Domain 7 - Security Operations

Test ID: 178688630

Pregunta #1 de 163

Id. de pregunta: 1192971

Su organización está considerando la posibilidad de alquilar un centro de datos externo para proporcionar recuperación de instalaciones si se produce un desastre. La administración desea arrendar un sitio frío. ¿Cuáles son algunas desventajas de este tipo de sitio?

a. gastos

b. tiempo de recuperación

c. tiempo de administración

d. Disponibilidad de las pruebas

A) opción A
B) opción b
C) Opción d
D) opción c
E) Opciones B y D
F) Opciones A y C

Pregunta #2 de 163

Id. de pregunta: 1111779

Se le ha pedido que reduzca el área expuesta de un equipo con Windows Server 2012 que actúa como servidor web. ¿Qué paso NO se incluye en la reducción de los ataques de área expuesta?

A) Deshabilite los servicios innecesarios.
B) Utilice privilegios mínimos.
C) Deshabilite los protocolos innecesarios.
D) Deshabilite la auditoría.

Pregunta #3 de 163

Id. de pregunta: 1105417

Se le ha pedido que proporcione una copia de un acuerdo contractual entre su organización y un tercero. ¿Qué tipo de evidencia representa este documento?

A) mejor evidencia
B) evidencia secundaria
C) pruebas de oídas
D) pruebas concluyentes

Pregunta #4 de 163

Id. de pregunta: 1111793

¿Qué principio estipula que no se deben realizar múltiples cambios en un sistema informático al mismo tiempo?

A) atención debida
B) Debida diligencia
C) uso aceptable
D) gestión de cambios

Pregunta #5 de 163

Id. de pregunta: 1114772

Como parte de la directiva de seguridad de su organización, debe supervisar las infracciones de control de acceso. ¿Qué método(s) debe(n) utilizar?

a. ACL

b. IDSs

c. Copias de seguridad

d. Registros de auditoría

A) Opción d
B) opción c
C) opción A
D) opción b
E) todas las opciones

F) Opciones B y D Sólo

G) opciones b, c y d solamente

Pregunta #6 de 163

Id. de pregunta: 1105413

Las pruebas deben ser legalmente permisibles en un tribunal de justicia y deben proporcionar una base para un caso. Todas las siguientes características de la evidencia son importantes, EXCEPTO:

A) suficiencia

B) Relevancia

C) confidencialidad

D) fiabilidad

Pregunta #7 de 163

Id. de pregunta: 1105521

¿Qué estipulación generalmente NO se proporciona en un contrato de proveedor fuera del sitio?

A) Probar la disponibilidad de la instalación fuera del sitio

B) plazo de disponibilidad de la instalación fuera del sitio

C) disponibilidad del sitio de la instalación fuera del sitio

D) ubicación específica de la instalación fuera del sitio

E) costo de la instalación fuera del sitio

Pregunta #8 de 163

Id. de pregunta: 1114780

¿Qué afirmación es cierta para el manejo de incidentes informáticos?

A) El equipo de respuesta a incidentes informáticos es responsable de la recuperación de un sistema.

B) En la investigación por parte del equipo de respuesta a incidentes informáticos debe participar un representante de la alta dirección.

C) El desarrollo del sistema se puede llevar a cabo mientras se maneja un incidente informático.

D) Los daños en un sistema después de que se produce un ataque se pueden reparar mientras se maneja un incidente informático.

Pregunta #9 de 163

Id. de pregunta: 1105489

¿Qué afirmación es cierta de una base informática de confianza (TCB)?

A) Un TCB garantiza que un sistema informático sea completamente seguro en todo momento.

B) Un TCB sólo direcciona el sistema operativo de un equipo.

C) El término TCB se originó a partir de las normas ITSEC.

D) Un TCB contiene el núcleo de seguridad y otros mecanismos de protección de seguridad.

Pregunta #10 de 163

Id. de pregunta: 1192961

Los usuarios informan de que el servidor de Terminal Server de Windows Server de su empresa está experimentando problemas de rendimiento. Tiene una línea de base de rendimiento para el servidor. Sospecha que el servidor de Terminal Server está bajo ataque de un pirata informático. ¿Qué herramienta debe utilizar para determinar si el rendimiento del servidor se ha degradado?

A) un escáner de puertos

B) una prueba de vulnerabilidad

C) un analizador de red

D) Monitor de sistema

Pregunta #11 de 163

Id. de pregunta: 1105498

¿Cuál es una descripción correcta de un sistema honeypot?

A) Un equipo utilizado para atraer a un atacante

B) Una herramienta utilizada para detectar alteraciones en los archivos de sistema

C) una metodología de prueba utilizada para revelar vulnerabilidades

D) Un tipo de ataque en el que el sistema de destino está inundado de solicitudes de servicio no autorizadas

---

Pregunta #12 de 163

Id. de pregunta: 1105406

Usted es el investigador de incidentes de su organización que realiza una investigación de incidentes de rutina. El siguiente paso que debe realizar es el análisis de red. ¿Cuál de los siguientes ejemplos se considera este tipo de análisis?

A) análisis de contenido

B) imágenes de disco

C) análisis de registros

D) ingeniería inversa

Pregunta #13 de 163

Id. de pregunta: 1105454

Su organización ha decidido implementar una columna vertebral dual. ¿Cuál es el propósito de esto?

A) Para proporcionar redundancia de controlador de disco duro

B) Para proporcionar redundancia de disco duro

C) Para proporcionar redundancia de servidor

D) para proporcionar redundancia de red de área local (LAN)

Pregunta #14 de 163

Id. de pregunta: 1105493

Su empresa ha implementado un sistema de detección de intrusiones basado en host (HIDS). Recientemente se ha preocupado por los problemas cuando se implementan estos sistemas. ¿Cuál es un problema importante al implementar este tipo de sistema?

A) Normalmente se ejecuta como un servicio o un proceso en segundo plano.

B) Se supervisa todo el tráfico de red entrante al host.

C) Debe implementarse en cada equipo que lo necesite.

D) Es difícil descubrir los archivos que han sido alterados por un ataque.

Pregunta #15 de 163

Id. de pregunta: 1114004

Un técnico de seguridad le informa de que un servidor de archivos está experimentando cargas de programa iniciales (IPL) no programadas. ¿Qué declaración explica MEJOR este problema?

A) El sistema está arrancando en modo de restauración del sistema.

B) El sistema está arrancando en la última configuración válida conocida.

C) El sistema se está reiniciando.

D) El sistema está arrancando en modo de usuario único.

Pregunta #16 de 163

Id. de pregunta: 1105421

Después de una reciente violación de seguridad de la red, reunió pruebas informáticas para usar para procesar a los sospechosos. ¿Qué condición debe cumplirse para que las pruebas sean admisibles en un tribunal de justicia?

A) El contenido de las pruebas informáticas siempre debe ser verificado por un experto en un tribunal de justicia.

B) La relevancia de la evidencia informática no es una preocupación primordial.

C) Las pruebas informáticas deben ser suficientes y fiables.

D) La evidencia informática debe ser descifrada antes de ser presentada en un tribunal de justicia.

Pregunta #17 de 163

Id. de pregunta: 1111768

Como parte de una investigación de incidentes, debe asegurarse de que la copia principal del medio original se almacena correctamente. Se deben completar todos los pasos siguientes, EXCEPTO:

A) Selle la copia principal en un contenedor y etiquete el contenedor para asegurarse de que la copia principal es segura.

B) Etiquete la copia principal con la fecha, la hora, las iniciales del recopilador y el número de caso, si corresponde.

C) Cifre la copia principal para asegurarse de que el contenido está protegido.

D) Selle el contenedor con cinta de evidencia y escriba en la cinta para asegurarse de que se pueda detectar un sello roto.

Pregunta #18 de 163

Id. de pregunta: 1114790

Debe documentar las directrices adecuadas que deben incluirse como parte de cualquier directiva de seguridad que implique al personal que viaja con dispositivos emitidos por la compañía. Se le ha dado una lista que debe incluirse en las directrices de la siguiente manera:

A. Dispositivos de transporte en equipaje facturado.

B. Utilice el cifrado cuando sea posible.

C. No deje el dispositivo desatendido.

D. No utilice redes WiFi.

¿Cuáles son las directrices válidas que deben incluirse como parte de las directrices para el personal?

