Dominio 3: Arquitectura e ingeniería de seguridad ID de prueba: 175720902

Pregunta # 1 de 193

ID de pregunta: 1105091

Su organización está considerando la posibilidad de construir o comprar una nueva instalación. ¿Qué factor de accesibilidad se debe considerar durante la fase de construcción o adquisición de la infraestructura de una instalación?

A) población de la zona

B) tráfico

C) terreno peligroso

D) tasa de criminalidad

Pregunta # 2 de 193

ID de pregunta: 1114698

¿Cuáles de las siguientes afirmaciones sobre la computación en la nube y la computación en red son verdaderas?

una. Tanto la computación en la nube como la computación en red son escalables.

B. La computación en cuadrícula es adecuada para almacenar objetos tan pequeños como 1 byte.

C. La computación en la nube puede ser más amigable con el medio ambiente que la computación en red.

D. La computación en la nube se compone de clientes ligeros, computación en red y computación de servicios públicos.

A) opciones ayb

B) opción d

C) opciones a, c y d

D) opción c

MI) todas las opciones

F) opciones a, byc

GRAMO) opción b

H) opción a

Pregunta # 3 de 193

ID de pregunta: 1111720

¿En qué modo NO funciona 3DES?

A) DES-EEE2

B) DES-EEE3

C) DES-EDE3

D) DES-DDD2

Pregunta # 4 de 193

ID de pregunta: 1192937

Haga clic en cada uno de los títulos de los escenarios para expandir o contraer su contenido. Debe leer el escenario completo para responder la pregunta.

Fondo

Usted es un profesional de seguridad contratado recientemente por una institución financiera que cotiza en bolsa para ayudar a administrar la seguridad de la organización. La oficina principal de la empresa se encuentra en Nueva York, NY, y tiene sucursales adicionales en todo Estados Unidos.

Asuntos actuales

La infraestructura actual incluye servidores Windows, servidores UNIX, clientes Windows, clientes Mac, dispositivos móviles Windows y dispositivos móviles Mac implementados en todas las oficinas. El departamento de TI de la empresa tiene un gran personal ubicado en la oficina de Nueva York. Cada sucursal tiene un pequeño personal de TI local que solo se ocupa de los problemas de esa sucursal.

Ha identificado varios casos en los que los ataques contra los sistemas cliente no se evitaron o no se detectaron a nivel de cliente porque no se implementaron controles para prevenir el ataque. Se robaron datos de algunos dispositivos. Toda una sucursal se infectó con malware y virus y requirió varios días de tiempo de recuperación, lo que significó una pérdida de ingresos. Por último, recientemente descubrió que varios sistemas cliente tienen instaladas versiones de SO sin licencia. Debe asegurarse de que se implementen los controles adecuados para mitigar estos riesgos.

En una auditoría reciente, descubrió que varios dispositivos móviles carecían de las actualizaciones adecuadas para sus sistemas operativos o aplicaciones. Además, los usuarios habían desactivado las funciones de limpieza remota y ubicación GPS en estos dispositivos y habían instalado varias aplicaciones no autorizadas. Necesita una solución para mitigar estos riesgos y controlar la configuración y las aplicaciones de los dispositivos móviles cuando esos dispositivos están conectados a la empresa.

Debido a varios contratos entre su empresa y terceros, debe asegurarse de que ciertos sistemas dentro de su infraestructura logren EAL7 en el modelo de evaluación Common Criteria.

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 devolver el servidor al estado operativo. Durante ese tiempo, el personal de la oficina principal no pudo acceder a la información importante de recursos humanos almacenada en el servidor afectado.

Se espera que los usuarios utilicen un cifrado simétrico y asimétrico para garantizar la confidencialidad de los datos. Debe implementar un sistema adecuado para administrar las claves de cifrado, los hash y los certificados digitales en todos los equipos cliente. También debe proteger las contraseñas, cifrar las unidades y administrar los derechos digitales para estas mismas computadoras.

La integridad de los datos se ha convertido en una preocupación cada vez más seria para los archivos creados y mantenidos por el departamento de investigación. Debe implementar la solución adecuada para estos archivos. Todos los archivos se encuentran en un único servidor al que solo pueden acceder los usuarios del departamento de investigación.

Nunca se completó formalmente un análisis de riesgos completo para toda la organización. Se le ha pedido que encabece este proyecto. Como parte de este proceso, debe identificar las amenazas geográficas para cada oficina individual.

Su organización desplegará dos oficinas internacionales a finales de este año. Se le ha invitado a participar en la selección de instalaciones y el proceso de seguridad interna del edificio para proporcionar información de seguridad particular.

Una de las oficinas internacionales previstas realizará tareas muy delicadas para una entidad gubernamental. Por esta razón, debe asegurarse de que la empresa seleccione una ubicación donde se pueda mantener un perfil bajo. ¿En cuál de los siguientes criterios basa su selección de instalaciones?

