.

Un usuario de información es una persona que utiliza los datos regularmente para cumplir con las responsabilidades del trabajo. Los usuarios deben poder acceder a la información basándose en el concepto de privilegios mínimos y solo en función de la necesidad de conocer para lograr los objetivos de seguridad de la organización.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
evaluar y aplicar los principios de gobierno de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, custodio de datos

---

Pregunta #51 de 137

Id. de pregunta: 1111652

Todos los siguientes están específicamente prohibidos por la Ley de Fraude y Abuso Informático, EXCEPTO:

✗ **A)** acceder a sabiendas a las computadoras de la institución financiera para obtener información no autorizada a la parte que accede

✗ **B)** revelar contraseñas de computadoras con la intención de defraudar

✗ **C)** acceder a sabiendas a las computadoras del gobierno federal para obtener información no autorizada a la parte que accede

✓ **D)** revelar información privada sin el permiso por escrito de la persona

explicación

Todos los actos enumerados están prohibidos por la Ley de Fraude y Abuso Informático, EXCEPTO la divulgación de información privada sin el permiso por escrito de la persona. Esta ley está prohibida por la Ley Federal de Privacidad de los Estados Unidos de 1974.

Los siguientes actos están específicamente prohibidos por la Ley de Fraude y Abuso Informático:

- Acceder a sabiendas a las computadoras del gobierno federal para obtener información no autorizada a la parte que accede
- Acceder a sabiendas a las computadoras de la institución financiera para obtener información no autorizada a la parte que accede
- Acceso consciente a las computadoras del gobierno federal cuando el acceso de esa computadora afecta el uso de la computadora por parte del gobierno
- Acceder a sabiendas a una computadora protegida para defraudar cuando no está autorizado para acceder a la computadora, o acceder a información que excede la información permitida por la parte que accede

- Transmitir a sabiendas aplicaciones, información, código o comandos para causar daños intencionalmente a un equipo protegido al que la parte que accede no está autorizada a acceder
- Revelar a sabiendas contraseñas de computadoras con la intención de defraudar
- Transmitir a sabiendas comunicaciones amenazantes para dañar un equipo protegido

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender los problemas legales y reglamentarios relacionados con la seguridad de la información en un entorno global

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Fraude Informático y Abuso Act (CFAA)

Pregunta #52 de 137

Id. de pregunta: 1104871

Está intentando predecir la probabilidad de que se produzca una amenaza y asignando valores monetarios en caso de que se produzca una pérdida. ¿Qué técnica está utilizando?

✗ **A)** Técnica delfos
✗ **B)** Análisis cualitativo de riesgos
✓ **C)** Análisis cuantitativo de riesgos
✗ **D)** Evaluación de la vulnerabilidad

explicación

El análisis cuantitativo de riesgos intenta predecir la probabilidad de que ocurra una amenaza y asigna un valor monetario en caso de que se produzca una pérdida.

La técnica Delphi es un tipo de análisis cualitativo de riesgos en el que cada miembro del equipo de análisis de riesgos emite opiniones anónimas. Las opiniones anónimas aseguran que los miembros no sean presionados a ponerse de acuerdo con otras partes.

Una evaluación de vulnerabilidad es un método para determinar las vulnerabilidades del sistema y sus riesgos. A continuación, se toman medidas para reducir el riesgo.

El análisis cualitativo de riesgos no asigna valores monetarios. Es simplemente un informe subjetivo compilado por el equipo de análisis de riesgos que describe las amenazas, las contramedidas y la probabilidad de que ocurra un evento.

Objetivo:

Seguridad y gestión de riesgos

Subobsecución:

Comprender y aplicar los conceptos de gestión de riesgos

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Quantitative Risk Analysis

---

Question #53 of 137

Question ID: 1104832

You are a member of the team that has been selected to create your organization's business continuity plan. What is the most vital document in this plan?

- ✗ **A)** occupant emergency plan (OEP)
- ✗ **B)** vulnerability analysis
- ✓ **C)** business impact analysis (BIA)
- ✗ **D)** disaster recovery plan

Explanation

The business impact analysis (BIA) is the most vital document to the business continuity plan. The majority of the steps of the business continuity plan rely on the results of the BIA. The goals of the BIA include resource requirements (identifying the resource requirements of the critical business unit processes), criticality prioritization (identifying and prioritizing every critical business unit process), and downtime estimation (estimating the maximum down time the business can tolerate).

The disaster recovery plan is created to ensure that your company is able to resume operation in a timely manner. As part of the business continuity plan, it mainly focuses on alternative procedures for processing transactions in the short term. It is carried out when the emergency occurs and immediately following the emergency. While it is an important part of the business continuity plan, it is not the most vital document because no other parts of the business continuity plan rely on it. Business recovery plans should be created for all areas within an organization.

A vulnerability analysis identifies your company's vulnerabilities. It is part of the BIA.

An occupant emergency plan (OEP) is created to ensure that injury and loss of life are minimized when an outage or disaster occurs. It also focuses on property damage. While it is an important part of the business continuity plan, it is not the most vital because no other parts of the business continuity plan rely on it.

Objective:

Security and Risk Management

Sub-Objective:

Identify, analyze, and prioritize Business Continuity (BC) requirements

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Business Impact Analysis (BIA)

Question #54 of 137

Question ID: 1111669

You have been instructed to maintain the business continuity plan. Which option is NOT a reason to do this?

✗ **A)** infrastructure changes

✗ **B)** personnel changes

✗ **C)** organizational changes

✓ **D)** budget changes

Explanation

Budget changes are not a reason to maintain the business continuity plan.

The business continuity plan should be maintained for several reasons including:

- Infrastructure changes
- Environment changes
- Organizational changes
- Hardware, software, and application changes
- Personnel changes

The steps in the business continuity planning process are as follows:

- Develop the business continuity planning policy statement.
- Conduct the business impact analysis (BIA).
- Identify preventative controls.
- Develop the recovery strategies.
- Develop the contingency plans.
- Test the plan, and train the users.
- Mantener el plan.

Objetivo:

Seguridad y gestión de riesgos

Subobsecución:

Identificar, analizar y priorizar los requerimientos de Continuidad del Negocio (BC, Business Continuity)

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Mantener el Plan

---

Pregunta #55 de 137

Id. de pregunta: 1114680

¿Qué controles son parte integral de la administración de la seguridad de la información?

a. Controles de la información

b. Controles físicos

c. Controles técnicos

d. Controles administrativos

e. Controles de comunicación

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

explicación

La administración de seguridad incluye tres categorías de controles: administrativos, técnicos y físicos.

Los controles administrativos incluyen el desarrollo y mantenimiento de políticas, procedimientos, normas y directrices. También incluye la realización de capacitación periódica sobre la concienciación sobre la seguridad y la implementación del proceso de control de cambios para supervisar los cambios en la infraestructura. La separación de funciones, la rotación de puestos, los procedimientos de personal y las investigaciones son ejemplos de este tipo de control.

Los controles técnicos incluyen la implementación y el mantenimiento de controles de acceso, análisis de auditoría, implementación de dispositivos de seguridad de hardware y software y técnicas de cifrado, autenticación e identificación.

Los controles físicos incluyen controles que una organización puede implementar para el perímetro y la seguridad interna de una infraestructura de instalación. Los controles de seguridad física incluyen cercas, guardias, iluminación, alarmas, circuito cerrado de televisión (CCTV), sistemas de detección de intrusos (IDS) y cerraduras.

Los controles técnicos, físicos y administrativos se pueden clasificar además como controles preventivos, correctivos, disuasorios, de recuperación, de compensación o detectives. Se despliegan controles preventivos para evitar cualquier incidencia antes de su ocurrencia. Los controles detectives pueden detectar y generar una alerta después de detectar cualquier evento no autorizado. Un ejemplo de control administrativo preventivo es la separación de funciones, que reduce drásticamente la posibilidad de colusión y previene el fraude. Un ejemplo de un control técnico detectivesco es un IDS que monitorea una red en tiempo real para cualquier actividad no autorizada.

Los controles de información y comunicación son términos genéricos y no constituyen una categoría de controles de seguridad de la información. Por lo tanto, ambas opciones no son válidas.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender y aplicar los conceptos de gestión de riesgos

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 1: Seguridad y Gestión de Riesgos, Administrativo

---

Pregunta #56 de 137

Id. de pregunta: 1104853

Durante la planificación de la continuidad del negocio, debe obtener la expectativa de pérdida única (SLE) del servidor de archivos de la empresa. ¿Qué fórmula debe utilizar para determinar esto?

- ✗ **A)** factor de exposición (EF) x tasa anualizada de ocurrencia (ARO)
- ✗ **B)** expectativa de pérdida anualizada (ALE) x tasa anualizada de ocurrencia (ARO)
- ✓ **C)** valor del activo x factor de exposición (EF)
- ✗ **D)** valor del activo x tasa anualizada de ocurrencia (ARO)

explicación

Para determinar la expectativa de pérdida única (LES) de un activo, debe utilizar la siguiente fórmula:

(Valor del activo) x (factor de exposición)

Las otras opciones no son válidas.

El factor de exposición (EF) es el porcentaje de pérdida que resultaría si ocurriera una determinada amenaza. La expectativa de pérdida anualizada (ALE) se calcula utilizando la siguiente fórmula:

(LES) x (tasa anualizada de ocurrencia)

La tasa anualizada de ocurrencia (ARO) es una estimación de la frecuencia de una amenaza específica que ocurre. Los valores pueden ser de 0,0 (nunca) a 1,0 (una vez al año).

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender y aplicar los conceptos de gestión de riesgos

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Análisis Cuantitativo de Riesgos

---

Pregunta #57 de 137

Id. de pregunta: 1104851

¿Qué declaración describe correctamente la seguridad de la información?

- ✗ **A)** La seguridad de la información es un procedimiento continuo.
- ✗ **B)** La seguridad de la información es una implementación única para proteger la infraestructura.
- ✓ **C)** La seguridad de la información es un proceso continuo.
- ✗ **D)** La seguridad de la información se ocupa únicamente del hardware y el software.

explicación

La seguridad de la información es un proceso continuo de protección de las operaciones comerciales de una organización. La seguridad comienza con el establecimiento de una política y estándares de seguridad, es seguida por la implementación de hardware y software a través de procedimientos operativos estándar, y termina con la impartición de capacitación en conciencia de seguridad a los empleados. La formación de concienciación sobre seguridad cubre el uso aceptable de los recursos y los riesgos que las amenazas pueden suponer para las operaciones empresariales.

La seguridad de la información gira como un proceso continuo mediante la protección de la red, la supervisión de la red, la prueba de la infraestructura en busca de lagunas y la rectificación de errores mediante el cierre de las lagunas

observadas durante el curso de la supervisión y las pruebas.

La seguridad de la información es un proceso y no un procedimiento. Un procedimiento hace referencia a los pasos repetibles estándar que se pueden seguir al implementar hardware y software. Los procedimientos incorporan todas las acciones detalladas paso a paso que el personal debe seguir.

La seguridad de la información no solo se ocupa del hardware y el software, sino que también abarca a las personas de la organización y la información procesada por ellas.

La seguridad de la información es un proceso en evolución que se mueve en paralelo a las operaciones comerciales de la organización y no es una inversión única.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender y aplicar los conceptos de gestión de riesgos

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 1: Seguridad y Gestión de Riesgos, Informes y Mejora Continua

---

Pregunta #58 de 137

Id. de pregunta: 1113897

¿Cuándo se utilizan las circunstancias extremas?

- ✗ **A)** cuando no se mantiene una cadena de custodia
- ✗ **B)** cuando un sospechoso es tentado
- ✓ **C)** cuando las pruebas podrían ser destruidas
- ✗ **D)** cuando un sospechoso queda atrapado

explicación

Las circunstancias extremas se utilizan cuando las pruebas podrían ser destruidas. Las circunstancias extremas permiten a los funcionarios incautar pruebas antes de su destrucción y sin una orden judicial. Un juez decidirá en un momento posterior si la incautación fue apropiada y si la evidencia puede ser admitida en la corte.

Cuando un sospechoso es tentado, las declaraciones del sospechoso pueden ser admitidas en la corte. Una tentación se produce cuando un sistema tiene defectos aparentes que estaban deliberadamente disponibles para la penetración y la explotación. La tentación a menudo se implementa atrayendo al perpetrador a una zona atractiva o presentándole un objetivo lucrativo después de que el delito ya se haya iniciado.

Cuando un sospechoso es atrapado, las declaraciones del sospechoso no pueden ser admitidas en la corte.

Cuando no se mantiene una cadena de custodia, las pruebas no serán admitidas en el tribunal porque no es posible probar el estado de las pruebas.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender los problemas legales y reglamentarios relacionados con la seguridad de la información en un entorno global

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y gestión de riesgos, contractuales, legales, estándares de la industria y cumplimiento normativo

---

Question #59 of 137

Question ID: 1192910

During a meeting, you present management with a list of the access controls used on your network. You explain that these controls include preventative, detective, and corrective controls. Which control is an example of a corrective control?

- ✗ **A)** router
- ✗ **B)** audit log
- ✗ **C)** intrusion detection system (IDS)
- ✓ **D)** antivirus software

Explanation

Antivirus software is an example of a corrective technical control because it attempts to correct any damage that was inflicted during a security breach. Antivirus software can also be considered a compensative technical control.

Routers are examples of preventative technical controls because they prevent security breaches. Routers are a compensatory technical control. IDSs are a detective technical control and a compensative technical control

Audit logs are examples of detective technical controls because they detect security breaches. Audit logs are also a compensative technical control.

There are three categories of access control: technical, administrative, and physical controls. Controls are the countermeasures for vulnerabilities. A technical control is put into place to restrict access. Technical controls work to protect system access, network architecture and access, control zones, auditing, and encryption and protocols. An

administrative control is a control that dictates how security policies are implemented to fulfill the company's security goals. Administrative controls include policies and procedures, personnel controls, supervisory structure, security training, and testing. A physical control is implemented to secure physical access to an object, such as a building, a room, or a computer. Physical controls include badges, locks, guards, network segregation, perimeter security, computer controls, work area separation, backups, and cabling.

The three access control categories provide seven different functionalities or purposes:

- Preventative - A preventative control prevents security breaches and avoids risks.
- Detective - A detective control detects security breaches as they occur.
- Corrective - A corrective control restores control and attempts to correct any damage that was inflicted during a security breach.
- Deterrent - A deterrent control deters potentials violations.
- Recovery - A recovery control restores resources.
- Compensative - A compensative control provides an alternative control if another control may be too expensive. All controls are generally considered compensative.
- Directive - A directive control provides mandatory controls based on regulations or environmental requirements.

Each category of control includes controls that provide different functions. For example, a fence is both a deterrent physical control and a compensative physical control. Monitoring and supervising is both a detective administrative control and a compensative administrative control.

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply risk management concepts

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Corrective

---

Question #60 of 137

Question ID: 1111650

Which United States law was established in 2001 to reduce restrictions to search telephone, e-mail communications, medical, financial, and other records?

✗ **A)** Kennedy-Kassebaum Act

✗ **B)** Ley Sarbanes-Oxley (SOX)

✓ **C)** Ley Patriota

✗ **D)** Ley Gramm-Leach-Bliley

explicación

La Ley Patriota se estableció en 2001 para reducir las restricciones a la búsqueda de registros telefónicos, de comunicaciones por correo electrónico, médicos, financieros y de otro tipo. Hasta que se estableció la Ley Patriota, los funcionarios encargados de hacer cumplir la ley estaban limitados por la Cuarta Enmienda. La Ley Patriota generalmente solo se usa en situaciones en las que el gobierno de los Estados Unidos está investigando a agentes de los gobiernos. Las restricciones de la Ley Patriota y la Cuarta Enmienda no se aplican a los individuos privados no empleados por el gobierno de los Estados Unidos. Sin embargo, hay excepciones en las que la Cuarta Enmienda se aplica a ciudadanos privados si el ciudadano está actuando en nombre del gobierno, incluyendo las siguientes:

- El gobierno es consciente de la intención de buscar o está al tanto de una búsqueda realizada por el particular y no se opone a estas acciones.
- El particular realiza la búsqueda para ayudar al gobierno.
- El particular lleva a cabo un registro que requeriría una orden de registro si lo lleva a cabo una entidad gubernamental.

La Ley Sarbanes-Oxley estableció prácticas y métodos contables que las empresas que cotizan en bolsa deben utilizar cuando informan de su situación financiera. La Ley Gramm-Leach-Bliley estableció políticas de privacidad para las instituciones financieras. La Ley Kennedy-Kassebaum, también conocida como ley de portabilidad y responsabilidad del seguro médico (HIPAA, por sus, por suste), estableció estándares nacionales para el almacenamiento, uso y transmisión de datos médicos.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender los problemas legales y reglamentarios relacionados con la seguridad de la información en un entorno global

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Leyes y Reglamentos

---

Pregunta #61 de 137

Id. de pregunta: 1104840

Como administrador de seguridad de una organización, debe evitar conflictos de intereses al asignar personal para completar determinadas tareas de seguridad. ¿Qué principio de seguridad de operaciones está implementando?

✗ **A)** atención debida
✓ **B)** separación de funciones
✗ **C)** Debida diligencia

✗ **D)** rotación de trabajos

explicación

Cuando se evitan conflictos de intereses al asignación de personal para completar determinadas tareas de seguridad, se está implementando la separación de funciones. La separación de funciones es una medida preventiva. Para cometer un acto ilegal, la colusión debe ocurrir entre el personal.

La diligencia debida se produce cuando se evalúa la información para identificar vulnerabilidades, amenazas y problemas relacionados con el riesgo.

El debido cuidado se produce cuando una organización ha tomado las medidas necesarias para proteger la organización, sus recursos y personal.

La rotación de trabajos se produce cuando más de una persona completa las tareas de un solo puesto dentro de la organización.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Contribuir y aplicar las políticas y procedimientos de seguridad del personal

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 1: Seguridad y Gestión de Riesgos, Separación de funciones

---

Pregunta #62 de 137

Id. de pregunta: 1192902

Haga clic en cada uno de los encabezados del escenario para expandir o contraer su contenido. Debe leer todo el escenario para responder a la pregunta.

fondo

Usted es un profesional de la seguridad contratado recientemente por una empresa que cotiza en bolsa para ayudar a administrar la seguridad de la organización. La compañía tiene una oficina principal en Atlanta, GA, y sucursales en todo el sureste de los Estados Unidos. El departamento de TI tiene un pequeño personal alojado en la oficina de Atlanta.

Temas actuales

El año pasado, una tormenta invernal cerró las operaciones en la mayoría de sus oficinas. Si bien ninguna de sus instalaciones fue destruida y las operaciones normales se restauraron en 24 horas, a la administración le preocupa

que no exista un plan de recuperación ante desastres. Se le ha pedido que prepare un plan para cubrir este tipo de interrupción.

Actualmente, su organización mantiene varias bases de datos grandes de contenido digital que son vitales para las operaciones de su organización. Se utilizan diferentes controles para administrar este contenido. La administración le ha pedido que implemente una solución para controlar la apertura, edición, impresión o copia de estos datos de una manera más centralizada.