A) Sólo B, C y D

B) Todas las directrices

C) Sólo B y C

D) Sólo A, B y C

Pregunta #19 de 163

Id. de pregunta: 1105494

Durante una auditoría de seguridad reciente de la red de su empresa, los contratistas sugirieron que los sistemas operativos de los equipos cliente no están suficientemente reforzados. ¿Qué pasos son cruciales para garantizar que un sistema operativo esté reforzado?

A) Configure todas las cuentas de usuario adecuadas.

B) Instale el software de monitoreo adecuado.

C) Deshabilite los servicios innecesarios.

D) Instale las herramientas administrativas adecuadas.

Pregunta #20 de 163

Id. de pregunta: 1105462

Los usuarios informan de que tienen problemas para acceder a varios servidores de la red de la organización. La causa de este problema debe ser determinada. ¿Quién debe solucionar este problema?

A) equipo de continuidad del negocio

B) equipo de operaciones

C) administrador del servidor

D) administrador de red

Pregunta #21 de 163

Id. de pregunta: 1105551

¿Qué afirmación es cierta de la iluminación de áreas críticas?

A) Las áreas críticas deben usar iluminación de emergencia y estar iluminadas de seis pies de altura a dos pies-velas.

B) Las áreas críticas deben usar iluminación de viaje y estar iluminadas de diez pies de altura a cuatro velas de pie.

C) Las áreas críticas deben usar iluminación continua y estar iluminadas de ocho pies de altura a dos velas de pie.

D) Las áreas críticas deben usar iluminación de reserva y estar iluminadas de diez pies de altura a dos velas de pie.

Pregunta #22 de 163

Id. de pregunta: 1114005

¿Cuál es el término para RAID 1 implementado con un solo controlador de disco duro?

A) creación de bandas de disco

B) duplicación de disco

C) creación de bandas de disco con paridad

D) espejado de disco

Pregunta #23 de 163

Id. de pregunta: 1105552

¿Qué opción NO es un control administrativo para la seguridad física?

A) gestión de instalaciones

B) control de personal

C) detección de intrusiones

D) respuesta y procedimientos de emergencia

Pregunta #24 de 163

Id. de pregunta: 1105424

Se ha producido una infracción de seguridad en el servidor de archivos de su organización. Como parte de una investigación de incidentes, se han creado dos copias de los medios originales. Se le ha pedido que cree resúmenes de mensajes para los archivos y directorios en el medio antes de que se analicen los datos.

¿Cuál es el propósito de esta acción?

A) para probar la confidencialidad de la imagen original

B) Para asegurarse de que el medio antiguo no contiene datos residuales

C) para demostrar la integridad de la imagen original

D) Para asegurarse de que el nuevo medio no contiene datos residuales

Pregunta #25 de 163

Id. de pregunta: 1105495

Su empresa implementa un honeypot como prevención de intrusiones. A la gerencia le preocupa que este honeypot se considere atrapamiento y le ha pedido que se asegure de que no se produzca el atrapamiento. ¿Qué situación debes prevenir?

A) permitir la navegación web en un honeypot

B) permitir descargas en un honeypot

C) puertos abiertos en un honeypot

D) servicios abiertos en un honeypot

Pregunta #26 de 163

Id. de pregunta: 1105520

¿Qué ocurre durante la fase de reconstitución de una recuperación?

A) Una organización vuelve a su sitio original

B) Una organización implementa la estrategia de recuperación

C) Una organización garantiza que sus instalaciones se restauren por completo en el sitio alternativo

D) Una organización realiza la transición a un sitio alternativo temporal

---

Pregunta #27 de 163

Id. de pregunta: 1114777

Está configurando los equipos servidor para una nueva empresa. Se le ha pedido que diseñe las listas de control de acceso (ACL) para los archivos y carpetas de los servidores. ¿Qué principios afectan al diseño?

un. Kerberos

b. SÉSAMO

c. necesidad de saber

d. Privilegio mínimo

e. inicio de sesión único

A) opción e

B) sólo opciones c, d y e

C) Sólo las opciones A y B

D) opción c

E) Opción d

F) opción A

G) Sólo las opciones C y D

H) opción b

Pregunta #28 de 163

Id. de pregunta: 1114009

¿Qué término es una estimación de la cantidad de tiempo que durará un equipo y generalmente es determinado por el proveedor del equipo o un tercero?

A) BCP

B) BIA

C) MTTR

D) MTBF

Pregunta #29 de 163

Id. de pregunta: 1105444

¿Qué declaración NO es una característica de un sistema de detección de intrusiones (NIDS) basado en red?

A) Un NIDS no supervisa las estaciones de trabajo individuales en una red.

B) Un NIDS supervisa el tráfico en tiempo real.

C) Un NIDS analiza la información cifrada.

D) Un NIDS analiza los paquetes de red en busca de intrusión.

Pregunta #30 de 163

Id. de pregunta: 1105490

¿Qué tipo de seguridad identifica el proceso de protección de los activos de información después de la implementación de la seguridad?

A) seguridad de las aplicaciones

B) seguridad física

C) seguridad de las operaciones

D) seguridad de control de acceso

Pregunta #31 de 163

Id. de pregunta: 1114771

Está realizando análisis de dispositivos integrados en un chip GPS en un teléfono móvil. Realizar hash criptográfico, crear sumas de comprobación y documentar toda la evidencia. ¿Qué fase del análisis de dispositivos integrados está realizando?

A) Colección

B) Presentación

C) Preservación

D) Análisis

Pregunta #32 de 163

Id. de pregunta: 1105423

¿A quién se le permite más probablemente dar pruebas de opinión en la corte?

A) un investigador de incidentes

B) un testigo

C) un experto

D) un oficial de la ley

Pregunta #33 de 163

Id. de pregunta: 1105434

Se le ha pedido que implemente un sistema que detecte los intentos de intrusión en la red y controle el acceso a la red para los intrusos. ¿Qué sistema debe implementar?

A) cortafuegos

B) IDENTIFICADORES

C) VPN

D) IPS

Pregunta #34 de 163

Id. de pregunta: 1114789

Desea asegurarse de que los empleados pueden utilizar un código para alertar a las autoridades correspondientes cuando están bajo coacción. ¿Con qué medida de seguridad física se puede utilizar?

a. Bloqueo de cifrado

b. Guardia de seguridad

c. bloqueo combinado

d. Sistema biométrico

A) opción c
B) opciones b, c y d
C) opción b
D) Opción d
E) opciones a, b y d
F) opción A
G) todas las opciones

Pregunta #35 de 163

Id. de pregunta: 1105437

La dirección de la empresa se ha preocupado recientemente por los problemas de seguridad que afectan a los empleados de la empresa. Se le ha pedido que mejore la responsabilidad del usuario mediante la supervisión de eventos del sistema. ¿Qué eventos de auditoría NO deben supervisarse?

A) modificaciones de la cuenta
B) intentos de inicio de sesión
C) creación de archivos
D) modificaciones de archivos

Pregunta #36 de 163

Id. de pregunta: 1114008

¿Qué plan garantiza que un puesto corporativo vital se llene en caso de que se desocupe durante un desastre?

A) plan de sucesión ejecutiva
B) plan de emergencia para ocupantes (OEP)

C) plan de continuidad de operaciones (COOP)

D) acuerdo recíproco

Pregunta #37 de 163

Id. de pregunta: 1192964

A su organización le preocupa que los usuarios no autorizados descarguen datos confidenciales en medios extraíbles. Usted decide cifrar los datos confidenciales de la empresa utilizando la función de cifrado del sistema operativo. ¿Qué garantiza esto?

A) Los datos están protegidos dondequiera que residan.

B) Los datos están protegidos mientras están en el medio original y en los medios extraíbles.

C) Los datos no están protegidos.

D) Los datos están protegidos mientras están en el medio original solamente.

Pregunta #38 de 163

Id. de pregunta: 1105539

¿Qué término se refiere a la cantidad de tiempo que una empresa puede tolerar la interrupción de un determinado activo, entidad o servicio?

A) tiempo de inactividad máximo tolerable

B) análisis de impacto en el negocio

C) tiempo medio entre el error

D) tiempo máximo de recuperación

E) tiempo medio de reparación

Pregunta #39 de 163

Id. de pregunta: 1105426

Ha establecido líneas de base de umbral de error de usuario para la red de su organización que le avisarán si se produce una actividad sospechosa. ¿Cómo se llaman las líneas de base?