A) alrededores

B) construcción

C) accesibilidad

D) visibilidad

Pregunta # 5 de 193

ID de pregunta: 1105079

En PKI, ¿cuál es la entidad que firma un certificado?

A) a principal

B) un sujeto

C) un emisor

D) un verificador

Pregunta # 6 de 193

Pregunta ID: 1105027

Se le ha pedido específicamente que implemente un cifrado de flujo. ¿Qué algoritmo criptográfico podrías usar?

A) RC6

B) RC4

C) MD5

D) RC5

Pregunta # 7 de 193

ID de pregunta: 1105106

¿Qué descripción se aplica a un aumento repentino?

A) una fuente de alimentación prolongada por debajo del voltaje normal

B) un voltaje bajo momentáneo

C) un apagón momentáneo

D) un alto voltaje prolongado

MI) un apagón prolongado

Pregunta # 8 de 193

Pregunta ID: 1105095

Durante una auditoría de seguridad reciente, un contratista de seguridad externo sugirió que recortara el paisaje alrededor de las entradas. Además, se ha sugerido que instale CCTV en todas las entradas. ¿Qué faceta del enfoque de prevención del delito a través del diseño ambiental (CPTED) se está abordando?

A) vigilancia natural

B) control de acceso natural

C) refuerzo territorial

D) endurecimiento del objetivo

Pregunta # 9 de 193

ID de pregunta: 1111719

Ha creado una clave criptográfica en el controlador de dominio de su organización. ¿Que deberías hacer después?

A) Inicializa la clave.

B) Termine la clave.

C) Activar la llave.

D) Distribuya la llave.

Pregunta # 10 de 193

ID de pregunta: 1111713

Su organización ha decidido implementar un sitio web para que los clientes compren los productos de su organización. El sitio web utilizará el protocolo SET. ¿Qué afirmación es verdadera de este protocolo?

A) SET utiliza firmas digitales y certificados digitales para realizar y verificar una transacción electrónica.

B) SET transmite automáticamente la información de la tarjeta de crédito de un usuario a una CA cuando se realiza una compra en línea.

C) SET trabaja en la capa de red del modelo OSI.

D) SET utiliza 3DES para el intercambio de claves simétricas.

Pregunta # 11 de 193

ID de pregunta: 1111704

¿Qué componente NO está asociado con los Criterios Comunes?

A) objetivo de seguridad

B) objetivo de la evaluación

B) objetivo de la evaluación

C) perfil de protección

D) acreditación

Pregunta # 12 de 193

ID de pregunta: 1105039

¿Qué algoritmo de cifrado se basa en el acuerdo de claves Diffie-Hellman?

A) HAVAL

B) Mochila

C) Algoritmo de cifrado de datos internacional

D) El Gamal

Pregunta # 13 de 193

ID de pregunta: 1105069

Su gerente le ha pedido que se asegure de que los archivos de contraseñas que se almacenan en los servidores no sean vulnerables a los ataques. ¿A qué tipo de ataque serían vulnerables estos archivos?

A) un ataque de inundación SYN

B) un ataque de diccionario

C) un ataque de canal lateral

D) un ataque de denegación de servicio (DoS)

Pregunta # 14 de 193

Pregunta ID: 1105050

¿Qué es una función de trampilla?

A) un ataque en el que se interceptan mensajes entre dos entidades para que un atacante pueda hacerse pasar por una de las entidades

B) un mecanismo que permite la implementación de la función inversa en una función unidireccional

C) un ataque que intenta repetidamente diferentes valores para determinar la clave utilizada

D) un mecanismo integrado en un algoritmo que permite a un individuo eludir o subvertir la seguridad de alguna manera

Pregunta # 15 de 193

ID de pregunta: 1114714

¿Qué se consideraría un error ambiental?

una. calentamiento excesivo

B. electricidad estática

C. problemas de autenticación

D. configuración de dispositivo no válida

A) opciones c y d
B) opción b
C) opciones byc
D) opción d
MI) opciones ayb
F) opción a
GRAMO) opción c

Pregunta # 16 de 193

ID de pregunta: 1104995

¿Qué ataque se considera un ataque pasivo?

A) intervención a la línea telefónica
B) ataque de penetracion
C) ataque de denegación de servicio (DoS)
D) juegos de datos

Pregunta # 17 de 193

Pregunta # 17 de 193

ID de pregunta: 1105053

Durante una operación XOR, se combinan dos bits. Ambos valores son iguales. ¿Cuál será el resultado de esta combinación?

A) 0

B) O

C) 1

D) X

Pregunta # 18 de 193

Pregunta ID: 1105077

Ha implementado una infraestructura de clave pública (PKI) para emitir certificados a los equipos de la red de su organización. Debe asegurarse de que los certificados validados estén protegidos. ¿Qué se debe asegurar en una PKI para hacer esto?

A) la clave pública del certificado de un usuario

B) la clave privada del certificado de un usuario

C) la clave pública de la CA raíz

D) la clave privada de la CA raíz

Pregunta # 19 de 193

ID de pregunta: 1104935

¿Qué afirmación es verdadera sobre las estaciones de trabajo en modo compartimentado (CMW)?