En los próximos seis meses, su empresa planea mover todos los servidores y granjas de servidores a un centro de datos centralizado. El centro de datos ocupará el tercer piso de un edificio de seis pisos que actualmente está en construcción. La administración le ha pedido que se asegure de que el acceso al centro de datos esté estrictamente controlado. Durante ese mismo tiempo, es probable que su organización compre un competidor para fusionarse con su organización existente.

Recientemente, uno de los servidores de la intranet fue víctima de un ataque de denegación de servicio (DoS). El departamento de TI tardó más de 24 horas en volver a poner en funcionamiento el servidor. Durante ese tiempo, el personal de la oficina principal no pudo acceder a la importante información sobre recursos humanos disponible en el servidor de la intranet afectado.

La semana pasada, descubrió que se utilizaron varias cuentas de usuario en un intento de piratear su red. Afortunadamente, las cuentas fueron bloqueadas debido a intentos de inicio de sesión no válidos. Revise los registros y determine que tres de las cuentas se crearon para el personal que ya no está empleado por su organización.

Después de presionar durante años, ha recibido permiso de la administración para diseñar e implementar un programa integral de concienciación de seguridad en toda la organización.

¿Qué tipo de interrupción afectó a muchas de las oficinas el año pasado?

- ✗ **A)** catástrofe
- ✓ **B)** desastre natural
- ✗ **C)** desastre causado por el ser humano
- ✗ **D)** desastre tecnológico

explicación

Un desastre natural afectó a muchas de las oficinas el año pasado. Una tormenta invernal es un desastre natural.

Una catástrofe es una interrupción que tiene un impacto más amplio y prolongado que un desastre natural, y por lo general implica instalaciones destruidas o tiempo de inactividad prolongado. La tormenta invernal no destruyó las instalaciones ni dio lugar a un tiempo de inactividad prolongado.

Un desastre tecnológico ocurre cuando un dispositivo falla. El fallo del servidor de la intranet podría considerarse un desastre tecnológico. Solo afectó al personal de la oficina principal.

Un desastre causado por el ser humano ocurre a través de la intención o error humano. El error del servidor de la intranet podría considerarse un desastre causado por el ser humano porque fue iniciado por atacantes externos.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Identificar, analizar y priorizar los requerimientos de Continuidad del Negocio (BC, Business Continuity)

Referencias:

Cissp Cert Guide (3ª edición), Capítulo 1: Seguridad y gestión de riesgos, continuidad del negocio

(Mi) CISSP señala la continuidad del negocio y la planificación de la recuperación ante desastres, https://itblog.adrian.citu.name/2012/10/16/my-cissp-notes-business-continuity-and-disaster-recovery-planning/

Pregunta #63 de 137

Id. de pregunta: 1192917

La administración le ha pedido que se asegure de que el voltaje se mantenga limpio y estable en sus instalaciones. ¿Qué componente es EL MÁS apropiado para este propósito?

✗ **A)** Hvac
✗ **B)** círculo concéntrico
✗ **C)** Hp.
✓ **D)** acondicionadores de línea

explicación

Las fluctuaciones en el suministro de voltaje, como picos y sobretensiones, pueden dañar los circuitos y componentes electrónicos. Un acondicionador de línea garantiza un suministro de voltaje limpio y constante filtrando la alimentación entrante y eliminando las fluctuaciones e interferencias.

Una fuente de alimentación ininterrumpida (UPS) proporciona una distribución limpia de la energía. El UPS proporciona una fuente de alimentación de respaldo. Un UPS también puede proporcionar supresión de sobretensiones, pero solo puede proteger los elementos conectados a él. Además, la protección proporcionada es muy limitada. Para problemas de voltaje para la fuente de alimentación primaria, debe utilizar reguladores de voltaje o acondicionadores de línea.

El sistema de calefacción, ventilación y aire acondicionado (HVAC) se instala en un edificio para regular la temperatura. Esto incluye plantas de aire acondicionado, enfriadores, conductos y sistemas de calefacción. HVAC también se conoce como control de clima. Es importante tener en cuenta que HVAC no tiene ningún papel en la

regulación de la tensión. HVAC debe mantener un nivel de humedad de 40 a 60 por ciento en el aire. La alta humedad puede causar condensación en las piezas de la computadora o corrosión en las conexiones eléctricas. Un nivel de humedad bajo puede causar electricidad estática que puede dañar los componentes electrónicos de los equipos informáticos. La electricidad estática también se puede reducir utilizando aerosoles antiestáticos y pisos antiestáticos.

El enfoque de círculo concéntrico define una zona de seguridad circular y determina el control de acceso físico. La zona debe estar asegurada por vallas, insignias, mantraps, guardias, perros y sistemas de control de acceso, como sistemas de identificación biométrica. El círculo concéntrico es una arquitectura de defensa en capas y no se ocupa de la energía eléctrica.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender y aplicar los conceptos de gestión de riesgos

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 1: Seguridad y Gestión de Riesgos, Electricidad

---

Pregunta #64 de 137

Id. de pregunta: 1192912

La administración le pide que proporcione una lista de todos los controles de acceso que detectarán cuando se produce un problema de seguridad. ¿Qué control es un ejemplo de esto?

✗ **A)** enrutador
✗ **B)** lista de control de acceso (ACL)
✓ **C)** registro de auditoría
✗ **D)** encriptación

Explanation

An audit log is an example of a detective technical control because it detects security breaches once they have occurred. An audit log is also considered to be a compensative technical control.

Routers, firewalls, and access control lists (ACLs) are examples of preventative technical controls because they prevent security breaches. They are all also compensative technical controls.

There are three categories of access control: technical, administrative, and physical controls. A technical control is put into place to restrict access. Technical controls work to protect system access, network architecture and access, control zones, auditing, and encryption and protocols. An administrative is developed to dictate how security policies are

implemented to fulfill the company's security goals. Administrative controls include policies and procedures, personnel controls, supervisory structure, security training, and testing. A physical control is implemented to secure physical access to an object, such as a building, a room, or a computer. Physical controls include badges, locks, guards, network segregation, perimeter security, computer controls, work area separation, backups, and cabling.

The three access control categories provide seven different functionalities or purposes:

- Preventative - A preventative control prevents security breaches and avoids risks.
- Detective - A detective control detects security breaches as they occur.
- Corrective - A corrective control restores control and attempts to correct any damage that was inflicted during a security breach.
- Deterrent - A deterrent control deters potentials violations.
- Recovery - A recovery control restores resources.
- Compensative - A compensative control provides an alternative control if another control may be too expensive. All controls are generally considered compensative.
- Directive - A directive control provides mandatory controls based on regulations or environmental requirements.

Each category of control includes controls that provide different functions. For example, a security badge is both a preventative physical control and a compensative physical control. Monitoring and supervising is both a detective administrative control and a compensative administrative control.

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply risk management concepts

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Detective

---

Question #65 of 137

Question ID: 1104800

Based on the Federal Privacy Act of 1974, which type of permission must be obtained by a government agency to disclose private information that the agency collected?

✗ **A)** verbal permission

✓ **B)** written permission

✗ **C)** no permission

✗ **D)** implied permission

Explanation

According to the Federal Privacy Act of 1974, a government agency needs written permission to disclose private information that the agency collected. If this written permission is not obtained, the individual whose information was disseminated can sue the federal government.

None of the other types of permission will allow a government agency to disclose private information.

Objective:
Security and Risk Management

Sub-Objective:
Understand legal and regulatory issues that pertain to information security in a global

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Federal Privacy Act of 1974

Question #66 of 137

Question ID: 1192903

Which statement is true of an information processing facility?

- ✓ **A)** Doors and walls should have the same fire rating.
- ✗ **B)** A critical path analysis does not have to include a redundant path for every critical path.
- ✗ **C)** Windows should be shielded by metallic bars.
- ✗ **D)** Critical areas must be illuminated six feet high.

Explanation

The doors and walls of an information processing facility should have the same fire rating, in conformance with safety codes and regulations. Fire extinguishers should be kept at known places in the information facility. Doors must resist forced entry to avoid theft or access to computer systems.

To avoid trapping people during fire and flood, windows should not be shielded with metallic bars.

According to the National Institute of Standards and Technology (NIST), critical areas must be illuminated to a height of eight feet high and with two foot-candles of intensity.

A critical path analysis can determine the level of protection for an environment by keeping track of environmental components, their interaction, and interdependencies. A critical path analysis includes a redundant path for every critical path to ensure uninterrupted business operation for the organization.

Objective:

Security and Risk Management

Sub-Objective:

Contribute to and enforce personnel security policies and procedures

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Fire

---

Question #67 of 137

Question ID: 1111656

All of the following are examples of computer-targeted crime, EXCEPT:

- ✗ **A)** installing a virus on a computer to destroy the data on the computer
- ✗ **B)** carrying out a distributed denial-of-service (DDoS) attack
- ✓ **C)** obtaining confidential data by attacking the servers that contain the data
- ✗ **D)** carrying out a buffer overflow attack

Explanation

Obtaining confidential data by attacking the servers that contain the data is NOT an example of computer-targeted crime. It is an example of a computer-assisted crime.

The four categories of computer crime are as follows:

- computer-assisted crime - This category of crime is one in which a computer is used as a tool to carry out a crime.
- computer-targeted crime - This category of crime is one in which a computer is the victim of the crime.
- computer-incidental crime - This category of crime is one in which a computer is involved in the crime incidentally. The computer is not the target of the crime and is not the main tool used to carry out the crime.
- computer-prevalence crime - This category of crime is one that results because computers are so prevalent in today's world. Examples include violating commercial software copyrights and software piracy.

Examples of computer-targeted crimes include the following:

- carrying out a buffer overflow attack
- carrying out a distributed denial of service (DDoS) attack
- installing a virus on a computer to destroy the data on the computer

It difficult to investigate computer crime and track down the criminal because criminals can hide their identity and hop from one network to the next.

Objective:
Security and Risk Management

Sub-Objective:
Understand legal and regulatory issues that pertain to information security in a global

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, computer-targeted crime

---

Question #68 of 137

Question ID: 1104834

Which role is considered the leader of the business continuity plan committee and is responsible for the overall success of the business continuity plan?

- ✗ **A)** IT manager
- ✗ **B)** security manager
- ✗ **C)** disaster recovery manager
- ✓ **D)** business continuity coordinator

Explanation

The business continuity coordinator is considered the leader of the business continuity plan committee and is responsible for the overall success of the business continuity plan.

The IT manager and security manager should be members of the business continuity committee or should have direct representatives. However, they usually do not lead the business continuity plan committee.

The disaster recovery manager is responsible for the short-term operations immediately following a disaster until all functions of the disaster recovery plan have been implemented. This person does not usually have the additional responsibility of being the leader of the business continuity plan committee.

Objective:
Security and Risk Management

Sub-Objective:
Identify, analyze, and prioritize Business Continuity (BC) requirements

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Personnel Components

Question #69 of 137

Question ID: 1104815

Internet Explorer (IE) is configured to block all pop-ups. You access a research site that implements a required pop-up immediately after login. You must ensure that the pop-up that is implemented after logging in is never blocked. What should you do?

✗ **A)** Change the pop-up blocker setting to Medium.

✗ **B)** Change the pop-up blocker setting to Low.

✗ **C)** Hold down Ctrl+Alt while the pop-up opens.

✓ **D)** Add the Web site to the Allowed sites list on the Pop-up Blocker Settings dialog box.

Explanation

You should add the Web site to the Allowed sites list on the Pop-up Blocker Settings dialog box in IE. This will ensure that the pop-up that is implemented after logging in is never blocked. If you upgrade Internet Explorer and pop-ups are not displaying properly, you should check the Pop-Up Blocker settings.

You should not hold down Ctrl+Alt while the pop-up opens. This technique should only be used when you want to view a pop-up once.

You should not change the Pop-Up Blocker setting to Medium or Low. This would reduce the security of Internet Explorer and would probably allow more pop-ups than you intended. In addition, there is no guarantee that the pop-up you want to see would not be blocked.

Objective:
Security and Risk Management

Sub-Objective:
Understand legal and regulatory issues that pertain to information security in a global

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Computer Crime Examples

Question #70 of 137

Question ID: 1114676

You have been asked to select members of the business continuity plan committee. This committee will work with you to create the business continuity plan. Which rules are vital to the formation of this committee?

a. All business units must be represented.

b. Senior management must be represented.

c. Only vital business units should be represented.

d. The committee should NOT be responsible for executing the business continuity plan.

- ✗ **A)** option c
- ✗ **B)** option d
- ✗ **C)** all of the options
- ✗ **D)** options c and d
- ✓ **E)** options a and b
- ✗ **F)** option a
- ✗ **G)** option b

Explanation

All business units must be represented in the business continuity plan committee. This will ensure that all systems vital to the operation of the business units are identified.

Senior management must be represented. Senior business management is ultimately responsible for identifying and prioritizing critical systems. In the business continuity and disaster recovery process, senior management should perform the following:

- Delegate recovery roles.
- Publicly praise successes.
- Closely control media and analyst communications.

Because all business units are vital to its operation, all business units should be represented. Trying to determine which business units are more vital than others is an impossible and subjective task.

The committee should be responsible for executing the business continuity plan. Giving them ownership and responsibility of the plan will ensure that more attention will be paid in the planning and testing phases.

Objective:
Security and Risk Management

Sub-Objective:
Identify, analyze, and prioritize Business Continuity (BC) requirements

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Continuity Planning and the Business Continuity Plan (BCP)

Question #71 of 137

Question ID: 1192897

Which role is delegated to personnel of the IT department and is responsible for maintaining the integrity and security of the data?

✗ **A)** data owner

✓ **B)** data custodian

✗ **C)** process owner

✗ **D)** system owner

Explanation

The data custodian is directly responsible for maintaining and protecting the data. This role is typically delegated to the IT department staff and includes implementing the organization security through the implementation and maintenance of security controls. The data custodian role also includes the following tasks:

- Maintaining records of activity
- Verifying the accuracy and reliability of the data
- Backing up and restoring data on a regular basis

The data owner is typically part of management. The data owner also controls the process of defining the IT service levels, provides information during the review of controls, and is responsible for authorizing the enforcement of security controls to protect the information assets of the organization. For example, a business unit manager has the primary responsibility of protecting information assets by exercising the due diligence and due care practices. Another information classification role is the data user.

The system owner is responsible for maintaining and protecting one or more data processing systems. The role primarily includes integration of the required security features into the applications and a purchase decision of the applications. The system owner also ensures that the remote access control, password management, and operation system configurations provide the necessary security. System and information owners are responsible for ensuring that proper controls are in place to address the integrity, confidentiality, and availability of IT systems and data. One system could have multiple information owners.

A process owner is responsible for defining, maintaining, and monitoring the different processes running in an organization. An example of a process may be accepting and shipping an order to a customer.

Objective:
Security and Risk Management

Sub-Objective:
Evaluate and apply security governance principles

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management Data Custodian

---

Question #72 of 137

Question ID: 1113906

Which statement is true of the staff members of an organization in the context of information security?

- ✓ **A)** They pose more threat than external hackers.
- ✗ **B)** They must be trained to handle internal violations of the security policy.
- ✗ **C)** They require extensive understanding of security.
- ✗ **D)** They are responsible for protecting and backing up confidential data.

Explanation

The staff members of an organization pose more threat than external hackers. Disgruntled employees typically attempt the security breaches in an organization. Existing employees can accidentally commit a security breach and may put the security of the organization at risk. User accounts should be immediately deleted and the associated privileges should be revoked for employees who have been terminated or have left the organization.

It is not the job of the staff member to handle and respond to issues of information security violation. Staff members should report the incident to the department manager. The department manager will take the necessary steps as a part of incident response.

Typically, it is the job of the IT department to ensure that critical data is duly backed up on a periodical basis and that only identified employees with necessary privileges have access to confidential information.

Only those staff members with a direct role in the security function of an organization need extensive security knowledge. Most staff members will need security awareness training on security policies, security practices, acceptable resource usage, and noncompliance implications.

Objective:
Security and Risk Management

Sub-Objective:
Contribute to and enforce personnel security policies and procedures

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Employment Candidate Screening

---

Question #73 of 137

Question ID: 1113900

Which statement is NOT true of the Computer Security Act of 1987?

✗ **A)** A computer security plan should be developed for a network.

✓ **B)** The act pertains to confidential and sensitive data held by private organizations.

✗ **C)** Computers containing sensitive information should be identified.

✗ **D)** There should be security awareness training for individuals.

Explanation

The Computer Security Act of 1987 pertains to confidential and sensitive information maintained by federal agencies. This act does not deal with data held by private organizations.

The Computer Security Act of 1987 has the following requirements:

- The federal agency should identify the computer systems that contain sensitive information.
- A security plan should be developed and implemented for the systems' security.
- Periodic security awareness training should be conducted for employees.
- Acceptable computer usage practices should be defined in advance.
- The government agencies should ensure that employees maintain a certain level of awareness and protection.

The primary purpose of the Computer Security Act of 1987 is to safeguard sensitive information of the federal government and to ensure that all federal computer systems fulfill a certain desired level of security to ensure the confidentiality, integrity, and availability of information.

Objective:
Security and Risk Management

Sub-Objective:
Understand legal and regulatory issues that pertain to information security in a global

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Computer Security Act of 1987

Computer Security Act of 1987, http://www.epic.org/crypto/csa/csa.html

---

Question #74 of 137

Question ID: 1104782

You are designing employee termination process guidelines. Which activity is NOT included in the employee termination process?

- ✓ **A)** signing a non-disclosure agreement
- ✗ **B)** submission of identification card by the employee
- ✗ **C)** escorting employee off the premises immediately
- ✗ **D)** disabling the employee's user account

Explanation

Non-disclosure agreements (NDAs) are signed at the time of hiring an employee and not during termination. NDAs impose a contractual obligation on employees to maintain the confidentiality of information, stating that a disclosure of information can lead to legal ramifications and penalties. An NDA is a contract through which the parties agree that they will not disclose the information covered by the agreement. An NDA creates a confidential relationship between the parties.

NDAs can be used to protect information that is confidential for an organization and its business operations.

Employees who have been terminated should submit company supplies, such as ID cards, badges, and keys, and should be escorted immediately off the premises after the exit interview process. The user account of the terminated employee should be either disabled or deleted, and the access privileges should be revoked.

Objective:
Security and Risk Management

Sub-Objective:
Determine compliance requirements

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Employment Agreement and Policies

---

Question #75 of 137

Question ID: 1111682

What is NOT an example of an operational control?

- ✓ **A)** a business continuity plan
- ✗ **B)** a backup control

✗ **C)** configuration management

✗ **D)** an audit trail

Explanation

A business continuity plan refers to the procedures undertaken for dealing with long-term unavailability of business processes and resources. Business continuity planning differs from disaster recovery. Disaster recovery aims at minimizing the impact of a disaster. Business continuity planning includes the following steps:

- Moving critical systems to another environment during the repair of the original facility
- Performing operations in a constrained mode with lesser resources till the conditions of the primary facility return to normal.
- Dealing with customers, partners, and shareholders through various channels until the original channel is restored.

Operational controls ensure the confidentiality, integrity, and availability of business operations by implementing security as a continuous process.

Audit trails are operational controls and detective controls. Audit trails identify and detect not only unauthorized users but also authorized users who are involved in unauthorized activities and transactions. Audit trails achieve the security objectives defined by the security policy of an organization, and ensure the accountability of users in the organization. They provide detailed information regarding the computer, the resource usage, and the activities of users. In the event of an intrusion, audit trails can help identify frauds and unauthorized user activity.