A) registros de auditoría

B) privilegio mínimo

C) niveles de recorte

D) administración de la configuración

Pregunta #40 de 163

Id. de pregunta: 1114788

¿Qué sistema de detección de intrusiones (IDS) utiliza un campo magnético para detectar intrusiones?

A) un detector de proximidad

B) un sistema fotoeléctrico

C) un sistema de detección acústica

D) un sistema infrarrojo pasivo

Pregunta #41 de 163

Id. de pregunta: 1111765

¿Durante qué paso de la respuesta a incidentes se produce el análisis de causa raíz?

A) Informes

B) revisión

C) detección

D) recuperación

E) respuesta

Pregunta #42 de 163

Id. de pregunta: 1105447

¿Qué afirmación es cierta de un sistema de detección de intrusiones basado en red (NIDS)?

A) Un NIDS está activo mientras se recopilan datos a través de la red.

B) Un NIDS no puede detectar un intruso que ha iniciado sesión en un equipo host.

C) Un NIDS es finito cuando genera alarmas.

D) Un NIDS no analiza la información en tiempo real.

Pregunta #43 de 163

Id. de pregunta: 1105510

¿Cuál es el término para proporcionar tolerancia a fallos copiando el contenido de un disco duro a otro?

A) agrupamiento
B) INCURSIÓN
C) intercambio en caliente
D) Espejado

Pregunta #44 de 163

Id. de pregunta: 1111797

¿Qué cubre el último paso de un plan de continuidad del negocio?

A) capacitación del personal
B) Probar el plan
C) analizar los riesgos
D) actualizar el plan

Pregunta #45 de 163

Id. de pregunta: 1105468

¿Cuál es el objetivo principal de la gestión de privilegios?

A) para garantizar una estructura de presentación de informes adecuada
B) Para evaluar la pertenencia a grupos
C) Para garantizar la administración de contraseñas
D) Para garantizar el control sobre los permisos de usuario y los derechos de acceso

Pregunta #46 de 163

Id. de pregunta: 1111770

Durante una investigación de incidente reciente, extrajo datos ocultos de la imagen de datos que se creó. ¿En qué paso del proceso de investigación de incidentes estuvo involucrado?

A) colección

B) examen

C) preservación

D) identificación

Pregunta #47 de 163

Id. de pregunta: 1105503

¿Quién es responsable de aprobar las solicitudes de cambio?

A) tablero de control de cambios

B) propietario del activo

C) administrador de cambios

D) cambiar de propietario

Pregunta #48 de 163

Id. de pregunta: 1111766

Su organización ha sido víctima recientemente de un ataque de red. ¿Quién realiza los procedimientos de emergencia en respuesta a este ataque?

A) el equipo de respuesta a incidentes

B) el equipo de seguridad cibernética

C) el equipo de detección de intrusiones

D) el equipo de prevención de incidentes

Pregunta #49 de 163

Id. de pregunta: 1192973

¿Cuál de los siguientes ejercicios de continuidad de las actividades puede ser bastante complicado y debe realizarse anualmente?

A) ejercicio de sobremesa

B) pruebas de simulación de desastres

C) simulacro de evacuación de emergencia

D) tutorial estructurado

Pregunta #50 de 163

Id. de pregunta: 1192962

¿Qué principio de control de acceso garantiza que una función determinada tenga más de una persona capacitada para desempeñar sus funciones?

A) privilegio mínimo

B) separación de funciones

C) rotación de trabajos

D) denegar implícita

Pregunta #51 de 163

Id. de pregunta: 1105523

¿Qué elemento del plan de continuidad de las actividades se ocupa principalmente de minimizar los daños a la propiedad y prevenir la pérdida de vidas?

A) análisis de impacto en el negocio (BIA)

B) análisis del riesgo

C) plan de recuperación ante desastres

D) análisis de vulnerabilidades

Pregunta #52 de 163

Id. de pregunta: 1113997

La policía local se pone en contacto con usted con respecto a un delito informático reciente. Usted proporciona evidencia a los investigadores. Los investigadores le dicen que la evidencia que usted proporcionó es evidencia corroborativa. ¿Qué afirmación es cierta de este tipo de evidencia?

A) Le permite probar un punto o una idea.

B) Siempre actúa como evidencia concreta.

C) A veces se puede usar solo.

D) Debe ser controlado por múltiples fuentes.

Pregunta #53 de 163

Id. de pregunta: 1113995

La red de su organización fue atacada recientemente. Durante el ataque, los hackers robaron información valiosa y patentada. Se le ha pedido que proporcione información que sea admisible como prueba en un tribunal de justicia para procesar a los sospechosos. ¿Qué debe proporcionar?

A) copias de datos de disco duro

B) volcados de memoria

C) Contraseñas

D) nombres de inicio de sesión de usuario

Pregunta #54 de 163

Id. de pregunta: 1105456

Un usuario hereda un permiso basado en su pertenencia a grupos. ¿Qué tipo de derecho se ha aplicado?

A) derecho explícito

B) derecho de acceso

C) capacidad

D) derecho implícito

Pregunta #55 de 163

Id. de pregunta: 1111782

¿Cuál es el primer paso del ciclo de vida del equipo?

A) Evaluación

B) Adquisición e implementación

C) Administración

D) Jubilación

Pregunta #56 de 163

Id. de pregunta: 1105425

Usted es el investigador de incidentes de su organización. Debe crear dos imágenes del disco duro de un servidor de archivos. Los procedimientos de investigación de incidentes indican que debe asegurarse de que los nuevos medios se purgan correctamente.

¿Qué debe hacer para cumplir con este requisito?

A) Asegúrese de que el nuevo medio tiene el formato correcto.

B) Asegúrese de que el nuevo medio no contiene ningún dato residual.

C) Asegúrese de que el nuevo medio esté correctamente etiquetado.

D) Asegúrese de que se crean resúmenes de mensaje de los datos copiados.

Pregunta #57 de 163

Id. de pregunta: 1105508

¿Qué solución tolerante a fallos es la más costosa de implementar?

A) Racimos

B) INCURSIÓN

C) Backups

D) controladores de disco redundantes

Pregunta #58 de 163

Id. de pregunta: 1192965

¿Cuáles de los siguientes deben ser miembros del Equipo de respuesta a incidentes de seguridad informática (CSIRT)?

a. Miembro del departamento de TI

B. Miembro del departamento legal

c. Miembro del departamento de relaciones públicas

d. Miembro del equipo directivo

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

Pregunta #59 de 163

Id. de pregunta: 1114775

¿Qué afirmaciones con respecto a una pista de auditoría NO son ciertas?

un. Una pista de auditoría es un control preventivo.

B. Una pista de auditoría ayuda en la detección de intrusiones.

c. Una pista de auditoría no registra los intentos de inicio de sesión correctos.

d. Una pista de auditoría establece la responsabilidad por el control de acceso.

E. Una pista de auditoría no se revisa tan pronto como se detecta una intrusión.

A) opciones b, d y e
B) opción e
C) opciones a, c y e
D) opción A
E) opción b
F) Opción d
G) opción c

Pregunta #60 de 163

Id. de pregunta: 1105476

Como miembro del equipo de seguridad de su organización, está examinando todos los aspectos de la seguridad de las operaciones de la red. Debe determinar las contramedidas que se pueden utilizar en la seguridad de las operaciones. Ya ha examinado los recursos y la información que deben protegerse. ¿Cuál es el tercer tipo de activo que debe examinarse?

A) personal

B) servidores de red

C) medios de red

D) hardware

Pregunta #61 de 163

Id. de pregunta: 1192974

Su organización tiene una caja fuerte para almacenar equipos portátiles corporativos cuando no se están utilizando. Como parte del plan de seguridad, debe asegurarse de que la caja fuerte enganche un bloqueo adicional si la temperatura de la caja fuerte excede un cierto nivel. Esto proporcionará protección contra la perforación. ¿Qué tipo de bloqueo debe implementar?