A) CMW opera según el principio de privilegio máximo.

B) CMW opera en un modo de seguridad dedicado.

C) CMW, de forma predeterminada, otorga acceso relacionado con la información a todos los usuarios que tengan autorización de seguridad.

D) CMW requiere el uso de etiquetas de información.

Pregunta # 20 de 193

ID de pregunta: 1111724

¿Cuál de estos ataques es un ataque al criptosistema de una organización?

A) Denegación de servicio (DoS)

B) ataque de fuerza bruta

C) desbordamiento de búfer

D) ataque de texto plano conocido

Pregunta # 21 de 193

ID de pregunta: 1105057

Recientemente, descubrió una carpeta en su computadora que contiene una copia segura de la clave privada para todos los usuarios de su organización. Mantiene esta copia para asegurarse de que puede recuperar las claves perdidas. ¿De qué práctica de seguridad es este un ejemplo?

A) CRL

B) criptografía cuántica

C) depósito de llaves

D) esteganografía

Pregunta # 22 de 193

ID de pregunta: 1105071

¿Qué se refiere al tipo de modelo de confianza que utilizan las CA?

A) anillo

B) jerarquía

C) autobús

D) malla

Pregunta # 23 de 193

ID de pregunta: 1132508

¿Qué clasificación de seguridad TCSEC aborda el uso del análisis de canal encubierto?

A) D

B) B1

C) B2

D) A1

Pregunta # 24 de 193

ID de pregunta: 1105070

El gerente del departamento de TI le informa que la red de su organización ha sido víctima de un ataque de solo texto cifrado. ¿Qué afirmación es verdadera con respecto a este tipo de ataque?

A) Es muy difícil para un atacante recopilar el texto cifrado en una red.

B) Los piratas informáticos consideran que un ataque de solo texto cifrado es el ataque más fácil.

C) Un ataque de solo texto cifrado se centra en descubrir la clave de cifrado.

D) Un ataque de cumpleaños es un ejemplo de un ataque de solo texto cifrado.

Pregunta # 25 de 193

ID de pregunta: 1114705

¿Qué afirmación es verdadera del algoritmo de Rijndael?

A) Rijndael utiliza longitudes de bloque fijas y longitudes de clave fijas.

B) Rijndael utiliza longitudes de bloque variables y longitudes de clave variables.

C) Rijndael utiliza longitudes de bloque fijas y longitudes de clave variables.

D) Rijndael utiliza longitudes de bloque variables y longitudes de clave fijas.

Pregunta # 26 de 193

ID de pregunta: 1105040

¿Qué es un algoritmo que se utiliza para crear un resumen de mensajes para un archivo a fin de garantizar su integridad?

A) picadillo

B) texto cifrado

C) Texto sin formato

C) Texto sin formato

D) Llave pública

Pregunta # 27 de 193

ID de pregunta: 1105016

¿Qué mecanismo retiene la información HTTP de la conexión anterior?

A) HTTPS

B) IPSec

C) galletas

D) SSH

Pregunta # 28 de 193

Pregunta ID: 1105063

Quiere enviar un archivo a una compañera de trabajo llamada María. No desea proteger el contenido del archivo para que no se vea; sin embargo, cuando María reciba el archivo, desea que pueda determinar si el contenido del archivo se modificó durante el tránsito.

¿Qué medida de protección debería utilizar?

A) cifrado simétrico

B) cifrado asimétrico

C) un certificado digital

D) una firma digital

Pregunta # 29 de 193

ID de pregunta: 1111725

Su organización ha implementado una infraestructura de clave pública (PKI) para emitir certificados. Recientemente, su organización emitió varios certificados a una organización asociada. Revocaste los certificados hoy. Sin embargo, a la gerencia le preocupa que el período de gracia de la solicitud de revocación evite que los certificados se revoquen de manera oportuna. ¿Qué afirmación es verdadera de este período?

A) Se relaciona con el tiempo máximo de respuesta que toma la CA para una revocación

revocación.

B) Se refiere al período de gracia para que un servidor de CA de respaldo se actualice.

C) Se refiere a la validez de una firma digital.

D) Se refiere al tiempo que tarda una autoridad de registro (RA) en registrar un usuario.

Pregunta # 30 de 193

ID de pregunta: 1113941

¿Qué tipo de sistema de rociadores de agua NO es apropiado para un entorno de procesamiento de datos?

A) sistema de rociadores de agua de tubería seca

B) sistema de rociadores de agua de diluvio

C) sistema de rociadores de agua de tubería húmeda

D) sistema de rociadores de agua de acción previa

Pregunta # 31 de 193

ID de pregunta: 1105045

Debe descifrar un archivo cifrado mediante cifrado asimétrico. ¿Qué se debe utilizar para descifrar el archivo?