Backup controls, software testing, and anti-virus management are other examples of operational software controls.

Configuration management is an operational control. Configuration management identifies both controls and audit changes made to the trusted computing base (TCB). The audit changes include changes made to the hardware, software, and firmware configurations throughout the operational life cycle of infrastructural assets. Configuration management ensures that changes to the infrastructure take place in a controlled manner and follow a procedural approach. Configuration management also ensures that future changes to the infrastructure do not violate the organization's security policy and security objectives.

Maintenance accounts are considered a threat to operational controls. This is because maintenance accounts are commonly used by hackers to access network devices.

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply risk management concepts

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Operational

Question #76 of 137

Question ID: 1104876

Which operations security triples component is used to group all hardware, software, and informational resources?

- ✓ **A)** assets
- ✗ **B)** vulnerability
- ✗ **C)** system
- ✗ **D)** threats
- ✗ **E)** media

Explanation

An asset is the operations security triples component that is used to group all hardware, software, and informational resources. Asset, threats, and vulnerabilities are the components of operation security are sometimes referred to as the operations security triples.

A threat is defined as a potential hazard that that can exploit vulnerabilities in the information system.

A vulnerability is a weakness in the system, software, hardware, or procedure. This weakness can be exploited by a threat agent, leading to a risk of loss potential.

Media and systems are not defined as the components of operations security triples.

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply risk management concepts

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Risk Management Concepts

---

Question #77 of 137

Question ID: 1192909

You are working with management and the human resources department to put a security policy and several personnel controls into place. To which access control category do the controls belong?

- ✗ **A)** technical
- ✓ **B)** administrative
- ✗ **C)** physical

✗ **D)** logical

Explanation

Security policy and personnel controls belong to the administrative category of access control. Included in this category are policies and procedures, personnel controls, supervisory structure, security awareness training, and testing. Often, personnel controls are also thought of as operational controls.

Logical access controls are the same as technical controls. Logical access controls include encryption, network architecture, and an access control matrix.

The physical category of access control includes network segregation, perimeter security, computer controls, work area separation, data backups, and cabling.

The technical category of access control includes system access, network architecture, network access, encryption and protocols, and auditing. Encryption and access control are considered preventative technical controls.

There are three categories of access control: technical, administrative, and physical controls. A technical control is put into place to restrict access to systems, network architectures, control zones, auditing, and encryption and protocols. An administrative control is a control that dictates how security policies are implemented to fulfill the company's security goals. Administrative controls include policies and procedures, personnel controls, supervisory structure, security training, and testing. A physical control is implemented to secure physical access to an object, such as a building, a room, or a computer. Physical controls include badges, locks, guards, network segregation, perimeter security, computer controls, work area separation, backups, and cabling.

The three access control categories provide seven different functionalities or purposes:

- Preventative - A preventative control prevents security breaches and avoids risks.
- Detective - A detective control detects security breaches as they occur.
- Corrective - A corrective control restores control and attempts to correct any damage that was inflicted during a security breach.
- Deterrent - A deterrent control deters potentials violations.
- Recovery - A recovery control restores resources.
- Compensative - A compensative control provides an alternative control if another control may be too expensive. All controls are generally considered compensative.
- Directive - A directive control provides mandatory controls based on regulations or environmental requirements.

Each category of control includes controls that perform many functions. For example, a fence is both a deterrent physical control and a compensative physical control. Monitoring and supervising is both a detective administrative control and a compensative administrative control.

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply risk management concepts

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Administrative

---

Question #78 of 137

Question ID: 1104887

Your company has recently announced a partnership with a third party. This third-party organization needs access to several file servers owned by your organization. You need to ensure that the third party is able to access the appropriate resources. What should you do FIRST?

✗ **A)** Provide minimal access for third-party users to the appropriate resources.
✓ **B)** Conduct a risk assessment for the third-party organization.
✗ **C)** Establish a written IT security policy for the relationship.
✗ **D)** Monitor third-party user access to the resources.

Explanation

Before granting access to any resources, you should conduct a risk assessment for the third-party organization. This risk assessment may include a visit to the third-party organization's location. You should assess physical and network security and access and administrative controls.

You should establish a written IT security policy for the relationship only AFTER the risk assessment has been completed.

You should provide minimal access for third-party users to the appropriate resources AFTER the written security policy for the relationship is established.

You should monitor third-party user access to the resources AFTER the access has been allowed. If possible, you should restrict third-party user access to specific days/times.

Objective:
Security and Risk Management

Sub-Objective:
Apply risk-based management concepts to the supply chain

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Third-party Assessment and Monitoring

The dangers of granting system access to a third-party provider, http://searchsecurity.techtarget.com/tip/The-dangers-of-granting-system-access-to-a-third-party-provider

---

Question #79 of 137

Question ID: 1104786

Which of the following was developed to meet information resource management requirements for the federal government?

- ✗ **A)** the Gramm-Leach-Bliley Act (GLBA) of 1999
- ✗ **B)** the Health Insurance Portability and Accountability Act (HIPAA)
- ✗ **C)** the Sarbanes-Oxley (SOX) Act
- ✓ **D)** OMB Circular A-130

Explanation

OMB Circular A-130 was developed to meet information resource management requirements for the federal government. According to this circular, independent audits should be performed every three years.

The Sarbanes-Oxley Act (SOX) was developed to ensure that financial information on publicly traded companies is accurate.

The Health Insurance Portability and Accountability Act (HIPAA) was developed to establish national standards for the storage, use, and transmission of health care data.

The Gramm-Leach-Bliley Act (GLBA) of 1999 was developed to ensure that financial institutions protect customer information and provide customers with a privacy notice.

Objective:
Security and Risk Management

Sub-Objective:
Understand legal and regulatory issues that pertain to information security in a global

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Information Technology Infrastructure Library (ITIL)

OMB Circular A-130, http://clinton1.nara.gov/White_House/EOP/OMB/html/omb-a130.html

---

Question #80 of 137

Question ID: 1111660

Which statement is true of the 1991 U.S. Federal Sentencing Guidelines?

✗ **A)** The guidelines deal with individuals acting as plaintiffs in civil lawsuits.

✗ **B)** The guidelines deal with individuals working outside the organization.

✗ **C)** The guidelines deal with individuals acting as defendants in criminal lawsuits.

✓ **D)** The guidelines deal with white-collar crimes that take place within the organization.

Explanation

The 1991 U.S. Federal Sentencing Guidelines apply to the following white-collar crimes that take place within an organization:

- Antitrust
- Federal securities
- Mail and wire fraud
- Bribery
- Contracts
- Money laundering

The principles underlined in the 1991 U.S. Federal Sentencing Guidelines provide a course of action to the law enforcement agencies dealing with white-collar corporate criminals. According to the guidelines, if a company's senior management is found guilty of corporate misconduct, criminal penalties can be imposed on them. A fine of up to $290 million dollars can be imposed on the senior officials of the company for noncompliance.

The 1991 U.S. Federal Sentencing Guidelines are meant for the senior management of the company and not for individuals working outside the organization.

The 1991 U.S. Federal Sentencing Guidelines do not deal with criminal lawsuits. Criminal lawsuits are dealt with by the criminal law.

The 1991 U.S. Federal Sentencing Guidelines do not deal with civil lawsuits against individuals. Civil lawsuits are handled by a civil law referred to as tort.

Objective:
Security and Risk Management

Sub-Objective:
Understand legal and regulatory issues that pertain to information security in a global

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, 1991 U.S. Federal Sentencing Guidelines

Federal Sentencing Guidelines, https://www.ussc.gov/guidelines/archive/1991-federal-sentencing-guidelines-manual

Question #81 of 137

Question ID: 1104877

Which control provides continuous management of hardware, software, and information assets?

✗ **A)** a system control

✗ **B)** an environmental control

✓ **C)** an operational control

✗ **D)** a physical control

Explanation

An operational control includes control over hardware, software, and information assets to provide a certain level of security. Operational controls include administrative management, accountability, management of security operations, change management, and adherence to the product evaluation criteria and standards. Examples of operational controls include control over access to all program libraries, version control and testing, and documentation and approval of hardware and software before they are deployed in a production environment.

System controls restrict the execution of certain types of instructions that can only be executed when an operating system is running in the supervisor mode. System controls are built into the operating system architecture and are executed in the form of operating system instructions.

Physical controls monitor the physical security aspects of a facility infrastructure and include perimeter security, fencing, guards, gates, locks, lighting, alarms, closed-circuit televisions (CCTVs), and intrusion detection systems. Physical security controls work in conjunction with operation security to achieve the security objectives of an organization.

Environmental controls include countermeasures against physical security threats, fire, flood, static electricity, humidity, and man-made disasters.

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply risk management concepts

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Risk Management Concepts

Question #82 of 137

Question ID: 1104858

You have implemented several software controls in your organization. Which category of access controls have you implemented?

- ✗ **A)** physical controls
- ✗ **B)** administrative controls
- ✗ **C)** preventative controls
- ✓ **D)** technical controls

Explanation

Software controls are technical controls. Technical controls include software-based tools that restrict access to objects. Software controls include employing anti-virus management and tools, implementing a formal application upgrade process, and routinely testing the backup data for accuracy.

Administrative tools are policies and procedures that are developed by management to ensure that the organization is secure.

Physical controls work with technical controls and administrative controls to actually implement the actual security mechanisms.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender y aplicar los conceptos de gestión de riesgos

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 1: Seguridad y Gestión de Riesgos, Lógico (Técnico)

Pregunta #83 de 137

Id. de pregunta: 1111641

Está realizando planos de identificación de activos y control de cambios. ¿En qué fase del ciclo de vida de la gestión de la seguridad está participando?

- ✗ **A)** Operar y mantener
- ✓ **B)** instrumento
- ✗ **C)** Supervisar y evaluar

✗ **D)** Planificar y organizar

explicación

Está involucrado en la fase de implementación del ciclo de vida de administración de seguridad. Esta fase incluye los siguientes componentes:

- Asignar roles y responsabilidades.
- Desarrolle e implemente políticas, procedimientos, estándares, líneas de base y directrices de seguridad.
- Identificar datos confidenciales.
- Implemente los siguientes blueprints:
- Identificación y gestión de activos
- gestión de riesgos
- Gestión de vulnerabilidades
- conformidad
- Administración de identidades y control de acceso
- Control de cambios
- Ciclo de vida del desarrollo de software
- Planificación de la continuidad del negocio
- Sensibilización y formación
- Seguridad física
- Respuesta a incidentes
- Implementar soluciones.
- Desarrollar soluciones de auditoría y monitorización.
- Establezca objetivos, acuerdos de nivel de servicio (SLA) y métricas.

La implementación de planos de identificación de activos y control de cambios no forma parte de ninguna de las otras fases.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
evaluar y aplicar los principios de gobierno de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y gestión de riesgos, Ciclo de vida del programa de seguridad

---

Pregunta #84 de 137

Id. de pregunta: 1111639

¿Qué marco de seguridad actúa como modelo para el gobierno de TI y se centra más en los objetivos operativos?

✓ **A)** CobiT

✗ **B)** COSO

✗ **C)** BS7799

✗ **D)** ISO 17799

explicación

Los Objetivos de control para la tecnología de la información y las tecnologías relacionadas (CobiT) es un marco de seguridad que actúa como modelo para el gobierno de TI y se centra más en los objetivos operativos.

El Comité de Organizaciones Patrocinadoras de la Comisión Treadway (COSO) es un marco de seguridad que actúa como modelo para el gobierno corporativo y se centra más en los objetivos estratégicos. El marco COSO se compone de los siguientes componentes:

- Entorno de control
- evaluación de riesgos
- Actividades de control
- Información y Comunicación
- monitorización

La Organización Internacional de Normalización (ISO) 17799 es una norma que proporciona recomendaciones sobre la seguridad empresarial. Los dominios cubiertos por iso 17799 son los siguientes:

- Directiva de seguridad de la información para la organización
- Creación de infraestructura de seguridad de la información
- Clasificación y control de activos
- Seguridad del personal
- Seguridad física y ambiental
- Gestión de comunicaciones y operaciones
- control de acceso
- Desarrollo y mantenimiento de sistemas
- Gestión de la continuidad del negocio
- conformidad

Este estándar muestra los marcos de seguridad, como CobiT y COSO, cómo lograr realmente los objetivos de seguridad a través de las mejores prácticas.

La norma británica 7799 (BS7799) es la norma en la que se basa la norma ISO 17799.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
evaluar y aplicar los principios de gobierno de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Objetivos de Control para tecnologías de la información y relacionadas (CobiT)

Pregunta #85 de 137

Id. de pregunta: 1192918

¿Qué control se utiliza mejor para identificar a los usuarios autorizados involucrados en actividades no autorizadas?

- ✓ **A)** control detectivesco
- ✗ **B)** control físico
- ✗ **C)** control de medios
- ✗ **D)** control preventivo

explicación

Los controles detectives, como las pistas de auditoría, identifican y detectan no solo a los usuarios no autorizados, sino también a los usuarios autorizados involucrados en actividades y transacciones no autorizadas. Las pistas de auditoría alcanzan los objetivos de seguridad definidos por la política de seguridad y garantizan la responsabilidad de los usuarios. Los controles detectives proporcionan información detallada sobre el sistema y el uso de recursos de usuario y las actividades del usuario. En caso de intrusión, las pistas de auditoría pueden resultar útiles al detectar el origen de un ataque. Por lo tanto, es necesario asegurarse de que no se realiza ninguna modificación o eliminación no autorizada en las entradas del registro de auditoría.

Los controles de medios garantizan que la confidencialidad, integridad y disponibilidad de los datos almacenados en los medios de almacenamiento se cumplan correctamente y no se vean comprometidas. Los controles de medios definen los controles adecuados para el etiquetado, la manipulación, el almacenamiento y la eliminación de medios de almacenamiento.

Los controles de seguridad física protegen la seguridad física de la infraestructura de la instalación de las amenazas de seguridad física. Los controles físicos incluyen cercas, puertas, cerraduras e iluminación. Los controles físicos trabajan en conjunto con la seguridad de las operaciones para lograr los objetivos de seguridad de la organización.

Los controles preventivos evitan que se produzcan resultados indeseables. Cifrado, software antivirus, contraseñas, vallas, puertas, cerraduras e iluminación, son ejemplos de controles preventivos.

La auditoría incluye los siguientes eventos:

Eventos de nivel de sistema:

- Id. de inicio de sesión
- Intentos de inicio de sesión
- Función realizada
- Rendimiento del sistema
- Bloqueos de terminales de usuario

Eventos de nivel de aplicación:

- Generación de mensajes de error
- Violación de la seguridad
- Acceso de archivos y carpetas
- Modificación de archivos y carpetas

Eventos de nivel de usuario:

- Comandos ejecutados
- Intentos de autenticación
- Servicio y recursos a los que se accede
- Duración de la actividad

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender y aplicar los conceptos de gestión de riesgos

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 1: Detective de Seguridad y Gestión de Riesgos

---

Pregunta #86 de 137

Id. de pregunta: 1104890

Se le ha pedido que diseñe e implemente un programa de concienciación de seguridad para su organización. ¿Qué opción NO es un objetivo de este programa?

✓ **A)** Para garantizar que no se infringe la directiva de seguridad
✗ **B)** para promover un uso y un comportamiento aceptables
✗ **C)** Para comunicar las ramificaciones de infringir la directiva de seguridad
✗ **D)** Para exigir el cumplimiento del programa de seguridad de la información

explicación

Un programa de reconocimiento de seguridad NO garantiza la no infracción de la directiva de seguridad.

Un programa de concienciación de seguridad promueve el uso y el comportamiento aceptables, impone el cumplimiento del programa de seguridad de la información y comunica las ramificaciones de infringir la directiva de seguridad.

El objetivo principal de la capacitación en materia de seguridad es concienciar a los empleados de sus responsabilidades de seguridad y de la conducta ética esperada y las actividades aceptables. El usuario debe comprender las actividades aceptables e inaceptables y la implicación de violar la política de seguridad. Un programa de concienciación sobre la seguridad se centra en el cumplimiento y el uso aceptable de los recursos y la conducta ética en la organización. Los usuarios pueden ser penalizados a través de acciones disciplinarias o despedidos por incumplimiento de la política de seguridad.

La implementación de la política de seguridad debe supervisarse de forma rutinaria para rastrear las infracciones de la política de seguridad y los intentos de infracción para garantizar que el personal adecuado pueda ser considerado responsable.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Establecer y mantener un programa de concienciación, educación y capacitación en materia de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y gestión de riesgos Educación, formación y sensibilización en materia de seguridad

---

Pregunta #87 de 137

Id. de pregunta: 1111671

Haga coincidir cada tipo de control de acceso con el ejemplo que mejor se ajuste a ese tipo.

{UCMS id=5711947716624384 type=Activity}

explicación

Los tipos de control de acceso deben coincidir con los ejemplos de la manera siguiente:

- Técnico - protocolos de cifrado
- Administrativo : directivas de seguridad
- Físico - cerraduras

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender y aplicar los conceptos de gestión de riesgos

Referencias:

Cissp Cert Guide (3ª edición), Capítulo 1: Seguridad y gestión de riesgos, conceptos de gestión de riesgos

---

Pregunta #88 de 137

Id. de pregunta: 1111683

El equipo de continuidad del negocio ha determinado que se debe implementar una zona desmilitarizada (DMZ) para garantizar que los usuarios públicos solo accedan a ciertos servidores. ¿Qué paso del proceso de continuidad del negocio está completando el equipo?

✗ **A)** Desarrollar estrategias de recuperación.
✗ **B)** Desarrollar el plan de contingencia.
✓ **C)** Identificar controles preventivos.
✗ **D)** Desarrollar la declaración de política de planificación de continuidad.

explicación

El equipo está identificando controles preventivos. Durante este paso, el equipo mitiga el riesgo mediante la identificación de controles preventivos, como una DMZ o un firewall.

No se está completando ninguno de los otros pasos.

Los pasos de la continuidad del negocio son los siguientes:

- Desarrollar la declaración de política de planificación de continuidad.
- Llevar a cabo la BIA.
- Identificar controles preventivos.
- Desarrollar estrategias de recuperación.
- Desarrollar el plan de contingencia.
- Pruebe el plan y realice entrenamientos y ejercicios.
- Mantener el plan.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender y aplicar los conceptos de gestión de riesgos

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 1: Seguridad y Gestión de Riesgos, Preventiva

---

Pregunta #89 de 137

Id. de pregunta: 1104810

Trabajas para una compañía farmacéutica. El departamento de investigación de su empresa ha creado recientemente una fórmula química para un nuevo medicamento. Desea asegurarse de que esta fórmula permanece secreta a perpetuidad. ¿Qué término de la ley de propiedad se aplica en este caso?

- ✓ **A)** secreto comercial
- ✗ **B)** patente
- ✗ **C)** derechos de autor
- ✗ **D)** marca

explicación

A trade secret is something a company owns, such as a formula or device, which is vital for its survival in the competitive market. A chemical formula for a new drug is a trade secret. A trade secret secures and maintains the confidentiality of proprietary technical or business-related information that is adequately protected from disclosure by the owner.

A copyright protects resources to control how the resource is distributed, reproduced, displayed, and adapted. Usually, a copyright covers pictures, graphics, written works, videos, and audio recordings. A copyright protects an expression or idea.