A) rebloqueo activo

B) relock térmico

C) relock pasivo

D) bloqueo de ranura

Pregunta #62 de 163

Id. de pregunta: 1105524

Un terremoto dañó el edificio que alberga el centro de datos de su organización. Como resultado, el sitio alternativo en Nueva Jersey debe configurarse y ponerse en línea. ¿Qué equipo debería ser responsable de esto?

A) equipo de evaluación de daños

B) equipo de restauración

C) equipo de salvamento

D) equipo de seguridad

Pregunta #63 de 163

Id. de pregunta: 1105438

Su empresa supervisa varios eventos para asegurarse de que la seguridad de los servidores no se ve comprometida y que el rendimiento de los servidores se mantiene dentro de ciertos umbrales.

Un consultor de seguridad ha sido contratado por su empresa para analizar las medidas de seguridad de la organización. El consultor ha solicitado acceso a los registros de supervisión de seguridad. Debe limitar la cantidad de información del registro de auditoría que proporciona descartando la información que no necesita el consultor. ¿Qué herramienta debe utilizar?

A) herramienta de detección de varianza

B) filtro de auditoría

C) herramienta de detección de firmas de ataques

D) herramienta de reducción de auditoría

Pregunta #64 de 163

Id. de pregunta: 1105457

¿Qué es un término que es sinónimo de etiqueta de seguridad?

A) tabla de capacidades

B) lista de control de acceso (ACL)

C) etiqueta de confidencialidad

D) regla

Pregunta #65 de 163

Id. de pregunta: 1192967

¿Qué afirmación es cierta para el modo de seguridad dedicado?

A) Algunos usuarios tienen la autorización y la aprobación formal necesarias para acceder a todos los datos.

B) Algunos usuarios tienen la autorización y la aprobación formal necesarias para acceder a algunos de los datos.

C) Todos los usuarios tienen la autorización y la aprobación formal necesarias para acceder a todos los datos.

D) Todos los usuarios tienen la autorización y la aprobación formal necesarias para acceder a algunos de los datos.

Pregunta #66 de 163

Id. de pregunta: 1192969

Su organización implementa un esquema de copia de seguridad completa/diferencial. Una copia de seguridad completa se completó hace dos días. Ayer se completó una copia de seguridad diferencial. ¿Qué archivos se respaldaron ayer?

A) Todos los archivos de un conjunto de copia de seguridad que se cambiaron o crearon desde la última copia de seguridad completa

B) Todos los archivos de un conjunto de copia de seguridad que se cambiaron o crearon desde la última copia de seguridad incremental

C) Todos los archivos de un conjunto de copia de seguridad

D) Todos los archivos de un conjunto de copia de seguridad que se cambiaron o crearon desde la última copia de seguridad diferencial

---

Pregunta #67 de 163

Id. de pregunta: 1105526

¿Qué instalación de copia de seguridad es propiedad de la empresa y se puede en línea con relativa facilidad?

A) sitio frío

B) sitio redundante

C) sitio cálido

D) sitio caliente

Pregunta #68 de 163

Pregunta con id.: 1114000

Como parte del mantenimiento de rutina, su organización requiere que los administradores del sistema realicen una revisión y auditoría de acceso de rutina. Como parte de este proceso, decide auditar el acceso de los usuarios a archivos y carpetas. ¿Qué directiva de auditoría de Windows debe habilitar?

A) Acceso al servicio de directorio

B) Eventos de inicio de sesión de cuenta

C) Eventos de inicio de sesión

D) Acceso a objetos

Pregunta #69 de 163

Id. de pregunta: 1105415

Usted está realizando una investigación forense de una reciente violación de la seguridad informática. Se le ha pedido que utilice imágenes de disco para crear una copia del contenido de un disco duro. ¿Qué afirmación es cierta de las imágenes de disco cuando se realiza en una investigación forense?

A) Una copia a nivel de bytes del disco ayuda en la investigación forense.

B) Una copia a nivel de bits del disco ayuda en la investigación forense.

C) No se debe volcar el contenido de la memoria.

D) Se debe utilizar la copia original del disco.

Pregunta #70 de 163

Id. de pregunta: 1105549

Su centro de datos tiene su propio bloqueo para evitar la entrada. El plan de seguridad de su organización indica que el bloqueo del centro de datos debe ser programable. ¿Qué tipo de bloqueo debe utilizar?

A) bloqueo mecánico

B) cerradura del vaso

C) cerradura de combinación

D) bloqueo de cifrado

Pregunta #71 de 163

Id. de pregunta: 1105431

Su empresa ha decidido implementar la supervisión basada en anomalías en la red. Obtendrá un nuevo servidor que realizará esta supervisión. Debe asegurarse de que la supervisión es eficaz. Para que este tipo de supervisión sea eficaz, ¿qué debe existir?

A) reglas

B) una base de datos

C) una línea de base

D) respuestas activas y pasivas

Pregunta #72 de 163

Id. de pregunta: 1111777

¿Qué actividad NO es una función de un sistema de detección de intrusiones (IDS)?

A) detección de variación del patrón normal

B) detección y respuesta a intrusiones

C) verificación de sólo las amenazas dentro de la red

D) detección y notificación de anomalías

Pregunta #73 de 163

Id. de pregunta: 1105465

Se le han dado varias sugerencias para aplicar el principio de privilegios mínimos. ¿Cuál es la mejor implementación de este principio?

A) Asegúrese de que todos los servicios utilizan la cuenta administrativa principal para ejecutar sus procesos.

B) Emita el mandato Ejecutar como para ejecutar tareas administrativas durante una sesión de usuario normal.

C) Completar tareas administrativas en un equipo que funciona sólo como un servidor.

D) Emitir una sola cuenta a cada usuario, independientemente de su función de trabajo.

Pregunta #74 de 163

Id. de pregunta: 1111795

Al desarrollar el plan de continuidad del negocio, su equipo debe crear un plan que garantice que el funcionamiento normal se pueda reanudar de manera oportuna. ¿Qué elemento está creando tu equipo?

A) análisis de vulnerabilidades

B) plan de continuidad del negocio

C) análisis de impacto en el negocio (BIA)

D) plan de recuperación ante desastres

Pregunta #75 de 163

Id. de pregunta: 1114783

¿Cuáles son algunas de las áreas en las que los empleados deben ser capacitados para que sigan los procedimientos cuando ocurre un desastre?

a. Procedimientos de restauración

b. Procedimientos de evacuación

c. Procedimientos de investigación

d. Procedimientos de comunicación

A) Opción d

B) opción b

C) opciones a, b y d

D) opciones a, b y c

E) opciones b, c y d

F) opción A

G) opción c

Pregunta #76 de 163

Id. de pregunta: 1111773

¿Qué afirmación es cierta de una investigación de delitos informáticos?

A) La evidencia no es fácil de modificar durante la investigación.

B) La evidencia no es importante desde una perspectiva legal.

C) El equipo de respuesta a incidentes de la compañía a veces no está dispuesto a involucrar a las autoridades policiales.

D) El costo de la investigación a menudo resulta ser un elemento disuasorio antes de que comience la investigación.

Pregunta #77 de 163

Id. de pregunta: 1105477

¿Qué bloqueo de dispositivo impide el acceso a discos duros o puertos no utilizados en un equipo?

A) control del interruptor periférico

B) bloqueo de ranura

C) trampa de cable

D) control del interruptor

E) control portuario

Pregunta #78 de 163

Id. de pregunta: 1105548

¿Cuál de los siguientes NO es un tipo de bloqueo mecánico?

A) warded

B) nivel

C) oblea

D) anclar

Pregunta #79 de 163

Id. de pregunta: 1105429

Se le ha pedido que supervise el tráfico de la red. Al investigar los diferentes métodos de monitoreo, se preocupa por la supervisión que requiere actualizaciones periódicas para garantizar su eficacia. ¿Qué tipo de supervisión requiere que las actualizaciones se obtengan regularmente para garantizar su eficacia?

A) basado en firmas

B) basado en anomalías

C) basado en el comportamiento

D) basado en red

Pregunta #80 de 163

Id. de pregunta: 1111776

¿Qué elemento NO es un componente funcional de un sistema de detección de intrusiones (IDS)?

A) fuente de información
B) componente de base de datos
C) análisis de informes de eventos
D) respuesta
E) detector de intrusiones estadísticas

Pregunta #81 de 163

Id. de pregunta: 1114003

La administración le ha pedido que implemente un honeypot. ¿Dónde debe residir este equipo?