A) Texto sin formato

B) llave privada

C) Llave pública

D) resumen del mensaje

Pregunta # 32 de 193

ID de pregunta: 1192923

¿Qué modelo de control de acceso utiliza el axioma de integridad de estrella (*) y el axioma de integridad simple?

A) Modelo Biba

B) Modelo de pared chino

C) Modelo de Clark-Wilson

C) Modelo de Clark-Wilson

D) Modelo Bell-LaPadula

Pregunta # 33 de 193

ID de pregunta: 1104946

¿Qué modelo de seguridad ilustra el modo de seguridad multinivel?

A) Modelo Bell-LaPadula

B) modelo de transacción finita

C) modelo de acceso

D) Modelo Brewer y Nash

Pregunta # 34 de 193

ID de pregunta: 1192926

Haga clic en cada uno de los títulos de los escenarios para expandir o contraer su contenido. Debe leer el escenario completo para responder la pregunta.

Fondo

Usted es un profesional de seguridad contratado recientemente por una institución financiera que cotiza en bolsa para ayudar a administrar la seguridad de la organización. La oficina principal de la empresa se encuentra en Nueva York, NY, y tiene sucursales adicionales en todo Estados Unidos.

Asuntos actuales

La infraestructura actual incluye servidores Windows, servidores UNIX, clientes Windows, clientes Mac, dispositivos móviles Windows y dispositivos móviles Mac implementados en todas las oficinas. El departamento de TI de la empresa tiene un gran personal ubicado en la oficina de Nueva York. Cada sucursal tiene un pequeño personal de TI local que solo se ocupa de los problemas de esa sucursal.

Ha identificado varios casos en los que los ataques contra los sistemas cliente no se evitaron o no se detectaron a nivel de cliente porque no se implementaron controles para prevenir el ataque. Se robaron datos de algunos dispositivos. Toda una sucursal se infectó con malware y virus y requirió varios días de tiempo de recuperación, lo que significó una pérdida de ingresos. Por último, recientemente descubrió que varios sistemas cliente tienen instaladas versiones de SO sin licencia. Debe asegurarse de que se implementen los controles adecuados para mitigar estos riesgos.

En una auditoría reciente, descubrió que varios dispositivos móviles carecían de las actualizaciones adecuadas para

sus sistemas operativos o aplicaciones. Además, los usuarios habían desactivado las funciones de limpieza remota y ubicación GPS en estos dispositivos y habían instalado varias aplicaciones no autorizadas. Necesita una solución para mitigar estos riesgos y controlar la configuración y las aplicaciones de los dispositivos móviles cuando esos dispositivos están conectados a la empresa.

Debido a varios contratos entre su empresa y terceros, debe asegurarse de que ciertos sistemas dentro de su infraestructura logren EAL7 en el modelo de evaluación Common Criteria.

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 devolver el servidor al estado operativo. Durante ese tiempo, el personal de la oficina principal no pudo acceder a la información importante de recursos humanos almacenada en el servidor afectado.

Se espera que los usuarios utilicen un cifrado simétrico y asimétrico para garantizar la confidencialidad de los datos. Debe implementar un sistema adecuado para administrar las claves de cifrado, los hash y los certificados digitales en todos los equipos cliente. También debe proteger las contraseñas, cifrar las unidades y administrar los derechos digitales para estas mismas computadoras.

La integridad de los datos se ha convertido en una preocupación cada vez más seria para los archivos creados y mantenidos por el departamento de investigación. Debe implementar la solución adecuada para estos archivos. Todos los archivos se encuentran en un único servidor al que solo pueden acceder los usuarios del departamento de investigación.

Nunca se completó formalmente un análisis de riesgos completo para toda la organización. Se le ha pedido que encabece este proyecto. Como parte de este proceso, debe identificar las amenazas geográficas para cada oficina individual.

Su organización desplegará dos oficinas internacionales a finales de este año. Se le ha invitado a participar en la selección de instalaciones y el proceso de seguridad interna del edificio para proporcionar información de seguridad particular.

¿Qué debe implementar en los equipos cliente para administrar mejor las claves de cifrado, las contraseñas, el cifrado de unidades y los derechos digitales de los usuarios?

A) TPM

B) PKI

C) VM

D) DNS

Pregunta # 35 de 193

ID de pregunta: 1192929

Se le ha pedido que implemente software antivirus para su entorno de virtualización. ¿Dónde debería instalar el software antivirus?

A) en cada computadora virtual solamente

B) solo en la computadora host

C) solo en la computadora física

D) tanto en la computadora host como en todas las computadoras virtuales

Pregunta # 36 de 193

ID de pregunta: 1105044

¿Qué tipo de cifrado reemplaza el texto original en un mensaje con un texto diferente?

A) cifrado de sustitución

B) cifrado de transposición

C) cifrado de flujo

D) cifrado de bloque

Pregunta # 37 de 193

ID de pregunta: 1104936

¿Qué afirmación es verdadera sobre el modelo de flujo de información?

A) El modelo de flujo de información no permite el flujo de información desde un nivel de seguridad más bajo a un nivel de seguridad más alto.