A trademark protects a word, symbol, or some other form of identification used in the sale or advertising of services to identify the services of one person and distinguish them from the services of others. Trademarks generally represent a company to the world.

A patent only lasts for 20 years and becomes public domain after that. Keeping the formula a trade secret ensures that the public does not have access to the formula in 20 years.

Objective:
Security and Risk Management

Sub-Objective:
Understand legal and regulatory issues that pertain to information security in a global

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Trade Secret

---

Pregunta #90 de 137

Id. de pregunta: 1192895

¿Por qué objetivos de seguridad deben ser responsables los propietarios de sistemas y los propietarios de datos?

- ✗ **A)** confidencialidad y disponibilidad
- ✗ **B)** confidencialidad
- ✗ **C)** confidencialidad e integridad
- ✓ **D)** disponibilidad, integridad y confidencialidad
- ✗ **E)** integridad
- ✗ **F)** disponibilidad
- ✗ **G)** integridad y disponibilidad

explicación

Los propietarios del sistema y de los datos son responsables de garantizar que se establezcan los controles adecuados para mantener la integridad, la confidencialidad y la disponibilidad de la información.

El propietario del sistema es responsable de mantener y proteger uno o más sistemas de procesamiento de datos. El rol de propietario de un sistema incluye la integración de las características de seguridad necesarias en las aplicaciones y la decisión de compra de las aplicaciones. El propietario del sistema también garantiza que el control de acceso remoto, la administración de contraseñas y la configuración del sistema operativo proporcionen la seguridad necesaria.

El propietario de los datos suele formar parte de la administración. El propietario de los datos controla el proceso de definición de los niveles de servicio de TI, proporciona información durante la revisión de los controles y es responsable de autorizar la aplicación de controles de seguridad para proteger los activos de información de la organización. Por ejemplo, un gerente de unidad de negocio tiene la responsabilidad principal de proteger los activos de información mediante el ejercicio de la debida diligencia y las prácticas de debido cuidado.

Confidencialidad, integridad y disponibilidad son los tres objetivos de seguridad considerados como fundamentales para la protección de los activos de información de una organización. Estos tres objetivos también se conocen como la tríada de la CIA.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
evaluar y aplicar los principios de gobierno de seguridad

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 1: Seguridad y Gestión de Riesgos, DataOwner

---

Pregunta #91 de 137

Id. de pregunta: 1104838

¿Qué afirmación es cierta de una instalación de procesamiento de información?

- ✗ **A)** Un análisis de ruta crítica no tiene que incluir una ruta redundante para cada ruta crítica.
- ✗ **B)** Las áreas críticas deben iluminarse a seis pies de altura.
- ✗ **C)** Las ventanas deben estar blindadas por barras metálicas.
- ✓ **D)** Las puertas y las paredes deben tener la misma calificación de incendio.

explicación

Las puertas y paredes de una instalación de procesamiento de información deben tener la misma calificación de incendio, de conformidad con los códigos y regulaciones de seguridad. Los extintores de incendios deben mantenerse en lugares conocidos de la instalación de información. Las puertas deben resistir la entrada forzada para evitar robos o accesos a sistemas informáticos.

Para evitar atrapar a las personas durante incendios e inundaciones, las ventanas no deben estar protegidas con barras metálicas.

Según el Instituto Nacional de Estándares y Tecnología (NIST), las áreas críticas deben iluminarse a una altura de ocho pies de altura y con dos velas de intensidad.

Un análisis de ruta crítica puede determinar el nivel de protección de un entorno realizando un seguimiento de los componentes ambientales, su interacción e interdependencias. Un análisis de paths críticos incluye un path redundante para cada path crítico para garantizar un funcionamiento ininterrumpido del negocio para la organización.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Identificar, analizar y priorizar los requerimientos de Continuidad del Negocio (BC, Business Continuity)

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Incendios

Pregunta #92 de 137

Id. de pregunta: 1113895

¿Qué rol de negocio debe garantizar que todas las operaciones se ajusten a los objetivos de negocio?

✗ **A)** titular de los datos

✗ **B)** custodio de datos

✗ **C)** propietario del sistema

✓ **D)** propietario de negocio/misión

explicación

La persona en el rol de propietario de negocio/misión debe asegurarse de que todas las operaciones se ajusten a los objetivos del negocio o de la misión.

Los propietarios del sistema y de los datos son responsables de garantizar que se establezcan los controles adecuados para mantener la integridad, confidencialidad y disponibilidad de la información.

El propietario del sistema es responsable de mantener y proteger uno o más sistemas de procesamiento de datos. El rol de propietario de un sistema incluye la integración de las características de seguridad necesarias en las aplicaciones y la decisión de compra de las aplicaciones. El propietario del sistema también garantiza que el control de acceso remoto, la administración de contraseñas y la configuración del sistema operativo proporcionen la seguridad necesaria.

El propietario de los datos suele formar parte de la administración. El propietario de los datos controla el proceso de definición de los niveles de servicio de TI, proporciona información durante la revisión de los controles y es responsable de autorizar la aplicación de controles de seguridad para proteger los activos de información de la organización. Por ejemplo, un gerente de unidad de negocio tiene la responsabilidad principal de proteger los activos de información mediante el ejercicio de la debida diligencia y las prácticas de debido cuidado.

El custodio de los datos es directamente responsable de mantener y proteger los datos. Este rol normalmente se delega en el personal del departamento de TI e incluye la implementación de la seguridad de la organización a través de la implementación y el mantenimiento de los controles de seguridad. El rol de custodio de datos también incluye las siguientes tareas:

- Mantenimiento de registros de actividad
- Verificación de la exactitud y fiabilidad de los datos
- Copia de seguridad y restauración de datos de forma regular

Objetivo:

Seguridad y gestión de riesgos

Subobsecución:

evaluar y aplicar los principios de gobierno de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Propietarios de Negocios/Misión

Propietarios de negocios, usuarios o partes interesadas,
http://www.ivtnetwork.com/sites/default/files/Staib_Eric_pres.pdf

---

Pregunta #93 de 137

Pregunta con id.: 1192900

Haga clic en cada uno de los encabezados del escenario para expandir o contraer su contenido. Debe leer todo el escenario para responder a la pregunta.

fondo

Usted es un profesional de la seguridad contratado recientemente por una empresa que cotiza en bolsa para ayudar a administrar la seguridad de la organización. La compañía tiene una oficina principal en Atlanta, GA, y sucursales en todo el sureste de los Estados Unidos. El departamento de TI tiene un pequeño personal alojado en la oficina de Atlanta.

Temas actuales

El año pasado, una tormenta invernal cerró las operaciones en la mayoría de sus oficinas. Si bien ninguna de sus instalaciones fue destruida y las operaciones normales se restauraron en 24 horas, a la administración le preocupa que no exista un plan de recuperación ante desastres. Se le ha pedido que prepare un plan para cubrir este tipo de interrupción.

Actualmente, su organización mantiene varias bases de datos grandes de contenido digital que son vitales para las operaciones de su organización. Se utilizan diferentes controles para administrar este contenido. La administración le ha pedido que implemente una solución para controlar la apertura, edición, impresión o copia de estos datos de una manera más centralizada.

En los próximos seis meses, su empresa planea mover todos los servidores y granjas de servidores a un centro de datos centralizado. El centro de datos ocupará el tercer piso de un edificio de seis pisos que actualmente está en construcción. La administración le ha pedido que se asegure de que el acceso al centro de datos esté estrictamente controlado. Durante ese mismo tiempo, es probable que su organización compre un competidor para fusionarse con su organización existente.

Recientemente, uno de los servidores de la intranet fue víctima de un ataque de denegación de servicio (DoS). El departamento de TI tardó más de 24 horas en volver a poner en funcionamiento el servidor. Durante ese tiempo, el

personal de la oficina principal no pudo acceder a la importante información sobre recursos humanos disponible en el servidor de la intranet afectado.

La semana pasada, descubrió que se utilizaron varias cuentas de usuario en un intento de piratear su red. Afortunadamente, las cuentas fueron bloqueadas debido a intentos de inicio de sesión no válidos. Revise los registros y determine que tres de las cuentas se crearon para el personal que ya no está empleado por su organización.

Después de presionar durante años, ha recibido permiso de la administración para diseñar e implementar un programa integral de concienciación de seguridad en toda la organización.

¿Cuál de los siguientes debe implementar para cumplir con los requisitos de administración para el contenido digital?

✗ **A)** una directiva específica del problema

✓ **B)** DRM

✗ **C)** derechos de autor

✗ **D)** directiva de grupo

explicación

Debe implementar la administración de derechos digitales (DRM) para cumplir los requisitos de administración para el contenido digital. DRM controlará la apertura, edición, impresión y copia de contenido digital.

Un derecho de autor garantiza que una obra protegida por derechos de autor esté protegida de cualquier forma de reproducción o uso sin el consentimiento del titular de los derechos de autor.

Una directiva de grupo se puede usar para implementar ciertas restricciones en un servidor o red. Sin embargo, no se utiliza para limitar el acceso a los contenidos digitales.

Se puede utilizar una directiva específica para proporcionar orientación sobre la protección del contenido digital. Sin embargo, la política en sí no impedirá la apertura, edición, impresión y copia de contenido digital.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender los problemas legales y reglamentarios relacionados con la seguridad de la información en un entorno global

Referencias:

Gestión de derechos digitales, http://searchcio.techtarget.com/definition/digital-rights-management

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Cuestiones Legales y Regulatorias

Pregunta #94 de 137

Id. de pregunta: 1104835

Su organización acaba de ampliar su red para incluir otro piso del edificio donde se encuentran sus oficinas. Se le ha pedido que se asegure de que el nuevo piso se incluya en el plan de continuidad del negocio. ¿Qué debes hacer?

✗ **A)** Completar una prueba de simulación.

✗ **B)** Complete una prueba de recorrido estructurada.

✓ **C)** Actualizar el plan de continuidad del negocio para incluir el nuevo piso y sus funciones.

✗ **D)** Completar una prueba paralela.

explicación

Debe actualizar el plan de continuidad del negocio para incluir el nuevo piso y sus funciones. Cuando se agregan nuevos recursos, hardware o software, solo tendrá que modificar el plan de continuidad del negocio para incluir los nuevos recursos, hardware o software. Lo más probable es que su plan ya cubra los recursos que existen en el nuevo piso. Sin embargo, el plan tendrá que incorporar el hecho de que los nuevos recursos existen.

No es necesario realizar ninguna prueba hasta que estén programadas. Actualmente, el nuevo piso no está incluido en el plan de continuidad del negocio. Por lo tanto, cualquier tipo de prueba no incluirá recursos en ese piso.

Una prueba de recorrido estructurada recorre los diferentes escenarios del plan para asegurarse de que no se deja nada fuera.

Una prueba de simulación simula un fallo real basado en un escenario para probar la reacción del personal. El propósito principal de esta prueba es asegurarse de que no se deja nada fuera.

Una prueba paralela garantiza que sistemas específicos puedan funcionar en un sitio alternativo. Los sistemas se venden en línea en el sitio alternativo y se produce un uso regular.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Identificar, analizar y priorizar los requerimientos de Continuidad del Negocio (BC, Business Continuity)

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Mantener el Plan

---

Pregunta #95 de 137

Id. de pregunta: 1104842

Ha desarrollado la directiva de seguridad de la información para su organización. ¿Qué paso debe preceder a la adopción de esta política?

✗ **A)** aplicación de las normas

✓ **B)** obtener la aprobación de la administración

✗ **C)** llevar a cabo la capacitación de conciencia de seguridad

✗ **D)** aplicación de los procedimientos

explicación

La obtención de la aprobación de la administración debe preceder a la adopción de una política de seguridad de la información. El desarrollo de la política de seguridad de la información debe ser supervisado por el gerente de operaciones comerciales de una organización.

Una directiva de seguridad define los objetivos de seguridad generales de una organización. Establece la autoridad y responsabilidad de cada individuo. También establece procedimientos para aplicar la política de seguridad. La alta dirección de una organización tiene la responsabilidad principal de la seguridad de la organización. Por lo tanto, deben determinar el nivel de protección necesario y aprobar la directiva de seguridad. Los directores de departamento también contribuyen al desarrollo de la política de seguridad de la información. El desarrollo de la directiva de seguridad de la información normalmente se encarga a un administrador de nivel medio, como el gerente de operaciones empresariales.

La implementación de estándares, procedimientos y directrices debe ocurrir después del desarrollo de una política de seguridad de la información. La directiva de seguridad define el procedimiento para configurar un programa de seguridad y sus objetivos. La administración asigna los roles y responsabilidades y define el procedimiento para aplicar la directiva de seguridad.

La formación en materia de concienciación sobre seguridad se basa en las directrices y normas definidas en la directiva de seguridad. Por lo tanto, la capacitación se lleva a cabo después de la creación y adopción de la política de seguridad. La concienciación y la formación ayudan a los usuarios a ser más responsables de sus acciones. La conciencia de seguridad mejora la conciencia de los usuarios de la necesidad de proteger los recursos de información. La educación en seguridad ayuda a la administración a desarrollar la experiencia interna para administrar los programas de seguridad.

La descripción de tecnologías específicas para la seguridad de la información no se incluye en la directiva de seguridad.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Contribuir y aplicar las políticas y procedimientos de seguridad del personal

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Documentación de Seguridad

---

Pregunta #96 de 137

Id. de pregunta: 1104850

Su organización ha desarrollado e implementado nuevas estrategias de seguridad para la red. ¿Qué debes hacer a continuación?

- ✗ **A)** Establecer el presupuesto para las nuevas estrategias de seguridad.
- ✗ **B)** Compre los recursos para las nuevas estrategias de seguridad.
- ✓ **C)** Evaluar la efectividad de las nuevas estrategias de seguridad.
- ✗ **D)** Obtenga las métricas sobre las nuevas estrategias de seguridad.

explicación

Después de desarrollar e implementar nuevas estrategias de seguridad, debe evaluar la eficacia de las nuevas estrategias de seguridad.

Debe establecer el presupuesto para las nuevas estrategias de seguridad cuando se estén desarrollando las estrategias.

Usted debe comprar los recursos para las nuevas estrategias de seguridad cuando se están implementando las estrategias.

Debe obtener las métricas de las nuevas estrategias de seguridad cuando se implementen las estrategias.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender y aplicar los conceptos de gestión de riesgos

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, NIST

Pregunta #97 de 137

Id. de pregunta: 1302569

¿Qué afirmación NO es cierta para la construcción de una instalación de procesamiento de información?

✗ **A)** Los pisos elevados necesitan ser conectado a tierra eléctricamente.

✗ **B)** Las puertas necesitan la misma calificación de incendios que las paredes circundantes.

✓ **C)** Todas las paredes deben tener una calificación mínima de incendio de una hora.

✗ **D)** Las puertas deben prohibir las entradas forzadas.

explicación

Todas las paredes de una instalación de procesamiento de información tienen diferentes clasificaciones de incendios en función del tipo que son. Mientras que las paredes internas deben tener una calificación mínima de incendio de una hora, las paredes adyacentes deben tener una calificación mínima de incendio de dos horas.

Diferentes materiales de construcción tienen diferentes calificaciones de incendio. Por lo tanto, el tipo de material de construcción que se utiliza debe cumplir con las calificaciones de incendio que dependen del uso del edificio. Las paredes, techos y pisos deben estar hechos de materiales que cumplan con las calificaciones de incendio requeridas. Las puertas deben tener la misma calificación de incendio que las paredes circundantes. Además, las puertas deben prohibir la entrada forzosa.

Los pisos elevados deben estar conectado a tierra eléctricamente porque se utilizan para ocultar y proteger los cables y cables eléctricos. Un piso elevado es una plataforma con paneles desmontables donde se instala el equipo que se encuentra en el pavimento con espacio entre el mismo y el cableado de la vivienda de la planta principal del edificio. A menudo se utiliza un piso elevado para suministrar aire acondicionado al equipo de procesamiento de datos y a la habitación. La ventilación del suelo, al igual que con toda la ventilación de la sala de computadoras, no debe ventilarse a ninguna otra oficina o área. Los conductos de aire HVAC que sirven a otras habitaciones no deben pasar a través de la sala de computadoras a menos que se proporcione un sistema de amortiguación automático.

El suelo elevado, también llamado falso suelo o piso secundario, tiene requisitos muy estrictos en cuanto a su construcción y uso. Los cables eléctricos deben estar encerrados en un conducto de metal, y los cables de datos deben estar encerrados en caminos de rodadura con todos los cables no utilizados eliminados. Las aberturas en el piso elevado deben ser lisas, nobrasivas y protegidas contra la entrada de escombros u otros combustibles. Obviamente, el suelo elevado y la cubierta deben construirse con materiales no combustiónbles.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Identificar, analizar y priorizar los requerimientos de Continuidad del Negocio (BC, Business Continuity)

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Incendios

Pregunta #98 de 137

Id. de pregunta: 1111692

Como parte de una nueva iniciativa de seguridad, su organización ha decidido que todos los empleados deben recibir formación sobre seguridad. ¿Cuál es el objetivo de esta formación?

✗ **A)** Todos los empleados del departamento de TI deben ser capaces de manejar los ataques de ingeniería social.

✓ **B)** Todos los empleados deben entender sus responsabilidades de seguridad.

✗ **C)** Todos los empleados del departamento de TI deben ser capaces de manejar incidentes de seguridad.

✗ **D)** Todos los empleados, excluyendo a la alta dirección, deben entender las implicaciones legales de la pérdida de información.

explicación

El objetivo principal de la capacitación en conciencia de seguridad es garantizar que todos los empleados entiendan sus responsabilidades de seguridad, la conducta ética que se espera de ellos y el uso aceptable de un programa de seguridad efectivo. Un programa de seguridad eficaz incluye una mezcla de métodos técnicos y no técnicos. Es importante entender la cultura corporativa y su efecto en la seguridad de la organización. Un programa de concienciación sobre la seguridad se trata de comunicar la actitud de la empresa sobre la protección de los recursos. Un ejemplo de una forma rentable de mejorar la conciencia de seguridad en una organización es crear un programa de premios o reconocimiento para los empleados.

Las responsabilidades de los usuarios para la protección de los activos de información se definen en las políticas, procedimientos, estándares y mejores prácticas de seguridad de la información de la organización desarrollados para la protección de la información.

La capacitación en conciencia de seguridad se puede personalizar para diferentes grupos de empleados, como la alta gerencia, el personal técnico y los usuarios. Cada grupo tiene diferentes responsabilidades y necesitan entender la seguridad desde una perspectiva relacionada con su dominio. Por ejemplo, la capacitación en materia de seguridad para el grupo de administración debe centrarse en una comprensión clara de los riesgos potenciales, la exposición y las obligaciones legales resultantes de la pérdida de información. El personal técnico debe estar bien versado en cuanto a los procedimientos, normas y directrices que deben seguirse. La capacitación de los usuarios debe incluir ejemplos de actividades aceptables e inaceptables y el peligro de incumplimiento. La capacitación de los usuarios puede centrarse en amenazas, como la ingeniería social, que puede conducir a la divulgación de información confidencial que puede obstaculizar las operaciones comerciales al comprometer la confidencialidad y la integridad de los activos de información. En particular, se debe tener conocimiento de esos ataques a los funcionarios para evitar intentos de acceso no autorizado.