A) en la red pública
B) sobre la zona de distensión (DMZ)
C) en la red privada
D) en la red privada virtual (VPN)

Pregunta #82 de 163

Id. de pregunta: 1113996

Está recopilando evidencia de un incidente de seguridad reciente en su organización. Debe copiar el medio original. ¿Cuál es el número mínimo de copias que debe hacer?

A) 1
B) 2
C) 3
D) 4

Pregunta #83 de 163

Id. de pregunta: 1105511

Debe proteger los datos de las redes informáticas de los picos de energía. ¿Qué debes usar?

A) un aspersor

B) una tarjeta clave

C) un sistema de calefacción

D) un supresor de sobretensiones

Pregunta #84 de 163

Pregunta con ID: 1105500

Recibe un correo electrónico no solicitado de un proveedor de la aplicación que indica que una revisión de seguridad está disponible para la aplicación. La directiva de seguridad de su empresa establece que todas las aplicaciones deben actualizarse con revisiones de seguridad y Service Packs. ¿Qué debes hacer?

A) Inserte el CD de instalación de la aplicación para instalar la revisión de seguridad.

B) Vaya al sitio Web del proveedor para descargar la revisión de seguridad.

C) Haga clic en el vínculo incrustado en el mensaje de correo electrónico para instalar la revisión de seguridad.

D) Haga clic en el vínculo incrustado en el mensaje de correo electrónico para probar la revisión de seguridad.

Pregunta #85 de 163

Id. de pregunta: 1111778

Se le ha encomendado la tarea de diseñar la directiva de auditoría para su empresa en función de la directiva de seguridad de su empresa. ¿Cuál es el primer paso que debes dar?

A) Realizar la auditoría.

B) Informar de los resultados de la auditoría a la administración.

C) Planee la estrategia de auditoría.

D) Evaluar los resultados de la auditoría.

Pregunta #86 de 163

Id. de pregunta: 1105532

Su organización está investigando instalaciones informáticas alternativas para asegurarse de que la organización puede funcionar si se destruye la instalación principal. ¿Cuál es la consideración más importante a la hora de elegir una instalación informática alternativa?

A) recursos disponibles

B) cantidad de tiempo necesario

C) costar

D) ubicación

Pregunta #87 de 163

Id. de pregunta: 1111769

Cerca del final de una investigación de incidente reciente, el investigador de incidentes sugiere que su organización tome varias contramedidas recomendadas. ¿Qué etapa del proceso de investigación se está llevando a cabo?

A) colección

B) análisis

C) presentación

D) examen

Pregunta #88 de 163

Id. de pregunta: 1111792

Está implementando software antivirus en la red de su organización. Todas las siguientes son directrices con respecto al software antivirus, EXCEPTO:

A) Configure el software antivirus para analizar automáticamente los discos externos.

B) Configure los análisis antivirus para que se produzcan automáticamente según una programación definida.

C) Actualice las firmas antivirus sólo a través de un servidor local.

D) Instale el software antivirus en todos los equipos servidor, equipos cliente, puntos de entrada de red y dispositivos móviles.

Pregunta #89 de 163

Id. de pregunta: 1114781

Recientemente, un empleado de su organización realizó copias ilegales de la propiedad intelectual de su organización. Esto es una violación directa de las políticas de empleo de su organización. Debe crear un equipo de respuesta a incidentes para investigar el delito.

¿Quién NO debe ser parte de un equipo de respuesta a incidentes?

a. Departamento de recursos humanos

b. un departamento de Relaciones Públicas

c. Personal directivo superior

d. Gobierno federal

e. Departamento de Tecnología de la Información

A) opciones A y B
B) opción e
C) Opciones B y D
D) opción A
E) opción b
F) opción c
G) Opción d
H) Opciones C y E

Pregunta #90 de 163

Id. de pregunta: 1105491

Como jefe de departamento de TI, debe garantizar una alta disponibilidad y rendimiento para la red de su organización. También debe asegurarse de que la red es segura. ¿Cuál es la relación entre el rendimiento de la red y la seguridad?

A) Cuando se aumentan los mecanismos de seguridad, no tiene ningún efecto en el rendimiento.
B) Cuando se aumentan los mecanismos de seguridad, el rendimiento suele disminuir.
C) La seguridad siempre debe tener una prioridad más alta que el rendimiento.

D) Cuando se aumentan los mecanismos de seguridad, el rendimiento suele aumentar.

Pregunta #91 de 163

Id. de pregunta: 1105420

Durante una investigación reciente de una brecha de seguridad de la red, el equipo de respuesta a incidentes reunió pruebas de oídas. ¿Qué afirmación es cierta de este tipo de evidencia?

A) Las pruebas de oídas no siempre son admisibles en el tribunal de justicia.

B) Las pruebas de oídas sólo se refieren a las pruebas orales.

C) Las pruebas de oídas se consideran suficientes para procesar a un sospechoso.

D) La evidencia de oídas es siempre una prueba de primera mano de información confiable.

Pregunta #92 de 163

Id. de pregunta: 1114774

¿Qué elementos NO complementan un sistema de detección de intrusiones (IDS)?

a. sistema de análisis de vulnerabilidades

b. sensores

c. honeypots

d. Celdas acolchadas

e. Software de monitoreo centralizado

A) Opción d

B) opción A

C) opción c

D) opción e

E) Opciones C y D

F) opciones A y B

G) opciones B y E

H) opción b

Pregunta #93 de 163

Id. de pregunta: 1105467

¿Qué instrucción describe mejor un control de dos hombres?

A) Un operador controla más de una posición dentro de una organización.

B) Las responsabilidades de un usuario de equipo y un administrador del sistema están segregadas.

C) Dos operadores revisan y aprueban el trabajo del otro.

D) Dos operadores trabajan juntos para completar una tarea determinada.

Pregunta #94 de 163

Id. de pregunta: 1111780

¿En qué momento se debe agregar un cambio de configuración al registro de cambios?

A) Una vez implementado el cambio

B) Después de probar el cambio

C) Una vez aprobado el cambio

D) Una vez solicitado el cambio

Pregunta #95 de 163

Id. de pregunta: 1105410

¿Qué tipo de prueba negará la necesidad de presunciones en el tribunal de justicia?

A) evidencia corroborativa

B) evidencia directa

C) evidencia secundaria

D) pruebas de oídas

Pregunta #96 de 163

Id. de pregunta: 1105412

Para investigar delitos informáticos, ¿con qué agencia trabaja el FBI?

A) Interpol y NSA

B) Cia y Comisión Europea

C) Departamento de Defensa

D) Servicio Secreto y aplicación de la ley local

Pregunta #97 de 163

Id. de pregunta: 1114001

¿Qué se entiende por MTBF?

A) la cantidad estimada de tiempo que se tardará en reemplazar un equipo

B) la cantidad estimada de tiempo que un equipo debe permanecer operativo antes de la falla

C) la cantidad estimada de tiempo que se tardará en reparar un equipo cuando se produzca un fallo

D) la cantidad estimada de tiempo que se utilizará un equipo antes de que deba reemplazarse

---

Pregunta #98 de 163

Id. de pregunta: 1192966

Coincide con las descripciones de la izquierda con los tipos de malware a la derecha.

{UCMS id=5736282464452608 type=Activity}

Pregunta #99 de 163

Id. de pregunta: 1111789

Como parte del equipo de respuesta a incidentes, se le ha entregado un documento de procedimientos que identifica los pasos que debe completar durante una investigación forense.

¿Cuándo se debe completar el paso de recolección de evidencia?

A) después de que la evidencia se haya conservado solamente

B) después de que se haya identificado el incidente y se hayan conservado las pruebas

C) Sólo después de que se haya identificado el incidente

D) después de que se ha identificado el incidente, la evidencia se ha conservado, y la evidencia ha sido analizada

---

Pregunta #100 de 163

Id. de pregunta: 1111774

¿Qué problema se supervisa mejor mediante el registro de la carga de la CPU y el uso de memoria?

A) Problema de servidor de seguridad

B) problema de seguridad

C) problema de uso del tiempo de inactividad

D) problema de rendimiento

Pregunta #101 de 163

Id. de pregunta: 1111771

¿Cuál es el término para el proceso de recopilación, análisis y preservación de evidencia?