B) El modelo de flujo de información permite el flujo de información dentro del mismo nivel de seguridad.

C) El modelo de Biba no se basa en el modelo de flujo de información.

D) El modelo de flujo de información solo se ocupa de la dirección del flujo.

Pregunta # 38 de 193

ID de pregunta: 1113924

¿Cuál es el propósito de un dispositivo que usa acceso directo a memoria (DMA)?

¿Cuál es el propósito de un dispositivo que usa acceso directo a memoria (DMA)?

A) Se comunica mediante una dirección lógica.

B) Implementa la transferencia de datos de alta velocidad entre el dispositivo y la memoria.

C) Proporciona multiprocesamiento mediante una entrada / salida (E / S) impulsada por interrupciones.

D) Implementa la transferencia de datos de alta velocidad entre el dispositivo y la CPU.

Pregunta # 39 de 193

ID de pregunta: 1105074

¿Qué es una lista de números de serie de certificados digitales que no han caducado, pero que deben considerarse inválidos?

A) UDP

B) QUE

C) CRL

D) KDC

Pregunta # 40 de 193

ID de pregunta: 1111710

Un servidor de archivos se ha reiniciado inesperadamente en modo de usuario único. No está seguro de qué causó el reinicio. ¿Que deberías hacer después?

A) Recupere archivos dañados del sistema de archivos.

B) Reinicie el servidor de archivos.

C) Valide la configuración crítica y los archivos del sistema.

D) Identifique la causa del reinicio inesperado.

Pregunta # 41 de 193

ID de pregunta: 1113918

¿Qué modelo de control de acceso utiliza estados y transiciones de estado al diseñar el sistema de protección?

A) Modelo Take-Grant

B) Modelo de flujo de información

C) Modelo Biba

D) Modelo Bell-LaPadula

Pregunta # 42 de 193

ID de pregunta: 1111709

¿Cuál es la mejor descripción de la memoria caché?

A) memoria no volátil que mantiene su contenido incluso durante cortes de energía

B) memoria especial utilizada en dispositivos portátiles

C) memoria volátil que pierde su contenido durante cortes de energía

D) memoria utilizada para la transferencia de datos a alta velocidad

Pregunta # 43 de 193

ID de pregunta: 1113921

Está revisando los estándares de seguridad de Common Criteria. ¿Qué nivel de garantía de evaluación de criterios comunes (EAL) es el punto de referencia común para sistemas operativos y productos?

A) EAL 4

B) EAL 3

C) EAL 5

D) EAL 6

MI) EAL 7

Pregunta # 44 de 193

ID de pregunta: 1113933

¿Qué algoritmo hash utiliza un valor hash de 192 bits y se desarrolló para sistemas de 64 bits?

A) MD5

B) SHA

C) Tigre

D) HAVAL

Pregunta # 45 de 193

ID de pregunta: 1192928

Usted es responsable de administrar una computadora con Windows Server 2012 que aloja varias computadoras virtuales. Necesita instalar los últimos parches para el sistema operativo. ¿Dónde debería instalar los parches?

A) tanto en la computadora host como en todas las computadoras virtuales de Windows Server 2012

B) solo en cada computadora virtual con Windows Server 2012

C) solo en la computadora física

D) solo en la computadora host

Pregunta # 46 de 193

ID de pregunta: 1105066

¿Qué servicio cumple la criptografía al garantizar que un remitente no pueda negar el envío de un mensaje una vez que se transmite?

A) autenticidad

B) no repudio

C) integridad

D) confidencialidad

Pregunta # 47 de 193

ID de pregunta: 1132509

¿Qué característica identifica el nivel de seguridad de TCSEC B2?

A) protección estructurada

B) protección de acceso controlado

C) protección mínima

C) protección mínima

D) seguridad etiquetada

Pregunta # 48 de 193

ID de pregunta: 1111732

¿Qué tipo de sistema de rociadores de agua se usa mejor en climas más fríos?

A) tubo mojado

B) diluvio

C) tubería seca

D) pre-acción

Pregunta # 49 de 193

ID de pregunta: 1114715

La gerencia ha solicitado que se instalen detectores de agua para garantizar que se detecte el agua antes de que se produzcan daños importantes. ¿En qué lugares se deben instalar los detectores de agua?

una. bajo pisos elevados

B. entre paredes

C. bajo los cimientos del edificio

D. en falsos techos

A) opciones ayd

B) opción d

C) opción c

D) opción a

MI) opción b

F) opciones byc

Pregunta # 50 de 193

ID de pregunta: 1105117

Los planes de diseño del centro de datos de su organización requieren que se utilicen paneles de vidrio en una pared

del centro de datos para garantizar que el personal del centro pueda ser visto en todo momento. ¿Qué tipo de vidrio se debe utilizar?

A) irrompible

B) acrílico

C) templado

D) cableado

MI) estándar

Pregunta # 51 de 193

ID de pregunta: 1105103

¿Qué control de seguridad física es MÁS apropiado cuando se requiere un juicio discriminatorio para mantener la seguridad física de una instalación?