Antes de desarrollar la formación en concienciación sobre seguridad, es importante que el entorno corporativo se entienda completamente.

La formación en concienciación sobre seguridad incluye las siguientes ventajas:

- Ayuda a los operadores a comprender el valor de la información.
- Puede ayudar a los administradores de sistemas a reconocer los intentos de intrusión no autorizados.
- Puede ayudar a una organización a reducir el número y la gravedad de los errores y omisiones.

La conciencia de seguridad, la capacitación en seguridad y la educación en seguridad generalmente se consideran tres temas únicos. La conciencia de seguridad se utiliza para reforzar el hecho de que la seguridad apoya la misión de la organización mediante la protección de recursos valiosos. El propósito de la capacitación es enseñar a las personas las habilidades que les permitirán realizar su trabajo de manera más segura. La capacitación se centra en la conciencia de seguridad.

La educación en seguridad es más profunda que la capacitación en seguridad y está dirigida a los profesionales de la seguridad y a aquellos cuyos trabajos requieren experiencia en seguridad. El compromiso de la gerencia es necesario debido a los recursos utilizados en el desarrollo e implementación del programa y también porque el programa afecta a su personal.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Establecer y mantener un programa de concienciación, educación y capacitación en materia de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y gestión de riesgos Educación, formación y sensibilización en materia de seguridad

---

Pregunta #99 de 137

Id. de pregunta: 1104817

¿Qué organización ha elaborado una declaración relacionada con la ética relativa al uso de Internet?

- ✓ **A)** Iab
- ✗ **B)** IEEE
- ✗ **C)** ICANN
- ✗ **D)** Ietf

explicación

La Junta de Arquitectura de Internet (IAB) ha elaborado una declaración relacionada con la ética relativa al uso de Internet. Como parte de esta declaración, la IAB afirma que el uso de Internet es un privilegio, no un derecho. El

comportamiento poco ético incluye buscar deliberadamente obtener acceso no autorizado, interrumpir el uso de Internet, desperdiciar recursos deliberadamente, destruir la integridad de la información basada en computadoras y comprometer la privacidad de otra persona.

El Grupo de Trabajo de Ingeniería de Internet (IETF) es un comité supervisado por IAB. El objetivo del IETF es mejorar Internet. Se adhiere a la misma ética que el IAB, pero el IETF no tiene su propia declaración de ética.

El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) desarrolla estándares para nuevas tecnologías, incluyendo la inalámbrica.

La Corporación de Internet para la Asignación de Nombres y Números (ICANN) es la organización responsable de la asignación de direcciones IP y la gestión de DNS.

Otra organización que debe comprender es el Instituto Nacional de Estándares y Tecnología (NIST), que es un laboratorio de estándares de medición que forma parte del Departamento de Comercio de los Estados Unidos. Esta organización desarrolla metodologías de gestión de riesgos. El NIST ha identificado varias técnicas de autoprueba aceptadas: mapeo de red, escaneo de vulnerabilidades, pruebas de penetración, descifrado de contraseñas, revisión de registros, detección de virus y marcación de guerra.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender, adherirse y promover la ética profesional

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Internet Architecture Board (IAB)

Pregunta #100 de 137

Id. de pregunta: 1104758

¿Qué término se utiliza para describir la fiabilidad y accesibilidad de una red y sus recursos?

- ✗ **A)** autenticación de red
- ✗ **B)** confidencialidad de la red
- ✗ **C)** integridad de la red
- ✓ **D)** disponibilidad de la red

explicación

El término disponibilidad de red describe la fiabilidad y accesibilidad de una red y sus recursos.

La integridad de la red garantiza que una red y sus recursos estén seguros de cambios malintencionados o accidentales. La confidencialidad de la red garantiza que una red y sus recursos no se divulguen a sujetos no autorizados. La autenticación de red comprueba la identidad de un sujeto antes de conceder al sujeto acceso a la red.

La disponibilidad de la red afecta directamente al dominio telecomunicaciones y seguridad de la red. El dominio telecomunicaciones y seguridad de redes se ocupa de las estructuras, los métodos de transmisión, los formatos de transporte y las medidas de seguridad utilizadas para proporcionar integridad, disponibilidad, autenticación y confidencialidad a través de redes públicas y privadas.

La mayoría de los tiempos de inactividad no planificados se deben a un error de hardware.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender y aplicar los conceptos de confidencialidad, integridad y disponibilidad

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 1: Seguridad y Gestión de Riesgos, Disponibilidad

---

Pregunta #101 de 137

Id. de pregunta: 1104792

Usted es el analista de seguridad de una institución financiera de los Estados Unidos que cotiza en bolsa. Todas las siguientes leyes afectan a su organización, EXCEPTO:

✗ **A)** Basilea II
✗ **B)** GLBA
✓ **C)** HIPAA
✗ **D)** Sox

explicación

La Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA, por susta en bolsa) no afecta a una institución financiera que cotiza en bolsa. Todas las demás leyes afectarán a la institución financiera.

La Ley Sarbanes-Oxley (SOX) de 2002 fue escrita para evitar que las empresas cometan fraude al proporcionar a sabiendas informes financieros inexactos a los accionistas y al público. Se ocupa principalmente de las prácticas contables corporativas. El artículo 404 de esta ley se refiere específicamente a la tecnología de la información.

La Ley Gramm-Leach-Bliley (GLBA) de 1999 fue escrita para garantizar que las instituciones financieras desarrollen avisos de privacidad y permitan a sus clientes evitar que las instituciones financieras compartan información con

terceros.

La Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA, por sus contra, por sus, se redactó para evitar que las organizaciones médicas (incluidas las compañías de seguros de salud, los hospitales y los consultorios médicos) compartan información sobre la atención médica de los pacientes sin consentimiento. Se ocupa principalmente de la seguridad, integridad y privacidad de la información del paciente.

El Acuerdo de Basilea II se basa en tres pilares principales: requisitos mínimos de capital, supervisión y disciplina de mercado. Estos pilares se aplican a las instituciones financieras.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender los problemas legales y reglamentarios relacionados con la seguridad de la información en un entorno global

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Portabilidad de Seguros De Salud y Ley de Responsabilidad (HIPAA)

Pregunta #102 de 137

Id. de pregunta: 1111643

¿Qué término indica que una empresa ha tomado medidas razonables para proteger su información confidencial y sus empleados?

- ✗ **A)** la debida responsabilidad
- ✗ **B)** Debida diligencia
- ✓ **C)** atención debida
- ✗ **D)** obligación debida

explicación

El debido cuidado implica que una empresa asume la responsabilidad de las acciones que tienen lugar dentro de la organización mediante la adopción de medidas razonables para prevenir las brechas de seguridad y para proteger los activos de información y los empleados. El debido cuidado también garantiza el daño mínimo y la pérdida de información y de individuos en caso de una intrusión porque las contramedidas ya están en su lugar. El debido cuidado es el esfuerzo continuo de asegurarse de que las políticas, procedimientos y estándares correctos estén en su lugar y se sigan. La debida atención se determina en función de los requisitos legislativos. El debido cuidado no está dirigido a aumentar los beneficios de una empresa. La empresa ejerce la práctica del debido cuidado de la siguiente manera:

- La empresa implementa controles de acceso físicos y lógicos.
- La compañía garantiza la seguridad de las telecomunicaciones mediante el uso de la autenticación y el cifrado.
- Las copias de seguridad de la información, las aplicaciones y el hardware se realizan a intervalos regulares.
- Los planes de recuperación ante desastres y continuidad del negocio están en marcha dentro de la empresa.
- La empresa realiza revisiones periódicas, simulacros y pruebas para probar y mejorar los planes de recuperación ante desastres y continuidad del negocio.
- Los empleados de la compañía son informados sobre el comportamiento anticipado y las implicaciones de no seguir los estándares esperados.
- La empresa tiene políticas de seguridad, estándares, procedimientos y directrices para una gestión eficaz de la seguridad.
- La compañía realiza capacitación en conciencia de seguridad para sus empleados.
- La red de la empresa ejecuta definiciones de antivirus actualizadas en todo momento.
- El administrador realiza periódicamente pruebas de penetración desde fuera y dentro de la red.
- La compañía implementa una función de devolución de llamada o de marcado preestablecido en aplicaciones de acceso remoto.
- La empresa cumple y actualiza los acuerdos de nivel de servicio (SLA) externos.
- La compañía se asegura de que se cumplan las responsabilidades de seguridad aguas abajo.
- La compañía implementa contramedidas que aseguran que la piratería de software no está teniendo lugar dentro de la compañía.
- La empresa se asegura de que se está llevando a cabo una auditoría y revisión adecuadas de los registros de auditoría.
- La compañía lleva a cabo verificaciones de antecedentes de los empleados potenciales.

El fracaso de una empresa para lograr los estándares mínimos anteriores se considera negligencia de acuerdo con los estándares de atención debida. Si una empresa no ejerce el debido cuidado, la alta dirección de la empresa puede ser considerada legalmente responsable de la negligencia y podría tener que pagar daños y perjuicios en virtud del principio de negligencia culpable de la legislación por la pérdida sufrida debido a controles de seguridad insuficientes.

La debida diligencia es realizada por la compañía antes de que se establezcan los estándares para el debido cuidado. La debida diligencia implica que la empresa investiga y determina las posibles vulnerabilidades y riesgos asociados con los activos de información y la red de empleados de la empresa.

La obligación debida y la debida responsabilidad no son utilizadas por una empresa para garantizar medidas razonables para proteger los activos de información.

Los ejemplos de ejercicio del debido cuidado o la diligencia debida incluyen la implementación de programas de capacitación y concientización sobre seguridad, la implementación de declaraciones de cumplimiento de los empleados y la implementación de controles en la documentación impresa.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
evaluar y aplicar los principios de gobierno de seguridad

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 1: Seguridad y Gestión de Riesgos, Due Care y Due Diligence

---

Pregunta #103 de 137

Id. de pregunta: 1104891

A medida que diseña la capacitación de reconocimiento de seguridad, enumera los diferentes grupos que requieren capacitación diferente. ¿Qué grupo debe recibir capacitación en seguridad que sea parte educación y parte marketing?

- ✓ **A)** Ejecutivos
- ✗ **B)** Desarrolladores
- ✗ **C)** Administradores
- ✗ **D)** Empleados

explicación

Los ejecutivos de la empresa deben recibir capacitación en seguridad que sea parte educación y parte marketing. El componente educativo debe diseñarse para dar a los ejecutivos una visión general de los riesgos y requisitos de seguridad de la red. El componente de marketing debe incluir información que convenza a los ejecutivos de la necesidad de fuertes medidas de seguridad en una red informática. Sin el apoyo de los ejecutivos de la empresa, una empresa normalmente no puede montar una defensa de seguridad de red eficaz.

Los administradores requieren actualizaciones de seguridad frecuentes para poder configurar una red de forma segura. Los desarrolladores requieren formación en seguridad para asegurarse de que programan de una manera que mantenga o mejore la seguridad de la red. Los empleados requieren capacitación general en seguridad de red en temas como ingeniería social, creación de credenciales de red y directiva de seguridad de la empresa.

Las técnicas de ingeniería social incluyen piggybacking, suplantación de personalización y hablar.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Establecer y mantener un programa de concienciación, educación y capacitación en materia de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Niveles Requeridos

---

Pregunta #104 de 137

Id. de pregunta: 1104811

¿Qué afirmación es cierta en cuanto a la responsabilidad derivada?

✗ **A)** Se refiere a la responsabilidad de la organización de mantener la privacidad de la información de los empleados.

✗ **B)** Pertenece a una sola organización.

✓ **C)** Garantiza que las organizaciones que trabajan juntas bajo un contrato son responsables de su gestión de la seguridad de la información.

✗ **D)** Es un término utilizado para representar los pasivos contractuales de las operaciones comerciales.

explicación

La responsabilidad posterior garantiza que las organizaciones que trabajan juntas en virtud de un contrato sean responsables de la gestión de la seguridad de la información y de los controles de seguridad desplegados. Las empresas podrían firmar contratos para trabajar juntas de manera integrada. Un ejemplo de este tipo de contrato es la extranet. En este contrato, cada empresa debe aplicar el concepto de debido cuidado y diligencia debida e implementar contramedidas para proteger los activos de información. La responsabilidad aguas abajo garantiza que cada empresa proporcione su parte de seguridad y es responsable de cualquier negligencia causada debido a la falta de controles de seguridad en su infraestructura.

La responsabilidad derivada se refiere a varias organizaciones que trabajan bajo un contrato y no se limita a una sola organización.

La responsabilidad posterior se refiere a las obligaciones legales o comerciales y no a las obligaciones contractuales de las operaciones comerciales. La responsabilidad posterior implica a una empresa y a los socios comerciales de la empresa.

La responsabilidad posterior se refiere a las obligaciones legales de los requisitos de seguridad y no se ocupa de la privacidad de la información de los empleados.

Las diversas tecnologías de las empresas vinculadas por el contrato deben ser interoperables para mantener la armonía en las operaciones comerciales. Se debe realizar una auditoría periódica para confirmar que las empresas no son negligentes con sus acciones y con sus respectivas preocupaciones de seguridad.

Por ejemplo, debido a la falta de administración de la seguridad de la información en una empresa, la red de un socio de canal está infectada con un ataque de gusano. Si el ataque de gusano afecta negativamente la funcionalidad de la empresa asociada, entonces los socios pueden demandar a la empresa principal por motivos de negligencia. Por lo tanto, la responsabilidad derivada es aplicable en tal situación.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender los problemas legales y reglamentarios relacionados con la seguridad de la información en un entorno global

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Derecho Civil /Agravio

---

Pregunta #105 de 137

Id. de pregunta: 1113899

¿Qué tipo de ley se basa en normas, no en la precedencia?

- ✗ **A)** derecho consuetudinario
- ✗ **B)** common law
- ✓ **C)** derecho civil
- ✗ **D)** ley mixta

explicación

El derecho civil se basa en normas, no en la precedencia. El derecho civil se utiliza en los países europeos. Un sistema de derecho civil se centra en las leyes escritas.

El common law se compone de leyes penales, civiles y administrativas. El common law se utiliza en los Estados Unidos, Canadá, Reino Unido, Australia y Nueva Zelanda. En el common law, la culpabilidad debe probarse más allá de toda duda razonable. En los Estados Unidos, la rama judicial del gobierno es responsable de la creación del derecho consuetudinario.

El derecho consuetudinario se basa en las tradiciones y costumbres regionales. Este tipo de derecho no se utiliza en muchos países, pero se incluye principalmente en sistemas que utilizan sistemas jurídicos mixtos.

El derecho mixto está presente cuando dos o más sistemas jurídicos se utilizan conjuntamente en un país. En estos casos, un tipo de ley puede aplicarse en una situación, mientras que otro tipo de ley puede aplicarse en otra situación.

Bajo el common law, hay muchas categorías de derecho, incluyendo el derecho penal, el derecho civil y el derecho administrativo o reglamentario. En algunos países, también se consideran sistemas de derecho religioso.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:

Comprender los problemas legales y reglamentarios relacionados con la seguridad de la información en un entorno global

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Principales Sistemas Legales

---

Pregunta #106 de 137

Id. de pregunta: 1192915

Al completar el análisis de impacto empresarial, el comité descubre que una aplicación de recursos humanos se basa en los dos servidores siguientes:

- un servidor de recursos humanos administrado por el departamento de recursos humanos en San Antonio, Texas
- un servidor de base de datos administrado por el departamento de TI en San Antonio, Texas

A sugerencia del comité del plan de continuidad del negocio, la administración decide implementar servidores redundantes para ambos servidores y colocar los servidores redundantes en la sucursal en Seattle, Washington.

¿De qué son los dos nuevos servidores un ejemplo?

✗ **A)** una interdependencia

✗ **B)** un acuerdo recíproco

✗ **C)** una estrategia de copia de seguridad

✓ **D)** un control preventivo

explicación

Este es un ejemplo de un control preventivo. Durante el análisis de impacto en el negocio, el comité de continuidad del negocio determinará las amenazas para la organización. Como parte de este proceso, el comité tendrá que entender las dependencias entre los sistemas. El comité puede sugerir controles preventivos para prevenir ciertas amenazas.

Este no es un ejemplo de acuerdo recíproco. Un acuerdo recíproco se produce cuando dos organizaciones acuerdan establecer instalaciones fuera del sitio entre sí. Una desventaja de los acuerdos recíprocos es que el sitio podría no tener la capacidad para manejar las operaciones requeridas en una emergencia importante.

Esto no es una estrategia de copia de seguridad. Una estrategia de copia de seguridad se formula cuando se estipula la hora en que se producen las copias de seguridad reales y qué tipos de copias de seguridad se producen. Las estrategias de backup incluyen cintas de backup, bóveda electrónica, journaling remoto e instalaciones alternativas, incluidos sitios calientes, cálidos y fríos.

Este no es un ejemplo de interpendencia. La interdependencia se produce cuando dos funciones, departamentos o procesos dependen entre sí para la funcionalidad. Si bien la relación entre los dos servidores es una interpendencia, la

implementación de servidores redundantes es un control preventivo.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender y aplicar los conceptos de gestión de riesgos

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 1: Seguridad y Gestión de Riesgos, Preventiva

---

Pregunta #107 de 137

Id. de pregunta: 1111645

¿Qué función se delega en el personal del departamento de TI y es responsable de mantener la integridad y seguridad de los datos?

- ✗ **A)** propietario del proceso
- ✓ **B)** custodio de datos
- ✗ **C)** propietario del sistema
- ✗ **D)** titular de los datos

explicación

El custodio de los datos es directamente responsable de mantener y proteger los datos. Este rol normalmente se delega en el personal del departamento de TI e incluye la implementación de la seguridad de la organización a través de la implementación y el mantenimiento de los controles de seguridad. El rol de custodio de datos también incluye las siguientes tareas:

- Mantenimiento de registros de actividad
- Verificación de la exactitud y fiabilidad de los datos
- Copia de seguridad y restauración de datos de forma regular

El propietario de los datos suele formar parte de la administración. El propietario de los datos también controla el proceso de definición de los niveles de servicio de TI, proporciona información durante la revisión de los controles y es responsable de autorizar la aplicación de controles de seguridad para proteger los activos de información de la organización. Por ejemplo, un gerente de unidad de negocio tiene la responsabilidad principal de proteger los activos de información mediante el ejercicio de la debida diligencia y las prácticas de debido cuidado. Otro rol de clasificación de información es el usuario de datos.

El propietario del sistema es responsable de mantener y proteger uno o más sistemas de procesamiento de datos. El rol incluye principalmente la integración de las características de seguridad necesarias en las aplicaciones y una decisión de compra de las aplicaciones. El propietario del sistema también garantiza que el control de acceso remoto, la administración de contraseñas y las configuraciones del sistema operativo proporcionen la seguridad necesaria. Los propietarios de sistemas e información son responsables de garantizar que se establezcan los controles adecuados para abordar la integridad, confidencialidad y disponibilidad de los sistemas y datos de TI. Un sistema podría tener varios propietarios de información.

El propietario de un proceso es responsable de definir, mantener y supervisar los diferentes procesos que se ejecutan en una organización. Un ejemplo de un proceso puede ser aceptar y enviar un pedido a un cliente.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
evaluar y aplicar los principios de gobierno de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Custodio de Datos

---

Pregunta #108 de 137

Id. de pregunta: 1104868

¿A qué categoría de controles pertenece la auditoría y supervisión del sistema?