A) cadena de custodia

B) cadena de evidencia

C) manejo de incidentes

D) procedimiento legal

Pregunta #102 de 163

Id. de pregunta: 1105533

¿Qué sitio suele tardar más en configurarse cuando es necesario?

A) sitio redundante

B) sitio cálido

C) sitio caliente

D) sitio frío

Pregunta #103 de 163

Id. de pregunta: 1105507

Su organización está implementando un nuevo servidor de archivos. Se le ha pedido que implemente un subsistema de disco que es un sistema de disco resistente a errores (FRDS).

¿Qué criterio debe cumplir este sistema?

A) Protege contra la pérdida de acceso a los datos debido a un corte de energía externo.

B) Protege contra la pérdida de acceso a los datos debido a fallas en la fuente de alimentación.

C) Protege contra la pérdida de datos debido a un corte de energía externo.

D) Protege contra la pérdida de datos debido a fallas en la unidad de disco.

Pregunta #104 de 163

Id. de pregunta: 1105405

¿Qué parte de un sistema informático debe ser inspeccionada en busca de archivos y datos ocultos?

A) espacio de bits

B) espacio reducido

C) espacio de custodia

D) espacio de holgura

Pregunta #105 de 163

Id. de pregunta: 1105492

Acaba de recibir una alerta de que se ha detectado un intento de intrusión en la red. Es necesario lanzar las contramedidas iniciales para este ataque. ¿Qué acción NO se recomienda como contramedida inicial?

A) Realizar las actividades necesarias para contener la intrusión.

B) Notifique al equipo de respuesta a incidentes.

C) Lanzar un contraataque contra el intruso.

D) Configure el IDS para caer los paquetes que son malévolos en naturaleza.

Pregunta #106 de 163

Id. de pregunta: 1105440

Al examinar los informes de rendimiento de los recursos de la organización, observa un aumento significativo del rendimiento en el servidor de archivos de la organización. El registro del servidor indica que se actualizaron la memoria y el disco duro del servidor de archivos. Como miembro del equipo de operaciones, ¿qué debe hacer?

A) Continúe supervisando el rendimiento del servidor de archivos.

B) Investigue el aumento del rendimiento del servidor de archivos.

C) Diagnostique el aumento del rendimiento del servidor de archivos.

D) Cree una nueva línea base de rendimiento para el servidor de archivos.

Pregunta #107 de 163

Id. de pregunta: 1111784

¿Qué funciones NO están asociadas en un entorno correctamente segregado?

A) autorización de acceso y auditoría

B) desarrollo de sistemas y mantenimiento de sistemas

C) entrada de datos y programación de trabajos

D) administración de seguridad y control de calidad

Pregunta #108 de 163

Id. de pregunta: 1105512

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

A) Dos

B) Uno

C) Cuatro

D) Tres

Pregunta #109 de 163

Id. de pregunta: 1111781

¿Qué proceso incluye la auditoría y el seguimiento de los cambios realizados en la base informática de confianza?

A) administración de la configuración

B) controles de entrada y salida

C) controles multimedia

D) controles del sistema

Pregunta #110 de 163

Id. de pregunta: 1114786

¿Cuáles son los principales tipos de cerraduras mecánicas?

a. Bloqueos combinados

b. Bloqueos de cifrado

c. cerraduras de tutela

d. Cerraduras del vaso

A) opción A

B) Opciones C y D

C) opción b

D) opción c

E) opciones A y B

F) Opción d

Pregunta #111 de 163

Id. de pregunta: 1105501

¿Qué tipo de actualización realiza reparaciones en un equipo durante su funcionamiento normal para que el equipo pueda seguir funcionando hasta que se pueda realizar una reparación permanente?

A) parche

B) Service Pack

C) revisión

D) paquete de soporte técnico

Pregunta #112 de 163

Id. de pregunta: 1105528

Durante el análisis de impacto en el negocio (BIA), el comité de continuidad del negocio identifica un servidor que tiene un tiempo de inactividad máximo tolerable (MTD) de 48 horas. ¿En qué categoría de tiempo de inactividad máximo tolerable (MTD) debe colocarse este sistema?

A) importante

B) crítico

C) accidental

D) normal

E) urgente

Pregunta #113 de 163

Id. de pregunta: 1114778

Como parte de la nueva iniciativa de seguridad de su organización, debe asegurarse de que todos los sistemas están reforzados. ¿Qué debes hacer?

un. Quite todas las aplicaciones innecesarias.

B. Quite o deshabilite todos los servicios innecesarios.

c. Configurar los servicios de aplicación para que usen la misma cuenta sin privilegios.

d. Configurar los servicios de base de datos para que usen una cuenta sin privilegios.

A) opción c

B) Opción d

C) opciones a, b y c

D) opción b

E) opciones a, b y d

F) opción A

G) todas las opciones

Pregunta #114 de 163

Id. de pregunta: 1105419

Durante una investigación forense reciente, varios resúmenes del mensaje fueron obtenidos. ¿Cuál es la principal desventaja de usar esta evidencia?

A) marca de tiempo modificada

B) autenticación estricta

C) tiempo de acceso más lento

D) procesamiento más rápido

Pregunta #115 de 163

Id. de pregunta: 1105463

¿Qué acuerdo le permite identificar actividades fraudulentas al permitir que un empleado desempeñe más de un rol en la organización?

A) separación de funciones

B) rotación de trabajos

C) control dual

D) vacaciones obligatorias

Pregunta #116 de 163

Id. de pregunta: 1114784

El comité de continuidad del negocio ha desarrollado el análisis de impacto en el negocio (BIA), ha identificado los controles preventivos que se pueden implementar y ha desarrollado las estrategias de recuperación. A continuación, el comité debería desarrollar un plan de contingencia.

¿Qué equipos deben incluirse en el desarrollo de este plan para ayudar en la ejecución del plan final?

a. equipo de restauración

b. Equipo de evaluación de daños

c. Equipo de salvamento

d. Equipo de gestión de riesgos

e. Equipo de respuesta a incidentes

A) opción b
B) opciones a, d y e
C) opción e
D) Opción d
E) opción A
F) opción c
G) opciones a, b y c

Pregunta #117 de 163

Id. de pregunta: 1114776

¿Qué tecnologías se consideran tecnologías de teleobservación?

a) Aeronaves no tripuladas

b) Aeronaves tripuladas

c. Satélites

d. Cámaras terrestres

A) Opción d
B) opción b
C) opción c
D) opción A
E) opciones a, b y c
F) opciones b, c y d
G) todas las opciones

Pregunta #118 de 163

Id. de pregunta: 1105432

Está creando una solución de supervisión para la red de su empresa. Defina una regla que impida que un cliente de correo electrónico ejecute el comando cmd.exe y le avise cuando se intente. ¿Qué tipo de monitoreo está utilizando?

A) basado en firmas

B) basado en la detección de uso indebido

C) basado en el comportamiento

D) basado en anomalías

Pregunta #119 de 163

Id. de pregunta: 1105464

Ha recibido una lista de usuarios y sus trabajos. Debe implementar el principio de privilegios mínimos. ¿Cuál es el siguiente paso que se debe realizar?

A) Configure los privilegios adecuados para la cuenta del usuario.

B) Determine el conjunto mínimo de privilegios necesarios para realizar el trabajo del usuario.

C) Configure las pertenencias a grupos adecuadas para la cuenta del usuario.

D) Determine el conjunto máximo de privilegios necesarios para realizar el trabajo del usuario.

Pregunta #120 de 163

Id. de pregunta: 1105409

¿Qué afirmación es cierta de la evidencia circunstancial?

A) Ayuda a probar un punto o una idea.

B) Se basa en documentos originales para probar un hecho.

C) Prueba directamente un hecho y no requiere corroboración.

D) Requiere inferencia a partir de los hechos de que se tenga acceso.

Pregunta #121 de 163

Pregunta con id.: 1105400

Un empleado es sospechoso de actividad delictiva que implica el acceso a datos en exceso de la autoridad del empleado. Usted ha obtenido la copia original firmada del acuerdo de no derecho a la privacidad que el empleado firmó cuando fue contratado. ¿Qué tipo de evidencia es este acuerdo?