A) guardias

B) televisión de circuito cerrado (CCTV)

C) contraseñas

D) perros

Pregunta # 52 de 193

ID de pregunta: 1104975

¿Qué es un circuito integrado con lógica interna programable?

A) cache

B) ROM

C) un PLD

D) memoria flash

Pregunta # 53 de 193

ID de pregunta: 1192925

Haga clic en cada uno de los títulos de los escenarios para expandir o contraer su contenido. Debe leer el escenario

completo para responder la pregunta.

Fondo

Usted es un profesional de seguridad contratado recientemente por una institución financiera que cotiza en bolsa para ayudar a administrar la seguridad de la organización. La oficina principal de la empresa se encuentra en Nueva York, NY, y tiene sucursales adicionales en todo Estados Unidos.

Asuntos actuales

La infraestructura actual incluye servidores Windows, servidores UNIX, clientes Windows, clientes Mac, dispositivos móviles Windows y dispositivos móviles Mac implementados en todas las oficinas. El departamento de TI de la empresa tiene un gran personal ubicado en la oficina de Nueva York. Cada sucursal tiene un pequeño personal de TI local que solo se ocupa de los problemas de esa sucursal.

Ha identificado varios casos en los que los ataques contra los sistemas cliente no se evitaron o no se detectaron a nivel de cliente porque no se implementaron controles para prevenir el ataque. Se robaron datos de algunos dispositivos. Toda una sucursal se infectó con malware y virus y requirió varios días de tiempo de recuperación, lo que significó una pérdida de ingresos. Por último, recientemente descubrió que varios sistemas cliente tienen instaladas versiones de SO sin licencia. Debe asegurarse de que se implementen los controles adecuados para mitigar estos riesgos.

En una auditoría reciente, descubrió que varios dispositivos móviles carecían de las actualizaciones adecuadas para sus sistemas operativos o aplicaciones. Además, los usuarios habían desactivado las funciones de limpieza remota y ubicación GPS en estos dispositivos y habían instalado varias aplicaciones no autorizadas. Necesita una solución para mitigar estos riesgos y controlar la configuración y las aplicaciones de los dispositivos móviles cuando esos dispositivos están conectados a la empresa.

Debido a varios contratos entre su empresa y terceros, debe asegurarse de que ciertos sistemas dentro de su infraestructura logren EAL7 en el modelo de evaluación Common Criteria.

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 devolver el servidor al estado operativo. Durante ese tiempo, el personal de la oficina principal no pudo acceder a la información importante de recursos humanos almacenada en el servidor afectado.

Se espera que los usuarios utilicen un cifrado simétrico y asimétrico para garantizar la confidencialidad de los datos. Debe implementar un sistema adecuado para administrar las claves de cifrado, los hash y los certificados digitales en todos los equipos cliente. También debe proteger las contraseñas, cifrar las unidades y administrar los derechos digitales para estas mismas computadoras.

La integridad de los datos se ha convertido en una preocupación cada vez más seria para los archivos creados y mantenidos por el departamento de investigación. Debe implementar la solución adecuada para estos archivos. Todos los archivos se encuentran en un único servidor al que solo pueden acceder los usuarios del departamento de investigación.

Nunca se completó formalmente un análisis de riesgos completo para toda la organización. Se le ha pedido que

Nunca se completó formalmente un análisis de riesgos completo para toda la organización. Se le ha pedido que encabece este proyecto. Como parte de este proceso, debe identificar las amenazas geográficas para cada oficina individual.

Su organización desplegará dos oficinas internacionales a finales de este año. Se le ha invitado a participar en la selección de instalaciones y el proceso de seguridad interna del edificio para proporcionar información de seguridad particular.

¿Cuál es la descripción correcta para el nivel de Criterios Comunes que deben alcanzar ciertos sistemas porque forman parte de contratos de terceros?

A) diseñado, probado y revisado metódicamente
B) semiformalmente diseñado y probado
C) Diseño semiformalmente verificado y probado.
D) diseño formalmente verificado y probado

Pregunta # 54 de 193

ID de pregunta: 1105087

La administración decide utilizar el código de autenticación de mensajes (MAC) para proteger los mensajes de la red. ¿Qué tipo de ataque previene esto?

A) ataques enmascarados
B) Ataques de denegación de servicio
C) ataques con bombas lógicas
D) Ataques de inundación SYN

Pregunta # 55 de 193

Pregunta ID: 1105058

Dada la clave, ¿qué es un algoritmo que calcula las subclaves para cada ronda de cifrado?

A) agrupación de claves
B) función unidireccional
C) depósito de llaves
D) horario clave

Pregunta # 56 de 193

ID de pregunta: 1105105

¿Qué característica de la instalación puede representar la amenaza de seguridad más significativa de la infraestructura de una instalación?