- ✗ **A)** control administrativo
- ✗ **B)** control físico
- ✓ **C)** control técnico
- ✗ **D)** control del sistema

explicación

La auditoría y supervisión del sistema son componentes del control técnico. La auditoría es necesaria para garantizar la responsabilidad de los usuarios. Proporciona detección si se produce un determinado evento. Un ejemplo de auditoría es una pista de auditoría de acceso al sistema que se emplea para realizar un seguimiento de todos los inicios de sesión correctos y no correctos. Una revisión oportuna de los registros de auditoría de acceso del sistema es necesaria para la seguridad de la red.

Los controles de seguridad física garantizan la seguridad física de la infraestructura de la instalación. Los controles físicos incluyen cercas, puertas, cerraduras e iluminación. Los controles físicos trabajan en conjunto con la seguridad de la operación para lograr los objetivos de seguridad de la organización.

Los controles del sistema no son una categoría reconocida de controles. Aunque una organización puede referirse a un control como un control de sistema en el que protege un sistema, los controles sólo se pueden dividir en tres categorías principales: técnico (lógico), administrativo (de gestión) y físico.

Los controles administrativos definen la directiva de seguridad, los estándares, las directrices y los procedimientos operativos estándar. Los controles administrativos también definen la estructura de supervisión y el plan de estudios de capacitación en materia de seguridad para los empleados de la organización. La rotación de funciones, la separación de funciones y las vacaciones obligatorias son controles administrativos.

La supervisión de auditoría le permite identificar cualquier cambio inusual en las actividades del usuario. La supervisión del rendimiento es para comprobar el rendimiento del sistema.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender y aplicar los conceptos de gestión de riesgos

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 1: Seguridad y Gestión de Riesgos, Técnica

---

Pregunta #109 de 137

Id. de pregunta: 1104886

Su organización ha pedido al equipo de seguridad que agregue ataques terroristas al plan de continuidad del negocio de la organización. ¿Qué tipo de amenaza representa esto?

- ✓ **A)** amenaza políticamente motivada
- ✗ **B)** amenaza hecha por el hombre
- ✗ **C)** amenaza del sistema de suministro
- ✗ **D)** amenaza ambiental natural

explicación

Un ataque terrorista es una amenaza políticamente motivada. Un ataque terrorista suele ser un ataque contra una visión de país en particular de un grupo que se opone a las opiniones políticas de ese país. A menudo, un grupo en particular se atribuye el mérito de un ataque terrorista. Las amenazas por motivos políticos incluyen huelgas, disturbios, desobediencia civil y ataques terroristas.

Las amenazas ambientales naturales incluyen inundaciones, terremotos, tornados, huracanes y temperaturas extremas.

Las amenazas del sistema de suministro incluyen cortes de energía, interrupciones de comunicaciones e interrupción de agua y gas.

Las amenazas provocadas por el hombre incluyen acceso no autorizado, explosiones, incidentes de empleados descontentos, errores de empleados, accidentes, vandalismo, fraude y robo. Si bien los ataques terroristas son causados por el hombre y, por lo tanto, podrían considerarse un ataque provocado por el hombre, con mayor frecuencia se clasifican como ataques por motivos políticos porque son planificados y llevados a cabo por organizaciones terroristas. La mayoría de los ataques hechos por el hombre son más limitados en alcance cuando se considera el perpetuador.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender y aplicar conceptos y metodologías de modelado de amenazas

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 1: Seguridad y gestión de riesgos, amenazas causadas por humanos

---

Pregunta #110 de 137

Id. de pregunta: 1192907

¿Cuál es otro término para los controles técnicos?

- ✓ **A)** controles lógicos
- ✗ **B)** controles detectivesco
- ✗ **C)** controles de acceso
- ✗ **D)** controles preventivos

explicación

Otro término para los controles técnicos es controles lógicos. Los controles técnicos se utilizan para restringir el acceso a los datos y los componentes del sistema operativo, las aplicaciones de seguridad, los dispositivos de red, los protocolos y las técnicas de cifrado.

Los controles de acceso se pueden incluir como parte de los controles técnicos. Sin embargo, controles de acceso no es un término que sea sinónimo de controles técnicos.

Los controles detectivescos son controles que se utilizan para detectar la intrusión cuando se produce. Si bien puede incluir controles técnicos de detectives en su plan de seguridad, los controles de detectives pueden ser técnicos,

físicos o administrativos. Los controles técnicos de detectives incluyen registros de auditoría y sistemas de detección de intrusiones (IDS).

Los controles preventivos son controles que se utilizan para prevenir la intrusión antes de que se produzca. Si bien puede incluir controles técnicos preventivos en su plan de seguridad, los controles preventivos pueden ser técnicos, físicos o administrativos. Los controles técnicos preventivos incluyen listas de control de acceso (ACL), enrutadores, cifrado, software antivirus, cifrado, tarjetas inteligentes y sistemas de devolución de llamada.

Los controles técnicos o lógicos incluyen todos los mecanismos de autenticación, incluidos la contraseña, los dos factores, Kerberos, la biometría, las tarjetas inteligentes y la autenticación RADIUS. La segmentación de red se logra mediante controles lógicos.

Hay tres categorías de control de acceso: controles técnicos, administrativos y físicos. Se ha establecido un control técnico para restringir el acceso. Los controles técnicos funcionan para proteger el acceso al sistema, la arquitectura y el acceso a la red, las zonas de control, la auditoría y el cifrado y los protocolos. Un administrativo se desarrolla para dictar cómo se implementan las políticas de seguridad para cumplir con los objetivos de seguridad de la empresa. Los controles administrativos incluyen políticas y procedimientos, controles de personal, estructura de supervisión, capacitación en seguridad y pruebas. Un control físico se implementa para proteger el acceso físico a un objeto, como un edificio, una sala o un equipo. Los controles físicos incluyen insignias, cerraduras, guardias, segregación de red, seguridad perimetral, controles informáticos, separación de áreas de trabajo, copias de seguridad y cableado.

Las tres categorías de control de acceso proporcionan siete funcionalidades o propósitos diferentes:

- Preventivo - Un control preventivo previene brechas de seguridad y evita riesgos.
- Detective - Un control detective detecta las brechas de seguridad a medida que ocurren.
- Correctivo : un control correctivo restaura el control e intenta corregir cualquier daño infligido durante una infracción de seguridad.
- Disuasión - Un control disuasorio disuade posibles violaciones.
- Recuperación: un control de recuperación restaura los recursos.
- Compensativo: un control compensativo proporciona un control alternativo si otro control puede ser demasiado costoso. Por lo general, todos los controles se consideran compensativos.
- Directiva - Un control de directiva proporciona controles obligatorios basados en regulaciones o requisitos ambientales.

Cada categoría de control incluye controles que proporcionan funciones diferentes. Por ejemplo, una insignia de seguridad es tanto un control físico preventivo como un control físico compensativo. La supervisión y supervisión es tanto un control administrativo detectivesco como un control administrativo compensativo.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender y aplicar los conceptos de gestión de riesgos

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 1: Seguridad y Gestión de Riesgos, Lógico (Técnico)

Pregunta #111 de 137

Id. de pregunta: 1192916

¿Qué tipos de controles son ejemplos de controles preventivos?

a. comprobación de límite

b. Controles de edición

c. Controles de paridad

d. Comprobación de registros

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

explicación

Los controles de edición son un ejemplo de controles preventivos. Los controles de edición se utilizan normalmente en formularios. Los controles de edición de una sola línea son útiles para recuperar una sola cadena del usuario. Los controles de edición permiten que el software evite errores de entrada de datos.

Una comprobación de límites es un ejemplo de control preventivo. La comprobación de límites proporciona un límite en la extensión de la transacción para evitar intentos de transacción no autorizados. Por ejemplo, un programa informático utilizado para procesar el programa de nómina semanal que implementa un límite que la cantidad de pago no debe exceder más de $3000. El propósito principal de la comprobación de límites es implementar un límite superior en una transacción.

Los controles de paridad y la comprobación de registros son términos genéricos y son opciones no válidas.

Las tres categorías de control de acceso proporcionan siete funcionalidades o propósitos diferentes:

- Preventivo - Un control preventivo previene brechas de seguridad y evita riesgos.
- Detective - Un control detective detecta las brechas de seguridad a medida que ocurren.
- Correctivo : un control correctivo restaura el control e intenta corregir cualquier daño infligido durante una infracción de seguridad.

- Disuasión - Un control disuasorio disuade posibles violaciones.
- Recuperación: un control de recuperación restaura los recursos.
- Compensativo: un control compensativo proporciona un control alternativo si otro control puede ser demasiado costoso. Por lo general, todos los controles se consideran compensativos.
- Directiva - Un control de directiva proporciona controles obligatorios basados en regulaciones o requisitos ambientales.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender y aplicar los conceptos de gestión de riesgos

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 1: Seguridad y Gestión de Riesgos, Preventivo

---

Pregunta #112 de 137

Id. de pregunta: 1114673

¿De qué manera debe una entidad cubierta proporcionar un aviso de privacidad a un paciente?

a. una copia publicada

b. una copia impresa en cada prestación de servicios

c. una copia notariada en la primera entrega de servicios

d. una copia impresa en la primera prestación de servicios

e. una copia impresa disponible bajo petición

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

explicación

Se debe proporcionar un aviso de privacidad a través de una copia publicada, una copia impresa en la primera entrega de servicios y una copia impresa disponible a petición de una entidad cubierta para el paciente.

The new privacy regulations require the doctors and other health care providers to provide a notice to their patients as to how the patient's personal medical information will be utilized. The patients must acknowledge the receipt of the notice. The covered entity will restrict the use or disclosure of information on the request of the patients.

All other options are incorrect.

Objective:
Security and Risk Management

Sub-Objective:
Understand legal and regulatory issues that pertain to information security in a global

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Health Insurance Portability and Accountability Act (HIPAA)

Question #113 of 137

Question ID: 1114678

Your company is establishing new employment candidate screening processes. Which of the following should be included?

a. Check all references.

b. Verify all education.

c. Review military records and experience.

d. Perform a background check.

- ✗ **A)** option d
- ✗ **B)** option b
- ✗ **C)** options a and b
- ✗ **D)** options c and d
- ✓ **E)** all of the options
- ✗ **F)** option a
- ✗ **G)** option c

Explanation

A employment candidate screening process should include all of the following actions:

- Check all references.
- Verify all education.
- Review military records and experience.
- Perform a background check.

In addition, drug tests should be administered at this time.

Objective:
Security and Risk Management

Sub-Objective:
Contribute to and enforce personnel security policies and procedures

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Personnel Security Policies

---

Question #114 of 137

Question ID: 1104830

Which process is concerned primarily with identifying vulnerabilities, threats, and risks?

✗ **A)** disaster recovery plan
✓ **B)** business impact analysis (BIA)
✗ **C)** contingency plan
✗ **D)** damage assessment

Explanation

A business impact analysis (BIA) is concerned primarily with identifying vulnerabilities, threats, and risks. The BIA is the most important part of the business continuity plan.

A contingency plan is primarily concerned with recovering major systems and applications after a disruption. It is broader in nature than a disaster recovery plan. A damage assessment is primarily concerned with determining the amount of damage that has occurred. A disaster recovery plan is primarily concerned with recovering systems and applications after a disruption. Each application and system should have a specific plan.

Objective:
Security and Risk Management

Sub-Objective:

Identify, analyze, and prioritize Business Continuity (BC) requirements

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Business Impact Analysis (BIA)

Question #115 of 137

Question ID: 1111658

You are researching computer crimes. All of the following are categories of this type of crime, EXCEPT:

- ✓ **A)** computer-commerce crime
- ✗ **B)** computer-incidental crime
- ✗ **C)** computer-targeted crime
- ✗ **D)** computer-assisted crime

Explanation

There are three categories of computer crime. Computer-commerce crime is not a valid category of computer crime.

The three categories of computer crime are as follows:

- computer-assisted crime - This category of crime is one in which a computer is used as a tool to carry out a crime.
- computer-targeted crime - This category of crime is one in which a computer is the victim of the crime.
- computer-incidental crime - This category of crime is one in which a computer is involved incidentally in the crime. The computer is not the target of the crime and is not the main tool used to carry out the crime.

Objective:

Security and Risk Management

Sub-Objective:

Understand legal and regulatory issues that pertain to information security in a global

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, computer-assisted crime

---

Question #116 of 137

Question ID: 1104779

Which operations security triples component is used to group all hardware, software, and informational resources?

- ✓ **A)** assets
- ✗ **B)** system
- ✗ **C)** vulnerability
- ✗ **D)** media
- ✗ **E)** threats

Explanation

An asset is the operations security triples component that is used to group all hardware, software, and informational resources. Asset, threats, and vulnerabilities are the components of operation security are sometimes referred to as the operations security triples.

A threat is defined as a potential hazard that that can exploit vulnerabilities in the information system.

A vulnerability is a weakness in the system, software, hardware, or procedure. This weakness can be exploited by a threat agent, leading to a risk of loss potential.

Media and systems are not defined as the components of operations security triples.

Objective:
Security and Risk Management

Sub-Objective:
Evaluate and apply security governance principles

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Information and Asset (Tangible/Intangible) Value and Costs

---

Question #117 of 137

Question ID: 1111655

As a health care provider, your organization must follow the guidelines of HIPAA. Which statement is true of HIPAA?

- ✗ **A)** The HIPAA task force performs an inventory of the employees.
- ✓ **B)** HIPAA is enforced by Office of Civil Rights (OCR) of the Department of Health and Human Services (HHS).
- ✗ **C)** HIPAA addresses the issues of security and availability.
- ✗ **D)** HIPAA imposes negligible penalties on offenders.

Explanation

La Oficina de Derechos Civiles (OCR) del Departamento de Salud y Servicios Humanos (HHS) es responsable de la aplicación de la Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA).

Hipaa también se conoce como Ley Kennedy-Kassebaum. El énfasis principal de HIPAA está en la simplificación de la administración a través de la mejora de la eficiencia en la prestación de atención médica. Esta simplificación se logra mediante la normalización del intercambio electrónico de datos y la protección de la confidencialidad y la seguridad de los datos sanitarios. Después de la implementación, HIPAA se adelanta a las leyes estatales, a menos que la ley estatal sea más estricta. Una ley estricta implica que la ley estatal es más estricta que las regulaciones hipaa en un cierto aspecto. En tal escenario, la ley estatal será aplicable. HIPAA se aplica a la información de salud que es creada o mantenida por proveedores de atención médica que participan en ciertas transacciones electrónicas, planes de salud y centros de intercambio de información de atención médica. Hipaa no es aplicable a las instituciones financieras, tales como bancos. Es aplicable a cualquier entidad que pueda almacenar información de atención médica de forma regular, incluidos hospitales, clínicas, universidades, escuelas, agencias de facturación y centros de intercambio de información.

El Título II, Simplificación Administrativa, de la Ley de Portabilidad y Responsabilidad del Seguro Médico aborda los estándares de transacción que incluyen conjuntos de códigos, identificadores de salud únicos, firmas electrónicas y de seguridad, y privacidad. El Título II cubre a los proveedores de atención médica que transmiten información médica electrónicamente en relación con transacciones estándar, planes de salud y centros de intercambio de información de atención médica. NO cubre a los empleadores. La versión 4010 del American National Standards Institute Accredited Standards Committee X12 (ANSI ASC X12) se aplica a la categoría de transacciones de HIPAA.

La implementación de HIPAA ha dado lugar a cambios en las transacciones de atención médica y los sistemas de información administrativa. Hipaa impone fuertes sanciones civiles y penales para los infractores no conformes. Las multas pueden variar de $ 25K a $ 250K si hay múltiples violaciones del mismo estándar. Una persona también puede ser encarcelada por hacer un uso induso deliberado de la información sanitaria.

El grupo de trabajo hipaa mantiene un inventario de los siguientes datos en una empresa:

- Sistemas
- Procesos
- políticas
- Procedimientos
- datos

El grupo de trabajo de HIPAA determina la información que es crítica para la atención al paciente y para la institución médica. Estos elementos se enumeran por prioridad, disponibilidad, confiabilidad, acceso y uso. El grupo de trabajo responsable del análisis de la información de la empresa debe documentar cuidadosamente el uso de los criterios.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:

Comprender los problemas legales y reglamentarios relacionados con la seguridad de la información en un entorno global

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Portabilidad de Seguros De Salud y Ley de Responsabilidad (HIPAA)

Pregunta #118 de 137

Id. de pregunta: 1114672

Usted es el administrador de seguridad de un centro de tratamiento de abuso de alcohol y drogas. ¿En qué tres situaciones es aceptable la divulgación de información confidencial relacionada con los pacientes de su organización?

a. a personal cualificado para la auditoría

b. a personal cualificado para la investigación

c. al personal médico en una emergencia médica

d. para la recuperación de información por parte de una persona ajena al programa que realiza una solicitud formal

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

explicación

La divulgación de información confidencial relacionada con pacientes con abuso de alcohol y drogas es aceptable sujeto a las siguientes condiciones:

- La divulgación está permitida por la orden judicial.
- El paciente da su consentimiento por escrito para la divulgación.
- La divulgación se hace al personal médico en caso de una emergencia médica o al personal calificado con fines de investigación y auditoría.

Es importante tener en cuenta que los registros de pacientes con abuso de alcohol y drogas están protegidos por las leyes y regulaciones federales. Aparte de las excepciones mencionadas anteriormente, no se permite la divulgación de

información confidencial relacionada con pacientes con abuso de alcohol y drogas. Por lo tanto, la información no puede ser revelada para la recuperación de información por una persona fuera del programa que hace una solicitud formal.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender los problemas legales y reglamentarios relacionados con la seguridad de la información en un entorno global

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Portabilidad de Seguros De Salud y Ley de Responsabilidad (HIPAA)

Confidencialidad de los registros de pacientes con abuso de alcohol y drogas, Título 42 CFR, Parte 2, Sección 1, https://www.gpo.gov/fdsys/granule/CFR-2010-title42-vol1/CFR-2010-title42-vol1-part2/content-detail.html

---

Pregunta #119 de 137

Id. de pregunta: 1192913

La política de seguridad de su empresa incluye pruebas del sistema y directrices de formación de concienciación sobre seguridad. ¿Qué tipo de control se tiene en cuenta?

- ✗ **A)** control administrativo detectivesco
- ✗ **B)** control técnico preventivo
- ✓ **C)** control administrativo preventivo
- ✗ **D)** control técnico detectivesco

explicación

Las pruebas y la capacitación se consideran controles administrativos preventivos. Los controles administrativos dictan cómo se implementan las políticas de seguridad para cumplir con los objetivos de seguridad de la empresa. Los controles preventivos son controles que se implementan para evitar brechas de seguridad. Los controles administrativos preventivos ponen énfasis en los mecanismos blandos que se implementan para apoyar los objetivos de seguridad e incluyen políticas de seguridad, clasificación de la información, procedimientos de personal, pruebas y capacitación en conciencia de seguridad. El uso de formularios pre-numerados para transacciones de ventas también es un control administrativo preventivo.