A) mejor evidencia

B) pruebas de oídas

C) evidencia secundaria

D) evidencia corroborativa

Pregunta #122 de 163

Id. de pregunta: 1105448

Recientemente ha sido contratado como administrador de seguridad de su organización. Se le han dado varios informes de seguridad. Uno de los informes muestra información estadística del detector de anomalías de la organización. ¿Cuál es la tarea principal de este sistema?

A) Para identificar cuellos de botella en segmentos de red

B) identificar el uso de los recursos de la red y establecer la rendición de cuentas

C) para identificar la actividad anormal

D) para identificar la actividad legítima

Pregunta #123 de 163

Id. de pregunta: 1105430

Se le ha pedido que implemente la supervisión de red que detecta cualquier cambio o desviación en el tráfico de red. Al configurar la supervisión, se establecen líneas de base de tráfico de red. ¿Qué tipo de monitoreo está implementando?

A) basado en el comportamiento

B) basado en firmas

C) basado en anomalías

D) basado en red

Pregunta #124 de 163

Id. de pregunta: 1113999

¿Qué tipo de sistema de detección de intrusiones (IDS) es un detector de mal uso?

A) IDS de control de acceso

B) IDS basados en el tiempo

C) IDS basados en firmas

D) IDS basados en el comportamiento

Pregunta #125 de 163

Id. de pregunta: 1105513

Administrar una pequeña red corporativa. El viernes por la noche, después del cierre de los negocios, realizó una copia de seguridad completa del disco duro de uno de los servidores de la compañía. El lunes por la noche, realizó una copia de seguridad diferencial del disco duro del mismo servidor y los martes, miércoles y jueves por la noche realizó copias de seguridad incrementales del disco duro del servidor.

¿Qué archivos se registran en la copia de seguridad que realizó el jueves?

A) Todos los archivos del disco duro que se cambiaron o crearon desde la copia de seguridad incremental del martes

B) Todos los archivos del disco duro

C) Todos los archivos del disco duro que se cambiaron o crearon desde la copia de seguridad diferencial del lunes

D) Todos los archivos del disco duro que se cambiaron o crearon desde la copia de seguridad incremental del miércoles

---

Pregunta #126 de 163

Id. de pregunta: 1111802

Haga coincidir las descripciones de la derecha con los ataques de ingeniería social de la izquierda.

{UCMS id=5678026064920576 type=Activity}

Pregunta #127 de 163

Id. de pregunta: 1114006

Durante un desastre natural reciente, se destruyó la ubicación principal de su organización. Para poner en línea el sitio alternativo, primero ha restaurado los sistemas más críticos. Ahora se ha completado un nuevo sitio primario y debe asegurarse de que el sitio se pone en línea de forma ordenada. ¿Qué debes hacer primero?

A) Restaure todas las funciones interdependientes en el nuevo sitio primario.

B) Restaure todas las funciones independientes en el nuevo sitio primario.

C) Restaure las funciones menos críticas en el nuevo sitio primario.

D) Restaure las funciones más críticas en el nuevo sitio primario.

Pregunta #128 de 163

Id. de pregunta: 1105436

La red de su empresa ha sido violada. Durante la violación, el atacante elimina los datos incriminatorios de los registros de auditoría de su empresa para evitar el enjuiciamiento. ¿Cómo se llama este proceso?

A) limpieza

B) claro

C) Eliminar

D) Fregar

Pregunta #129 de 163

Id. de pregunta: 1192970

¿Qué tipo de incidente NO se aborda generalmente en un plan de contingencia?

A) un error de conexión T1

B) un huracán

C) un corte de energía

D) un bloqueo del servidor

Pregunta #130 de 163

Id. de pregunta: 1111801

Su organización le ha pedido que vuelva a evaluar el plan de seguridad de la organización para ver si aborda completamente la prevención de delitos e interrupciones a través de la disuasión. ¿Qué mecanismo de seguridad

cubre esta cuestión?

A) Cercas

B) detectores de humo

C) notificación de aplicación de la ley

D) evaluación del nivel de daño

Pregunta #131 de 163

Id. de pregunta: 1114782

Debido al valor de los datos de su empresa, su empresa le ha pedido que garantice la disponibilidad de los datos. Desea implementar las técnicas que pueden ayudar a garantizar la disponibilidad de los datos. ¿Qué mecanismo(s) debe(n) implementar?

a. Técnicas de auditoría

b. Técnicas de recuperación de datos

c. Técnicas de autenticación

d. Técnicas de tolerancia a fallos

e. técnicas de control de acceso

A) Sólo las opciones A y C

B) opción b

C) opción e

D) opción A

E) Opción d

F) Opciones B y D Sólo

G) opción c

Pregunta #132 de 163

Id. de pregunta: 1111772

El gobierno de Estados Unidos está investigando un crimen. Se han puesto en contacto con usted en relación con la evidencia que se encuentra en los servidores de su organización. ¿Qué método NO es utilizado por la policía federal para obtener información?

A) interrogar al sospechoso para que revele la información

B) obtener una orden judicial

C) obtener una orden de registro

D) siguientes procedimientos subrayados en la Quinta Enmienda

---

Pregunta #133 de 163

Id. de pregunta: 1105518

Su organización ha creado un plan de recuperación ante desastres exhaustivo. ¿Cuándo debe aplicarse?

A) Después de que todos los sistemas vuelvan a estar en línea

B) Cuando la empresa está en modo de funcionamiento normal

C) Una vez que los sistemas críticos vuelven a estar en línea

D) Cuando la empresa está en modo de emergencia

Pregunta #134 de 163

Id. de pregunta: 1114002

Su organización ha respondido a un incidente de seguridad. La brecha ha sido contenida, y todos los sistemas han sido recuperados. ¿Qué debe hacer por último como parte de la respuesta al incidente?

A) revisión post mortem

B) análisis

C) clasificación

D) investigación

Pregunta #135 de 163

Id. de pregunta: 1113998

¿Qué cuaderno es el más preferido durante el curso de la investigación en el mantenimiento de registros legales?

A) bloc de notas enlazado

B) Bloc de notas claro

C) bloc de notas etiquetado

D) cuaderno espiral

Pregunta #136 de 163

Id. de pregunta: 1105531

Su organización está investigando instalaciones informáticas alternativas para asegurarse de que la organización puede funcionar si se destruye la instalación principal. ¿Qué instalación fuera del sitio es la más costosa de implementar?

A) sitio cálido

B) sitio caliente

C) sitio frío

D) mecanismo de ayuda mutua

Pregunta #137 de 163

Id. de pregunta: 1192968

¿Cuándo debe instalar una revisión de software en un servidor de producción?

A) Cuando la revisión está en formato beta

B) Una vez probada la revisión

C) antes de que se haya probado la revisión

D) inmediatamente después del lanzamiento del parche

Pregunta #138 de 163

Id. de pregunta: 1111796

Se le ha pedido que trabaje con un equipo para diseñar el plan de continuidad del negocio de su empresa. El equipo ha definido el alcance del plan de continuidad del negocio. ¿Cuál es el siguiente paso?

A) Identificar funciones críticas.

B) Identificar las dependencias entre las áreas de negocio y las funciones críticas.

C) Identificar las áreas de negocio clave.

D) Determine el tiempo de inactividad aceptable.

Pregunta #139 de 163

Id. de pregunta: 1105469

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) separación de funciones

B) rotación de trabajos

C) Debida diligencia

D) atención debida

Pregunta #140 de 163

Id. de pregunta: 1105404

¿Qué término de delito se utiliza para indicar cómo un delincuente cometió un delito?

A) medio

B) MAMÁ

C) motivo

D) oportunidad

Pregunta #141 de 163

Id. de pregunta: 1105550

¿Qué es una barrera física que actúa como la primera línea de defensa contra un intruso?

A) un bloqueo

B) un mantrap

C) una valla

D) un torniquete

Pregunta #142 de 163

Id. de pregunta: 1114770

Recientemente, un empleado utilizó el equipo que le asignó su organización para llevar a cabo un ataque contra la organización. Se le ha pedido que recopile todas las pruebas relacionadas con el sistema. Debe recopilar la evidencia utilizando el orden de volatilidad para preservar la evidencia.

Mueva los tipos de datos de la columna izquierda a la columna derecha y colótelos en el orden correcto de volatilidad, comenzando con el más volátil en la parte superior. (Se utilizarán todos los componentes).