A) mantraps

B) alfombras y aerosoles antiestáticos

C) pisos suspendidos

D) falsos techos

Pregunta # 57 de 193

ID de pregunta: 1114699

¿Cuál de los siguientes representa problemas de seguridad en la computación en la nube?

una. acceso de usuarios privilegiados

B. ubicación de los datos

C. segregación de datos

D. recuperación de datos

A) opción a

B) opción d

C) opciones c y d

D) opción c

MI) todas las opciones

F) opciones ayb

GRAMO) opción b

Pregunta # 58 de 193

ID de pregunta: 1104992

¿Qué es OVAL?

A) una aplicación que comprueba su red en busca de problemas de seguridad

A) una aplicación que comprueba su red en busca de problemas de seguridad conocidos

B) una aplicación diseñada para infectar un sistema informático

C) una pieza de hardware que aísla una red de otra

D) un estándar escrito en XML que proporciona contenido de seguridad abierto y disponible públicamente

---

Pregunta # 59 de 193

ID de pregunta: 1105119

Recientemente, su organización instaló un nuevo sistema de calefacción y aire acondicionado para sus instalaciones. Ahora, cuando se enciende la calefacción o el aire, las luces de la instalación se atenúan durante un breve período de tiempo. ¿Qué ocurre cuando las luces se atenúan?

A) un apagón

B) un apagón

C) una subida de tensión

D) una caída de poder

Pregunta # 60 de 193

ID de pregunta: 1104941

¿Qué principio de seguridad utilizado en el modelo Bell-LaPadula evita que se modifique el nivel de seguridad de sujetos y objetos una vez creados?

A) principio de dominación

B) principio estático

C) principio de privilegio mínimo

D) principio de tranquilidad

Pregunta # 61 de 193

ID de pregunta: 1114700

¿Qué medidas de seguridad debería emplear para proteger los teléfonos móviles propiedad de una organización?

una. Habilite las interfaces inalámbricas.

B. Mantenga el control físico.

C. Habilite la autenticación de usuario.

D. Desactive las funciones innecesarias.

A) opción d

B) opción c

C) opción a

D) opción b

MI) opciones b, c y d

F) opciones a, byc

Pregunta # 62 de 193

ID de pregunta: 1192934

¿Cuál es un ejemplo de un ataque de fuerza bruta?

A) usando un programa para adivinar las contraseñas de un archivo SAM

B) buscando en la basura de una empresa

C) recopilar paquetes de una conexión de red

D) enviar varios mensajes ICMP a un servidor web

Pregunta # 63 de 193

ID de pregunta: 1105098

Necesita almacenar algunos dispositivos de almacenamiento magnético en una instalación de almacenamiento temporal. ¿A qué temperatura podrían empezar a producirse daños?

A) 175 grados Fahrenheit

B) 100 grados Fahrenheit

C) 90 grados Fahrenheit

D) 350 grados Fahrenheit

Pregunta # 64 de 193

Pregunta # 64 de 193

ID de pregunta: 1105109

¿Qué ubicación sería MÁS apropiada para el centro de datos de la instalación de procesamiento de información de una empresa?

A) el último piso de la instalación

B) el núcleo de la instalación

C) la planta baja de la instalación

D) el sótano de la instalación

Pregunta # 65 de 193

ID de pregunta: 1105030

¿De qué tipo de algoritmo de cifrado es un ejemplo Diffie-Hellman?

A) asimétrico con autorización

B) asimétrico con autenticación

C) simétrico con firma digital

D) simétrico con autenticación

Pregunta # 66 de 193

ID de pregunta: 1104972

¿Cuál es la mejor descripción de un sistema abierto?

A) un sistema que contiene un solo punto de control

B) un sistema que se basa en estándares y protocolos de especificaciones publicadas

C) un sistema que no sigue los estándares de la industria

D) un sistema que contiene múltiples puntos de control

Pregunta # 67 de 193

ID de pregunta: 1105078

En PKI, ¿qué término se refiere a una clave pública que se puede utilizar para verificar el certificado utilizado en una firma digital?

firma digital?

A) Un objetivo

B) un emisor

C) una fiesta de confianza

D) un ancla de confianza

Pregunta # 68 de 193

ID de pregunta: 1113936

¿Qué afirmación es verdadera sobre la criptografía simétrica?

A) La criptografía simétrica es más rápida que la criptografía asimétrica.

B) La criptografía simétrica proporciona una mayor seguridad en comparación con la criptografía asimétrica.

C) La criptografía simétrica no requiere un mecanismo seguro para entregar claves correctamente.

D) La criptografía simétrica utiliza diferentes claves para cifrar y descifrar mensajes.

Pregunta # 69 de 193

ID de pregunta: 1105014

Ha decidido adjuntar una marca de tiempo digital a un documento que se comparte en la red. ¿Qué ataque previene esto?

A) un ataque de canal lateral

B) un ataque de solo texto cifrado

C) un ataque de repetición

D) un ataque de texto plano conocido

Pregunta # 70 de 193

ID de pregunta: 1113937

¿Qué factor NO afecta la fuerza relativa de un criptosistema?