Los controles técnicos de detectives incluyen registros de auditoría y sistemas de detección de intrusiones (IDS). Los controles administrativos detectives incluyen la supervisión y la supervisión, la rotación del trabajo, y las

investigaciones. Los controles técnicos preventivos incluyen listas de control de acceso (ACL), enrutadores, cifrado, software antivirus, imágenes de servidor, tarjetas inteligentes y sistemas de devolución de llamadas.

Hay tres categorías de control de acceso: controles técnicos, administrativos y físicos. Se ha establecido un control técnico para restringir el acceso a las redes y los sistemas. Un administrativo se desarrolla para dictar cómo se implementan las políticas de seguridad para cumplir con los objetivos de seguridad de la empresa. Un control físico se implementa para proteger el acceso físico a un objeto, como un edificio, una sala o un equipo. Las tres categorías de control de acceso proporcionan siete funcionalidades o propósitos diferentes:

- Preventivo - Un control preventivo previene brechas de seguridad y evita riesgos.
- Detective - Un control detective detecta las brechas de seguridad a medida que ocurren.
- Correctivo : un control correctivo restaura el control e intenta corregir cualquier daño infligido durante una infracción de seguridad.
- Disuasión - Un control disuasorio disuade posibles violaciones.
- Recuperación: un control de recuperación restaura los recursos.
- Compensativo: un control compensativo proporciona un control alternativo si otro control puede ser demasiado costoso. Por lo general, todos los controles se consideran compensativos.
- Directiva - Un control de directiva proporciona controles obligatorios basados en regulaciones o requisitos ambientales.

Cada categoría de control incluye controles que proporcionan funciones diferentes. Por ejemplo, una insignia de seguridad es tanto un control físico preventivo como un control físico compensativo. La supervisión y supervisión es tanto un control administrativo detectivesco como un control administrativo compensativo.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender y aplicar los conceptos de gestión de riesgos

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 1: Seguridad y Gestión de Riesgos, Preventiva

---

Pregunta #120 de 137

Id. de pregunta: 1302570

Haga clic en cada uno de los encabezados del escenario para expandir o contraer su contenido. Debe leer todo el escenario para responder a la pregunta.

fondo

Usted es un profesional de la seguridad contratado recientemente por una empresa que cotiza en bolsa para ayudar a administrar la seguridad de la organización. La compañía tiene una oficina principal en Atlanta, GA, y sucursales en

todo el sureste de los Estados Unidos. El departamento de TI tiene un pequeño personal alojado en la oficina de Atlanta.

Temas actuales

El año pasado, una tormenta invernal cerró las operaciones en la mayoría de sus oficinas. Si bien ninguna de sus instalaciones fue destruida y las operaciones normales se restauraron en 24 horas, a la administración le preocupa que no exista un plan de recuperación ante desastres. Se le ha pedido que prepare un plan para cubrir este tipo de interrupción.

Actualmente, su organización mantiene varias bases de datos grandes de contenido digital que son vitales para las operaciones de su organización. Se utilizan diferentes controles para administrar este contenido. La administración le ha pedido que implemente una solución para controlar la apertura, edición, impresión o copia de estos datos de una manera más centralizada.

En los próximos seis meses, su empresa planea mover todos los servidores y granjas de servidores a un centro de datos centralizado. El centro de datos ocupará el tercer piso de un edificio de seis pisos que actualmente está en construcción. La administración le ha pedido que se asegure de que el acceso al centro de datos esté estrictamente controlado. Durante ese mismo tiempo, es probable que su organización compre un competidor para fusionarse con su organización existente.

Recientemente, uno de los servidores de la intranet fue víctima de un ataque de denegación de servicio (DoS). El departamento de TI tardó más de 24 horas en volver a poner en funcionamiento el servidor. Durante ese tiempo, el personal de la oficina principal no pudo acceder a la importante información sobre recursos humanos disponible en el servidor de la intranet afectado.

La semana pasada, descubrió que se utilizaron varias cuentas de usuario en un intento de piratear su red. Afortunadamente, las cuentas fueron bloqueadas debido a intentos de inicio de sesión no válidos. Revise los registros y determine que tres de las cuentas se crearon para el personal que ya no está empleado por su organización.

Después de presionar durante años, ha recibido permiso de la administración para diseñar e implementar un programa integral de concienciación de seguridad en toda la organización.

Usted decide implementar la biometría para controlar el acceso al centro de datos. ¿Qué tipo de control de acceso ha implementado?

- ✗ **A)** control administrativo preventivo
- ✓ **B)** control físico preventivo
- ✗ **C)** control detectivesco físico
- ✗ **D)** control administrativo detectivesco

Explanation

Using biometrics to control access to the data center is a physical preventive control.

An administrative detective control is a control implemented to administer the organization's assets and personnel that will detect an attack. Administrative detective controls include monitoring, job rotation, investigations, security reviews, and background checks.

An administrative preventive control is a control implemented to administer the organization's assets and personnel that will prevent an attack. Administrative preventive controls include personnel procedures, security policies, separation of duties, information classification, security awareness training, and disaster recovery plans.

A physical detective control is a control implements to protect an organization's facilities and personnel that will detect an attack. Physical detective controls include guards, dogs, motion detectors, and CCTV.

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply risk management concepts

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Risk Management Concepts

---

Pregunta #121 de 137

Id. de pregunta: 1111640

Al desarrollar un programa de gestión de seguridad, ¿qué desarrollo será el resultado de seguir una estructura de ciclo de vida?

- ✓ **A)** Las políticas escritas se asignan a las actividades de seguridad y las admiten.
- ✗ **B)** El progreso y el rendimiento de la inversión no pueden evaluarse.
- ✗ **C)** La organización confía en la tecnología para todas las soluciones de seguridad.
- ✗ **D)** Las personas responsables de proteger los activos de la empresa no se comunican.

explicación

Cuando las políticas escritas se asignan a las actividades de seguridad y las respaldan, es el resultado de seguir una estructura de ciclo de vida.

Cuando no se sigue la estructura de ciclo de vida para desarrollar un programa de administración de seguridad, se producen las situaciones siguientes:

- Las políticas y procedimientos escritos NO se asignan a las actividades de seguridad ni son compatibles con las actividades de seguridad.

- Las personas responsables de proteger los activos de la empresa NO se comunican y están desconectadas entre sí.
- El progreso y el retorno de la inversión del gasto y la asignación de recursos NO pueden ser evaluados.
- Las deficiencias del programa de seguridad NO se entienden, y no existe una forma estandarizada de mejorar las deficiencias.
- El cumplimiento de las regulaciones, leyes y políticas NO está asegurado.
- La organización confía en la tecnología para todas las soluciones de seguridad.
- Las brechas de seguridad dan lugar a medidas de emergencia en un enfoque reactivo.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
evaluar y aplicar los principios de gobierno de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y gestión de riesgos, Ciclo de vida del programa de seguridad

---

Pregunta #122 de 137

Id. de pregunta: 1104814

Un usuario configura el filtro del bloqueador de elementos emergentes de Internet Explorer en Alto: Bloquear todas las ventanas emergentes. Sin embargo, el usuario desea ver una ventana emergente que se está bloqueando. ¿Qué debe hacer el usuario?

✗ **A)** Agregue el sitio a la lista Sitios permitidos.
✗ **B)** Cambie la configuración del bloqueador de elementos emergentes a Medio.
✓ **C)** Pulse Ctrl+Alt mientras se abre la ventana emergente.
✗ **D)** Cambie la configuración del bloqueador de elementos emergentes a Baja.

explicación

Debe mantener presionadas las teclas Ctrl+Alt mientras se abre la ventana emergente. El alto: Bloquear todas las ventanas emergentes configuración bloquea todas las ventanas emergentes. Para permitir que se muestre una sola ventana emergente, debe mantener presionadas las teclas Ctrl+Alt cuando se abra la ventana emergente.

No debe cambiar la configuración del bloqueador de elementos emergentes a Medio. Esto reduciría la seguridad de Internet Explorer y probablemente permitiría más ventanas emergentes de lo que el usuario pretendía. Además, no hay ninguna garantía de que la ventana emergente que el usuario desea ver no se bloquee.

No debe cambiar la configuración del bloqueador de elementos emergentes a Baja. Esto reduciría la seguridad de Internet Explorer y permitiría más ventanas emergentes de lo que el usuario pretendía.

No debe agregar el sitio a la lista Sitios permitidos. Esto permitiría que la ventana emergente se muestre siempre. El escenario indica que el usuario desea ver la ventana emergente, pero no indica que siempre se deba mostrar la ventana emergente.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender los problemas legales y reglamentarios relacionados con la seguridad de la información en un entorno global

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Ejemplos de Delitos Informáticos

---

Pregunta #123 de 137

Id. de pregunta: 1192921

Haga clic en cada uno de los encabezados del escenario para expandir o contraer su contenido. Debe leer todo el escenario para responder a la pregunta.

fondo

Usted es un profesional de la seguridad contratado recientemente por una empresa que cotiza en bolsa para ayudar a administrar la seguridad de la organización. La compañía tiene una oficina principal en Atlanta, GA, y sucursales en todo el sureste de los Estados Unidos. El departamento de TI tiene un pequeño personal alojado en la oficina de Atlanta.

Temas actuales

El año pasado, una tormenta invernal cerró las operaciones en la mayoría de sus oficinas. Si bien ninguna de sus instalaciones fue destruida y las operaciones normales se restauraron en 24 horas, a la administración le preocupa que no exista un plan de recuperación ante desastres. Se le ha pedido que prepare un plan para cubrir este tipo de interrupción.

Actualmente, su organización mantiene varias bases de datos grandes de contenido digital que son vitales para las operaciones de su organización. Se utilizan diferentes controles para administrar este contenido. La administración le ha pedido que implemente una solución para controlar la apertura, edición, impresión o copia de estos datos de una manera más centralizada.

En los próximos seis meses, su empresa planea mover todos los servidores y granjas de servidores a un centro de datos centralizado. El centro de datos ocupará el tercer piso de un edificio de seis pisos que actualmente está en

construcción. La administración le ha pedido que se asegure de que el acceso al centro de datos esté estrictamente controlado. Durante ese mismo tiempo, es probable que su organización compre un competidor para fusionarse con su organización existente.

Recientemente, uno de los servidores de la intranet fue víctima de un ataque de denegación de servicio (DoS). El departamento de TI tardó más de 24 horas en volver a poner en funcionamiento el servidor. Durante ese tiempo, el personal de la oficina principal no pudo acceder a la importante información sobre recursos humanos disponible en el servidor de la intranet afectado.

La semana pasada, descubrió que se utilizaron varias cuentas de usuario en un intento de piratear su red. Afortunadamente, las cuentas fueron bloqueadas debido a intentos de inicio de sesión no válidos. Revise los registros y determine que tres de las cuentas se crearon para el personal que ya no está empleado por su organización.

Después de presionar durante años, ha recibido permiso de la administración para diseñar e implementar un programa integral de concienciación de seguridad en toda la organización.

Al diseñar la capacitación en conciencia de seguridad, ¿cuál debería ser la base principal para desarrollar diferentes niveles de capacitación?

- ✗ **A)** riesgos cubiertos
- ✗ **B)** costar
- ✗ **C)** controles implementados
- ✓ **D)** audiencia

explicación

Al diseñar la capacitación de conciencia de seguridad, la base principal para desarrollar diferentes niveles de capacitación debe estar en la audiencia.

La administración de alto nivel debe recibir capacitación que proporcione comprensión de los riesgos y amenazas y el efecto que tienen en la reputación y las finanzas de la organización.

Los mandos intermedios deben recibir formación que cubra políticas, estándares, líneas de base, directrices y procedimientos para comprender cómo ayudan a proteger la seguridad.

El personal técnico debe recibir capacitación técnica sobre controles de seguridad y certificaciones de seguridad de la industria.

El personal de plantilla debe recibir capacitación para ayudarles a comprender sus responsabilidades mientras realizan sus tareas cotidianas.

El costo, los riesgos cubiertos o los controles implementados no son la base para desarrollar diferentes niveles de capacitación.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Establecer y mantener un programa de concienciación, educación y capacitación en materia de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y gestión de riesgos, educación, formación y sensibilización sobre la seguridad

Conciencia de seguridad - Implementación de una estrategia eficaz, https://www.sans.org/reading-room/whitepapers/awareness/security-awareness-implementing-effective-strategy-418

Pregunta #124 de 137

Id. de pregunta: 1104795

Su organización debe informar con precisión sus datos financieros a sus accionistas y al público. ¿Qué reglamento proporciona directrices sobre este tipo de información?

- ✓ **A)** Sox
- ✗ **B)** HIPAA
- ✗ **C)** Basilea II
- ✗ **D)** GLBA

explicación

La Ley Sarbanes-Oxley (SOX) de 2002 proporciona directrices sobre la presentación precisa de datos financieros corporativos a los accionistas y al público. Fue escrito para evitar que las empresas cometan fraude al proporcionar a sabiendas informes financieros inexactos a los accionistas y al público. Se ocupa principalmente de las prácticas contables corporativas. El artículo 404 de esta ley se refiere específicamente a la tecnología de la información.

La Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA, por sus contra, por sus, se redactó para evitar que las organizaciones médicas (incluidas las compañías de seguros de salud, los hospitales y los consultorios médicos) compartan información sobre la atención médica de los pacientes sin consentimiento. Se ocupa principalmente de la seguridad, integridad y privacidad de la información del paciente.

La Ley Gramm-Leach-Bliley (GLBA) de 1999 fue escrita para garantizar que las instituciones financieras desarrollen avisos de privacidad y permitan a sus clientes evitar que las instituciones financieras compartan información con terceros. También cubre problemas de privacidad con seguros y atención médica.

El Acuerdo de Basilea II se basa en tres pilares principales: requisitos mínimos de capital, supervisión y disciplina de mercado. Estos pilares se aplican a las instituciones financieras.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender los problemas legales y reglamentarios relacionados con la seguridad de la información en un entorno global

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Ley Sarbanes-Oxley (SOX)

Pregunta #125 de 137

Id. de pregunta: 1114677

Su organización le ha pedido que trabaje con un equipo para desarrollar un plan de continuidad del negocio para su organización. Los miembros del equipo han sugerido muchos eventos que deben considerarse como parte del plan de continuidad de las actividades. ¿Qué eventos deben ser considerados?

a. Desastres naturales

b. Error de hardware

c. reubicación del servidor

d. Renuncia de los empleados

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

explicación

Como parte del plan de continuidad de las actividades, deben tenerse en cuenta los desastres naturales. Los desastres naturales incluyen tornados, inundaciones, huracanes y terremotos. Es necesario definir una estrategia de continuidad del negocio para preservar los elementos informáticos, como el hardware, el software y los elementos de

red. La estrategia debe abordar el uso de las instalaciones durante un evento disruptivo y definir los roles del personal en la implementación de la continuidad.

También se debe tener en cuenta el error de hardware. Este hardware se puede limitar a un único componente del equipo, pero puede incluir errores de enlace de red o de línea de comunicaciones. La mayoría del tiempo de inactividad no planificado experimentado por una empresa suele deberse a un error de hardware.

El plan de continuidad del negocio solo debe incluir los eventos que interrumpen los servicios. Normalmente, la reubicación del servidor se planifica de tal manera que se garantice que no se interpa o se interpa un mínimo de los servicios. Como tal, por lo general no forma parte del plan de continuidad del negocio.

La renuncia de los empleados, incluso la renuncia de un gerente de TI de alto nivel, no debe considerarse como parte del plan de negocios. La renuncia de los empleados es una parte normal de hacer negocios. Sin embargo, las huelgas de empleados y las acciones de los empleados descontentos deben considerarse como parte del plan de continuidad del negocio.

En la etapa incipiente de un desastre, se deben tomar medidas de emergencia para prevenir lesiones y la pérdida de vidas. Usted debe intentar disminuir el daño a la función corporativa para evitar la necesidad de recuperación. El propósito de iniciar acciones de emergencia justo después de que ocurra un desastre es prevenir la pérdida de vidas y lesiones y mitigar más daños.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Identificar, analizar y priorizar los requerimientos de Continuidad del Negocio (BC, Business Continuity)

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Planificación de continuidad y el Plan de Continuidad del Negocio (BCP)

Pregunta #126 de 137

Id. de pregunta: 1104764

¿Qué función es una función estratégica que ayuda a desarrollar políticas, normas y directrices y garantiza que los elementos de seguridad se implementen correctamente?

✗ **A)** administrador de seguridad
✓ **B)** analista de seguridad
✗ **C)** usuario
✗ **D)** titular de los datos

explicación

El analista de seguridad es un rol estratégico que ayuda a desarrollar políticas, estándares y directrices y garantiza que los elementos de seguridad se implementen correctamente. La participación del analista de seguridad en la fase de diseño del sistema del ciclo de vida de desarrollo del sistema proporciona el máximo beneficio a la organización.

Un usuario tiene acceso habitualmente a los datos corporativos y debe tener asignado el nivel de acceso adecuado. Los usuarios deben participar en la fase de definición de requisitos del sistema para asegurarse de que el sistema cumple los requisitos del usuario.

El propietario de los datos aprueba las clases de datos y modifica las clases según las necesidades. Este rol debe garantizar que se establezcan los controles de seguridad y los derechos de acceso de usuario adecuados.

El administrador de seguridad crea nuevas cuentas de usuario y contraseñas, implementa software de seguridad y prueba parches y componentes de software. Este rol es de naturaleza más funcional en comparación con el rol de analista de seguridad.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
evaluar y aplicar los principios de gobierno de seguridad

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 1: Seguridad y Gestión de Riesgos, Analista de Seguridad

---

Pregunta #127 de 137

Id. de pregunta: 1111661

Su organización crea aplicaciones de software que se venden al público. Recientemente, la administración se ha preocupado por la piratería de software. ¿Qué organización se ocupa de la prevención de este delito?

✗ **A)** NCSC
✗ **B)** CIA
✗ **C)** DoD
✓ **D)** SPA

Explanation

The Software Protection Association (SPA) deals with the prevention of software piracy. Software piracy refers to the illegitimate use of either licensed software or an application. A software license specifies regulations relating to the use and the security of the software. The license is terminated if an individual or a company fails to abide by the license

requirements. Trade associations, such as the SPA and the Business Software Alliance (BSA), were formed by a group of companies to ensure that software laws are not violated. These groups ensure that software developed by the companies and the corresponding licensing issues are properly addressed. This, in turn, ensures that revenues of software development companies are not hampered.

The primary objective of the Central Intelligence Agency (CIA) is to preserve the national security of the United States and the lives of all Americans.

The Department of Defense (DoD) controls the United States military and coordinates its activities. DoD does not investigate computer crimes.

The National Computer Security Center (NCSC) is a centralized agency that evaluates computer security products and provides technical support to government offices and private firms.

To keep a check on software piracy, an organization should adopt standard practices, such as the use of licensed software and the regular scanning of the network and all computers to detect the use of unlicensed software. Use of licensed software is considered ethical.

Software piracy in the Asia/Pacific region accounts for about 4 billion dollars of lost income to software publishers. Cross-jurisdictional law enforcement issues make investigating and prosecuting such crime difficult. Issues in stopping overseas software piracy include the following:

- The cooperation of foreign law enforcement agencies and foreign governments must be obtained.
- The quality of the illegal copies of the software is improving, making it more difficult for purchasers to differentiate between legal and illegal products.
- The producers of the illegal copies of software are dealing in large quantities, resulting in faster deliveries of illicit software.