{UCMS id=5674327829643264 type=Activity}

Pregunta #143 de 163

Id. de pregunta: 1111790

Hacer coincidir las descripciones de la izquierda con el tipo de malware a la derecha que mejor coincide con la descripción.

{UCMS id=5754744247156736 type=Activity}

Pregunta #144 de 163

Id. de pregunta: 1114007

¿Qué plan está escrito para intentar evitar que un desastre afecte a la organización y/o para disminuir el impacto de un desastre?

A) proceso de gestión de incidentes
B) plan de continuidad del negocio
C) análisis de impacto en el negocio
D) plan de recuperación ante desastres

Pregunta #145 de 163

Id. de pregunta: 1192963

¿Qué método de restablecimiento de la contraseña del BIOS requiere acceso físico al equipo?

A) restablecer el contenido de CMOS a través de hardware
B) descifrar la contraseña del BIOS
C) restablecer el contenido de CMOS a través de software
D) uso de una contraseña de BIOS de puerta trasera

Pregunta #146 de 163

Id. de pregunta: 1105515

¿Qué solución de copia de seguridad electrónica realiza copias de seguridad de los datos en tiempo real pero transmite los datos a una instalación fuera del sitio en lotes?

A) bóveda electrónica

B) sombreado de disco

C) registro en diario remoto

D) administración jerárquica del almacenamiento (HSM)

Pregunta #147 de 163

Id. de pregunta: 1192972

Recientemente, las inundaciones dañaron el edificio que alberga el centro de datos de su empresa. Se le ha pedido a su equipo que determine qué funciones se vieron afectadas por la inundación y qué funciones son más críticas. ¿Qué paso de recuperación ante desastres está realizando?

A) evaluación de daños

B) estrategia de recuperación

C) ensayo

D) análisis de vulnerabilidades

Pregunta #148 de 163

Id. de pregunta: 1105435

¿Qué herramienta es un sistema de detección de intrusiones (IDS)?

A) Nessus

B) Tripwire

C) Resoplar

D) Etéreo

Pregunta #149 de 163

Id. de pregunta: 1114773

Ha decidido utilizar un sistema de detección de intrusiones basado en host (HIDS) para proporcionar mayor seguridad en la red de su empresa. ¿Qué fuentes de información NO son utilizadas por este sistema para analizar un intento de intrusión?

a. Registros del sistema

b. Paquetes de red

c. Alarmas del sistema operativo

d. Pistas de auditoría del sistema operativo

A) Opciones A y D
B) opción c
C) Opción d
D) opción A
E) Opciones B y C
F) opción b

Pregunta #150 de 163

Id. de pregunta: 1105474

La administración le ha notificado que el tiempo medio para reparar (MTTR) un disco duro crítico es demasiado alto. Debe abordar este problema con la menor cantidad de gastos. ¿Qué debes hacer?

A) Agregue otra unidad de disco duro e implemente la creación de reflejo de disco.
B) Agregue dos unidades de disco duro más e implemente la creación de bandas de disco con paridad.
C) Reemplace el disco duro por un disco duro más rápido.
D) Agregue otra unidad de disco duro e implemente la creación de bandas de disco.

Pregunta #151 de 163

Id. de pregunta: 1105396

¿Qué término de delito se utiliza para indicar cuándo y dónde ocurrió un delito?

A) medio

B) MAMÁ

C) motivo

D) oportunidad

Pregunta #152 de 163

Id. de pregunta: 1111798

¿Qué NO es un ejemplo de un control operativo?

A) un plan de continuidad del negocio

B) una pista de auditoría

C) administración de la configuración

D) un control de copia de seguridad

Pregunta #153 de 163

Id. de pregunta: 1105488

¿Qué afirmación es cierta de un modo de seguridad multinivel?

A) La clasificación de datos únicos se utiliza en el modo de seguridad multinivel.

B) El modo de seguridad multinivel implica el uso de etiquetas de confidencialidad.

C) El modo de seguridad multinivel está representado por el modelo de muro chino.

D) El modo de seguridad multinivel se basa en pertenencias basadas en roles.

Pregunta #154 de 163

Id. de pregunta: 1105445

Su organización ha decidido implementar un sistema de detección de intrusiones (NIDS) basado en red. ¿Cuál es la principal ventaja de utilizar este tipo de sistema?

A) sin contraataque al intruso

B) alto rendimiento de las estaciones de trabajo individuales de la red

C) capacidad de analizar información cifrada

D) bajo mantenimiento

Pregunta #155 de 163

Id. de pregunta: 1111794

Se le ha pedido que diseñe el proceso de gestión de cambios de su empresa. ¿Cuál es el primer paso de este proceso?

A) Solicitar el cambio.

B) Evaluar el impacto del cambio.

C) Aprobar el cambio.

D) Planifique el cambio.

Pregunta #156 de 163

Id. de pregunta: 1114787

Para mejorar la seguridad, ¿qué mecanismos deben utilizarse con un bloqueo de cifrado?

a. retraso de la puerta

b.key anulación

c. clave maestra

d. Alarma de rehenes

A) opción b

B) opción c

C) Opciones C y D

D) opción A

E) Opción d

F) todas las opciones

G) opciones A y B

Pregunta #157 de 163

Id. de pregunta: 1105486

¿Qué fallo del sistema operativo requiere la intervención del administrador del sistema para la restauración del sistema?

A) inicio en frío del sistema

B) reinicio de emergencia

C) recuperación de confianza

D) reinicio del sistema

Pregunta #158 de 163

Id. de pregunta: 1105536

Durante el próximo fin de semana, su equipo está programado para realizar pruebas que incluyen el cierre del sitio en vivo y llevar el sitio alternativo a la operación completa. ¿Qué prueba se realizará?

A) prueba de recorrido estructurado

B) prueba de simulación

C) prueba de interrupción completa

D) prueba paralela

Pregunta #159 de 163

Id. de pregunta: 1105433

Su empresa tiene varios tipos diferentes de supervisión de red que utiliza para detectar y prevenir ataques de red. ¿Qué tipo de monitoreo tiene más probabilidades de producir una alerta falsa?

A) basado en anomalías

B) basado en la detección de uso indebido

C) basado en firmas

D) basado en el comportamiento

Pregunta #160 de 163

Pregunta con id.: 1111800

De acuerdo con el plan de continuidad del negocio, esta semana su equipo debe completar una prueba de sistemas específicos para garantizar su funcionamiento en instalaciones alternativas. Los resultados de la prueba deben

compararse con el entorno vivo. ¿Qué prueba estás completando?

A) prueba de interrupción completa

B) prueba de recorrido estructurado

C) prueba de simulación

D) prueba paralela

Pregunta #161 de 163

Id. de pregunta: 1114791

Debe documentar las directrices adecuadas que deben incluirse como parte de cualquier directiva de seguridad que implique al personal que viaja con dispositivos emitidos por la compañía. Se le ha dado una lista de posibles consejos para que los viajeros deben ser incluidos en las directrices de la siguiente manera:

R. La privacidad al viajar, sin importar el medio de conexión, no está garantizada.

B. Los movimientos de personal se pueden rastrear utilizando dispositivos móviles.

C. El software malintencionado se puede insertar en un dispositivo desde cualquier conexión controlada por otra persona o a través de unidades usb.

D. No lleve el dispositivo con usted si no lo necesita.

¿Qué consejos son consejos válidos que deben incluirse como parte de las directrices para el personal?

A) Sólo B, C y D

B) Sólo A, B y C

C) Sólo A, C y D

D) Todos los consejos

Pregunta #162 de 163

Id. de pregunta: 1105525

Debe asegurarse de que se puedan recuperar todos los sistemas, redes y aplicaciones principales. ¿Qué debe crear o realizar?

A) análisis del riesgo

B) análisis de vulnerabilidades

C) plan de contingencia

D) análisis de impacto en el negocio (BIA)

Pregunta #163 de 163

Id. de pregunta: 1105472

Según la directiva de copia de seguridad de datos de su organización, debe realizar un seguimiento del número y la ubicación de las versiones de copia de seguridad de los datos de la organización. ¿Cuál es el objetivo principal de esta actividad?

A) Para crear una pista de auditoría

B) para garantizar la eliminación adecuada de la información

C) para demostrar la diligencia debida

D) Para restringir el acceso a las versiones de copia de seguridad