Objective:
Security and Risk Management

Sub-Objective:
Understand legal and regulatory issues that pertain to information security in a global

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Software Piracy and Licensing Issues

---

Question #128 of 137

Question ID: 1104885

Which statement is true of the staff members of an organization in the context of information security?

✗ **A)** They must be trained to handle internal violations of the security policy.

✓ **B)** They pose more threat than external hackers.

✗ **C)** They do not require extensive understanding of security.

✗ **D)** They are responsible for protecting and backing up confidential data.

Explanation

The staff members of an organization pose more threat than external hackers. Disgruntled employees typically attempt the security breaches in an organization. Existing employees can accidentally commit a security breach and may put the security of the organization at risk. User accounts should be immediately deleted and the associated privileges should be revoked for employees who have been terminated or have left the organization.

It is not the job of the staff member to handle and respond to issues of information security violation. Staff members should report the incident to the department manager. The department manager will take the necessary steps as a part of incident response.

Typically, it is the job of the IT department to ensure that critical data is duly backed up on a periodical basis and that only identified employees with necessary privileges have access to confidential information.

Only those staff members with a direct role in the security function of an organization need extensive security knowledge. Most staff members will need security awareness training on security policies, security practices, acceptable resource usage, and noncompliance implications.

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply threat modeling concepts and methodologies

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management,]Identity Threats and Vulnerabilities

---

Question #129 of 137

Question ID: 1104771

What should be the role of the management in developing an information security program?

✗ **A)** It is not required at all.

✓ **B)** It is mandatory.

✗ **C)** It is limited to the sanctioning of funds.

✗ **D)** It should be minimal.

Explanation

The role of the management in developing an information security program is mandatory. The primary purpose of security management is to protect the information assets of the organization. Therefore, the senior management should play a vital role in developing and driving the information security program. The scope of the security program should be defined and evaluated through management initiative before implementation. The management should assign responsibilities and define the roles for the implementation of the security program.

A top-down security management approach is recommended to make an information security program successful. A top-down approach requires the involvement and support of senior management in developing, initiating, and implementing a security policy for the organization. The initiative originates from the top management. The first step involves adopting a corporate information security policy to establish an information security program. A top-down approach ensures that the management exercises the practices of due diligence and due care to protect the information assets of the organization.

Objective:
Security and Risk Management

Sub-Objective:
Evaluate and apply security governance principles

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Security Governance Principles

---

Pregunta #130 de 137

Id. de pregunta: 1111665

Su organización ha decidido que es necesario desarrollar un plan de continuidad del negocio completo. Se le ha encomendado la tarea de iniciar este proyecto. ¿Qué paso debe completarse durante la fase de iniciación?

- ✓ **A)** Desarrollar la declaración de política de planificación de continuidad.
- ✗ **B)** Realizar el análisis de impacto empresarial (BIA).
- ✗ **C)** Identificar controles preventivos.
- ✗ **D)** Desarrollar estrategias de recuperación.

explicación

Durante el inicio del proyecto, debe desarrollar la declaración de directiva de planificación de continuidad. La declaración de directiva de planeación de continuidad establece el ámbito del proyecto del plan de continuidad del negocio, los roles de los miembros del equipo y los objetivos del proyecto. También debe seleccionar un coordinador

de continuidad del negocio y formar un equipo de continuidad del negocio. El equipo de continuidad del negocio debe trabajar con la gerencia para llegar a objetivos claros y definir el alcance del proyecto.

Debe identificar los controles preventivos una vez completado el análisis de impacto empresarial (BIA).

Debe realizar el BIA una vez que se complete la declaración de política de planificación de continuidad. La BIA ayuda a las unidades de negocio a comprender el impacto de un evento disruptivo.

Usted debe desarrollar estrategias de recuperación después de que se han identificado los controles preventivos.

Los pasos de la continuidad del negocio son los siguientes:

- Desarrollar la declaración de política de planificación de continuidad.
- Llevar a cabo la BIA.
- Identificar controles preventivos.
- Desarrollar estrategias de recuperación.
- Desarrollar el plan de contingencia.
- Pruebe el plan y realice entrenamientos y ejercicios.
- Mantener el plan.

Al desarrollar el plan de continuidad del negocio se deben tener en cuenta las siguientes reglas:

- Debería formarse un comité para decidir un curso de acción. Estas decisiones deben tomarse con antelación e incorporarse al plan.
- En sus procedimientos y tareas, el plan debe referirse a funciones, no a individuos específicos.
- Los proveedores críticos deben ser contactados con anticipación para validar que el equipo se puede obtener de manera oportuna.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Identificar, analizar y priorizar los requerimientos de Continuidad del Negocio (BC, Business Continuity)

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Planificación de continuidad y el Plan de Continuidad del Negocio (BCP)

Pregunta #131 de 137

Id. de pregunta: 1114679

¿Qué término se utiliza cuando queda algún riesgo incluso después de implementar contramedidas?

✗ **A)** responsabilidad legal

✓ **B)** riesgo residual

✗ **C)** ventaja legal

✗ **D)** responsabilidad derivada

explicación

Riesgo residual cuando queda algún riesgo incluso después de implementar contramedidas. El riesgo residual suele ser aceptable. El riesgo total es todo el riesgo y se produce cuando una organización no implementa ninguna protección.

riesgo total = amenazas x vulnerabilidad x valor de los activos

riesgo residual = (amenazas x vulnerabilidad x valor de activos) x brecha de controles

Una organización puede tener responsabilidad legal en la medida del riesgo residual y podría tener que incurrir en daños y perjuicios por no ejercer el debido cuidado y diligencia. Por consiguiente, la responsabilidad existe en la medida de la diferencia entre el costo de aplicar las contramedidas (C) y la pérdida estimada (L). La pérdida estimada siempre debe ser mayor que el costo de las contramedidas.

Es una práctica prudente por parte de la administración transferir el riesgo residual mediante prácticas, como los seguros, para mitigar la responsabilidad con respecto al riesgo residual.

El riesgo residual y la ventaja legal no son relevantes en términos de cuestiones de responsabilidad relacionadas con las prácticas de gestión de la seguridad de la información.

La responsabilidad posterior garantiza que las organizaciones que trabajan juntas en virtud de un contrato sean responsables de su gestión de la seguridad de la información y de los controles de seguridad desplegados por cada organización.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender y aplicar los conceptos de gestión de riesgos

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 1: Seguridad y Gestión de Riesgos, Riesgo Total Versus Riesgo Residual

---

Pregunta #132 de 137

Id. de pregunta: 1113902

Se le ha pedido que identifique los objetivos de la organización para su uso en el desarrollo de un modelo de seguridad de la organización. ¿Qué tipo de objetivos son objetivos diarios?

- ✓ **A)** objetivos operacionales
- ✗ **B)** objetivos tácticos
- ✗ **C)** objetivos estratégicos
- ✗ **D)** objetivos de la organización

explicación

Las metas operativas son metas diarias. Se centran en las actividades diarias que se deben completar para mantener las funciones de la empresa.

Los objetivos tácticos son objetivos de mitad de período. Toman más tiempo y esfuerzo que los objetivos operativos, pero menos tiempo y esfuerzo que los objetivos estratégicos.

Los objetivos estratégicos son objetivos a largo plazo. Miran más hacia el futuro que los objetivos operativos y tácticos, y tardan mucho más en planificarse e implementarse.

Objetivos organizacionales es un término genérico que se usa para abordar todos los objetivos de una organización. Cada objetivo de la organización se clasifica como de naturaleza operativa, táctica o estratégica.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Desarrollar, documentar e implementar políticas, estándares, procedimientos y directrices de seguridad

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Documentación de Seguridad

Diferencia entre objetivos estratégicos y operativos, http://smallbusiness.chron.com/difference-between-strategic-operational-objectives-24572.html

---

Pregunta #133 de 137

Id. de pregunta: 1113901

¿Qué afirmación es cierta de los hackers y crackers?

- ✗ **A)** Los hackers y crackers son siempre programadores expertos.
- ✓ **B)** Los hackers y crackers quieren verificar sus habilidades como intrusos.

✗ **C)** Los hackers y crackers solo irrumpen en los escritorios independientes de los ordenadores domésticos.

✗ **D)** Los hackers y crackers no tienen ningún motivo, oportunidades y medios (MOM).

explicación

Los hackers y crackers quieren verificar sus habilidades como intrusos. Quieren ver hasta dónde pueden llegar sus habilidades.

Los hackers y crackers pueden ser programadores expertos, niños de guiones o incluso empleados descontentos. En la mayoría de los escenarios, los ataques de piratería son llevados a cabo por empleados o ex empleados. Muchos delitos informáticos están asociados con los empleados dentro de la organización porque estos empleados tienen acceso autorizado que utilizan para realizar operaciones no autorizadas. La mayoría de los hackers y crackers no necesitan habilidades de programación reales para llevar a cabo sus ataques.

Los hackers y las galletas no solo irrumpen en las computadoras domésticas. Pueden derribar la red de toda una organización. Los hackers y crackers pueden realizar diferentes tipos de ataques, como denegación de servicio (DoS), inundación SYN, virus, gusanos, caballos de Troya y descifrado de contraseñas para explotar la vulnerabilidad de un recurso crítico.

Los hackers son generalmente considerados como personas que exploran los sistemas informáticos sin una verdadera intención maliciosa o simplemente para jugar bromas. Los crackers son hackers que son más maliciosos, por lo general con la intención de hacer daño real. Los hackers típicos son personas que se alejan de las normas de seguridad aceptadas de la sociedad.

La intrusión es impulsada por el motivo, la oportunidad y los medios (MOM) para entrar en la red de una organización. El motivo es la razón para realizar una intrusión, como el deseo de un individuo de desviarse de las normas aceptadas de conducta ética en una sociedad. La oportunidad se refiere a las vías para cometer un delito, como los sistemas vulnerables. Los medios implican las capacidades del intruso y las herramientas disponibles para el intruso mientras realiza una intrusión. Incluye las herramientas de software que un hacker o un cracker utiliza para explotar las vulnerabilidades.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender los problemas legales y reglamentarios relacionados con la seguridad de la información en un entorno global

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 1: Seguridad y Gestión de Riesgos, Hackers Versus Crackers

Pregunta #134 de 137

Id. de pregunta: 1192911

La administración ha expresado interés en implementar elementos disuasorios para desalentar las violaciones de seguridad. ¿Qué control es un ejemplo de esta estrategia?

✗ **A)** un registro de auditoría

✗ **B)** una tarjeta inteligente

✓ **C)** una valla

✗ **D)** un router

explicación

Una valla es un ejemplo de un control físico disuasorio porque intenta disuadir o desalentar las brechas de seguridad. Una valla también se considera un control compensativo.

Los enrutadores y las tarjetas inteligentes son ejemplos de controles técnicos preventivos porque se utilizan para evitar infracciones de seguridad. También son ejemplos de controles técnicos compensativos. Los registros de auditoría son controles técnicos detectivescos y controles técnicos compensativos.

Hay tres categorías de control de acceso: controles técnicos, administrativos y físicos. Se ha establecido un control técnico para restringir el acceso. Los controles técnicos funcionan para proteger el acceso al sistema, la arquitectura y el acceso a la red, las zonas de control, la auditoría y el cifrado y los protocolos. Se desarrolla un control administrativo para dictar cómo se implementan las políticas de seguridad para cumplir con los objetivos de seguridad de la empresa. Los controles administrativos incluyen políticas y procedimientos, controles de personal, estructura de supervisión, capacitación en seguridad y pruebas. Un control físico se implementa para proteger el acceso físico a un objeto, como un edificio, una sala o un equipo. Los controles físicos incluyen insignias, cerraduras, guardias, segregación de red, seguridad perimetral, controles informáticos, separación de áreas de trabajo, copias de seguridad y cableado.

Las tres categorías de control de acceso proporcionan siete funcionalidades o propósitos diferentes:

- Preventivo - Un control preventivo previene brechas de seguridad y evita riesgos.
- Detective - Un control detective detecta las brechas de seguridad a medida que ocurren.
- Correctivo : un control correctivo restaura el control e intenta corregir cualquier daño infligido durante una infracción de seguridad.
- Disuasión - Un control disuasorio disuade posibles violaciones.
- Recuperación: un control de recuperación restaura los recursos.
- Compensativo: un control compensativo proporciona un control alternativo si otro control puede ser demasiado costoso. Por lo general, todos los controles se consideran compensativos.
- Directiva - Un control de directiva proporciona controles obligatorios basados en regulaciones o requisitos ambientales.

Cada categoría de control incluye controles que proporcionan funciones diferentes. Por ejemplo, una insignia de seguridad es tanto un control físico preventivo como un control físico compensativo. La supervisión y supervisión es

tanto un control administrativo detectivesco como un control administrativo compensativo.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender y aplicar los conceptos de gestión de riesgos

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y gestión de riesgos, disuasión

---

Pregunta #135 de 137

Id. de pregunta: 1111688

¿Qué afirmación es cierta para los controles de acceso físico?

- ✗ **A)** Sólo los bloqueos combinados forman parte de los sistemas de control de acceso físico.
- ✗ **B)** Las contraseñas proporcionan la mejor forma de control de acceso físico en una instalación.
- ✓ **C)** Los dispositivos de vigilancia ofrecen más protección que las vallas en las instalaciones.
- ✗ **D)** Los CCTVs en el control de acceso físico no necesitan una capacidad de grabación.

explicación

Los dispositivos de vigilancia ofrecen más protección que las vallas en la instalación porque en realidad registran la actividad de las áreas de tráfico. Esto proporciona un mecanismo mediante el cual se pueden reproducir cintas para investigar las infracciones de seguridad.

Las contraseñas NO proporcionan la mejor forma de control de la instalación de acceso físico. Los televisores de circuito cerrado (CCTVs) siempre deben tener una capacidad de grabación. Todos los tipos de cerraduras forman parte de los sistemas de control de acceso físico.

Los controles de acceso físico pueden incluir lo siguiente como medidas de seguridad:

- guardias para proteger el perímetro de la instalación
- vallas alrededor de la instalación para evitar el acceso no autorizado por parte de los intrusos
- insignias para los empleados para una fácil identificación
- cerraduras (combinación, cifrado, mecánico y otros) dentro de la instalación para disuadir a los intrusos

- dispositivos de vigilancia, como CCTVs, para monitorear continuamente la instalación en busca de actividad sospechosa y registrar cada actividad para su uso futuro

Es importante tener en cuenta que aunque las contraseñas son una forma comúnmente utilizada de proteger los datos y los sistemas de información; no forman parte de los controles físicos de acceso en una instalación. Las contraseñas forman parte del mecanismo de autenticación de usuario.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender y aplicar los conceptos de gestión de riesgos

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Tipos de control de seguridad y gestión de riesgos

---

Pregunta #136 de 137

Id. de pregunta: 1111662

¿Qué organización es el comité coordinador para el diseño y la gestión de Internet?

✗ **A)** OLTP
✓ **B)** Iab
✗ **C)** IAC
✗ **D)** NCSC

explicación

La Junta de Arquitectura de Internet (IAB), que también se conoce como la Junta de Actividades de Internet, es responsable del diseño y la administración de Internet. El comité discute los temas relacionados con la arquitectura de Internet y administra el desarrollo de protocolos de Internet. El IAB designa al editor de solicitud de comentarios (RFC) y administra el Grupo de trabajo de ingeniería de Internet (IETF). El IAB considera lo siguiente como comportamiento poco ético:

- Tratar de obtener acceso no autorizado a los recursos de Internet
- Destrucción de la integridad de la información informática
- Interrumpir el uso previsto de Internet
- Desperdiciar recursos, incluidas las personas, la capacidad y los equipos, a través de estas acciones
- Comprometer la privacidad de los usuarios
- Ser negligente en la realización de experimentos de Internet

IAC no está asociado con el diseño y la gestión de Internet.

El procesamiento de transacciones en línea (OLTP) se utiliza generalmente cuando se agrupan varios sistemas de base de datos. Las transacciones se registran y confirman en tiempo real mediante OLTP. El propósito principal de OLTP es proporcionar resistencia y un alto nivel de rendimiento.

El Centro Nacional de Seguridad Informática (NCSC) es una agencia centralizada que evalúa los productos de seguridad informática y proporciona apoyo técnico a las oficinas gubernamentales y empresas privadas.

Los siguientes actos de individuos son considerados poco éticos por IAB:

- Acceso no autorizado a los recursos de Internet
- Interrupción de las actividades de Internet
- Despilfarro de recursos de Internet, como personas y ordenadores
- Destrucción de la integridad de la información
- Comprometer la privacidad de una persona
- Negligencia durante los experimentos de Internet

La IAB trabaja con agencias federales mediante el uso de procedimientos definidos y nuevas tecnologías para proteger Internet y hacerlo resistente a la interrupción.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender, adherirse y promover la ética profesional

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Internet Architecture Board

---

Pregunta #137 de 137

Id. de pregunta: 1104760

¿Cuáles son los objetivos de seguridad principales para la protección de los activos de información?

✗ **A)** riesgos, amenazas y vulnerabilidades
✗ **B)** riesgos, responsabilidades y vulnerabilidades
✓ **C)** confidencialidad, integridad y disponibilidad
✗ **D)** activos, pasivos y riesgos

explicación

La confidencialidad, la integridad y la disponibilidad son el núcleo de la protección de los activos de información de una organización. Estos tres objetivos también se conocen como la tríada de la CIA.

La disponibilidad incluye la capacidad de proporcionar redundancia y tolerancia a errores, de operar al nivel óptimo de rendimiento, la capacidad de hacer frente a vulnerabilidades y amenazas, como ataques DoS, y de recuperarse de interrupciones sin comprometer la seguridad y la productividad.

La integridad garantiza la corrección de los datos y la fiabilidad de la información, la protección de los datos y del sistema contra la alteración no autorizada, y la incapacidad de ataques y errores del usuario para afectar la integridad de los datos y del sistema.

La confidencialidad se define como el nivel mínimo de secreto mantenido para proteger la información confidencial de la divulgación no autorizada. La confidencialidad se puede implementar a través del cifrado, la clasificación de datos de control de acceso y la conciencia de seguridad. Mantener la confidencialidad de la información evita que una organización ataques, como el shoulder surf y la ingeniería social. Estos ataques pueden conducir a la divulgación de información confidencial y pueden interrumpir las operaciones comerciales.

Los riesgos, amenazas y vulnerabilidades se evalúan durante el curso del análisis de riesgos realizado por una organización. Durante un análisis de riesgo, un activo se valora en función de su sensibilidad y valor. La evaluación de riesgos, amenazas y vulnerabilidades proporciona una estimación de los controles que se deben colocar en una organización para lograr los objetivos de seguridad de una organización. Las técnicas comunes de recopilación de información utilizadas en el análisis de riesgos incluyen:

- Distribución de un cuestionario
- Empleo de herramientas automatizadas de evaluación de riesgos
- Revisión de los documentos de política existentes

El resto de las opciones no son válidas en términos de evaluación de seguridad y objetivos de seguridad de una organización.

Objetivo:
Seguridad y gestión de riesgos

Subobsecución:
Comprender y aplicar los conceptos de confidencialidad, integridad y disponibilidad

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 1: Seguridad y Gestión de Riesgos, confidencialidad, integridad y disponibilidad