A) el secreto de la clave secreta

B) el algoritmo de cifrado

C) la longitud de la clave secreta

D) el valor de intercambio clave

Pregunta # 71 de 193

ID de pregunta: 1105064

Debe determinar si la información de un archivo ha cambiado. ¿Qué deberías usar?

A) una firma digital

B) un certificado digital

C) cifrado de clave privada

D) cifrado de clave pública

Pregunta # 72 de 193

ID de pregunta: 1104969

¿Cuál es la mejor descripción de las direcciones absolutas que se utilizan en la arquitectura de la memoria?

A) la memoria utilizada en búsquedas complejas

B) las direcciones de memoria que no son únicas

C) las direcciones de memoria indexadas que utiliza el software

D) las direcciones de memoria física que utiliza una CPU

Pregunta # 73 de 193

ID de pregunta: 1104942

¿Qué procesos controlan el flujo de información en el modelo de control de acceso basado en celosía (LBAC)?

A) estrella (*) integridad e integridad simple axiomas

B) triple regla de acceso

C) seguridad simple, propiedad de estrella y reglas estrictas de propiedad de estrella

D) operadores de límite inferior mínimo superior y máximo

Pregunta # 74 de 193

ID de pregunta: 1104938

¿Qué modelo de control de acceso asegura la integridad a través de la implementación de reglas de monitoreo de integridad y reglas de preservación de integridad?

A) Modelo de pared chino

B) Modelo de Clark-Wilson

C) Modelo Bell-LaPadula

D) Modelo Biba

Pregunta # 75 de 193

ID de pregunta: 1105032

¿Qué afirmación NO es cierta sobre los modos de funcionamiento del algoritmo del estándar de cifrado de datos (DES)?

A) Los modos Cipher Block Chaining (CBC) y Cipher Feedback (CFB) se utilizan mejor para la autenticación.

B) La operación en modo Libro de códigos electrónico (ECB) es la más adecuada para el cifrado de bases de datos.

C) ECB es el modo DES más fácil y rápido que se puede utilizar.

D) ECB utiliza repetidamente texto cifrado producido para cifrar un mensaje que consta de bloques.

Pregunta # 76 de 193

ID de pregunta: 1114716

El plan de seguridad contra incendios de su empresa establece que el sistema de calefacción y aire acondicionado debe apagarse en caso de incendio. ¿Cuál de las siguientes NO representa razones para hacer esto?

una. Los sistemas de extinción de incendios no funcionarán si el sistema de calefacción y aire acondicionado está encendido.

B. Los sistemas de detección de incendios no funcionarán si el sistema de calefacción y aire acondicionado está

encendido.

C. Se evitará la propagación de humo por todo el edificio.

D. Se evitará que el oxígeno llegue al fuego.

A) opción c
B) opciones ayb
C) opción d
D) opción b
MI) opción a
F) opciones c y d

Pregunta # 77 de 193

ID de pregunta: 1114703

¿Qué tipos de cifrado requieren que se compartan las claves privadas?

una. cifrado asimétrico

B. cifrado de clave privada

C. cifrado de clave pública

D. cifrado simétrico

A) opción a
B) opciones ayc
C) opción c
D) opción d
MI) opción b
F) opciones by d

Pregunta # 78 de 193

ID de pregunta: 1105023

¿Qué servicio proporcionado por un criptosistema convierte la información en datos ininteligibles?

A) autorización

B) no repudio

C) integridad

D) confidencialidad

Pregunta # 79 de 193

ID de pregunta: 1113929

¿A qué tipo de ataque de contraseña se le suele llamar ataque exhaustivo?

A) ataque de suplantación de identidad

B) Ataque de diccionario

C) ataque de fuerza bruta

D) ataque de suplantación

Pregunta # 80 de 193

ID de pregunta: 1192931

Haga clic en cada uno de los títulos de los escenarios para expandir o contraer su contenido. Debe leer el escenario completo para responder la pregunta.

Fondo

Usted es un profesional de seguridad contratado recientemente por una institución financiera que cotiza en bolsa para ayudar a administrar la seguridad de la organización. La oficina principal de la empresa se encuentra en Nueva York, NY, y tiene sucursales adicionales en todo Estados Unidos.

Asuntos actuales

La infraestructura actual incluye servidores Windows, servidores UNIX, clientes Windows, clientes Mac, dispositivos móviles Windows y dispositivos móviles Mac implementados en todas las oficinas. El departamento de TI de la empresa tiene un gran personal ubicado en la oficina de Nueva York. Cada sucursal tiene un pequeño personal de TI local que solo se ocupa de los problemas de esa sucursal.

Ha identificado varios casos en los que los ataques contra los sistemas cliente no se evitaron o no se detectaron a nivel de cliente porque no se implementaron controles para prevenir el ataque. Se robaron datos de algunos dispositivos. Toda una sucursal se infectó con malware y virus y requirió varios días de tiempo de recuperación, lo que significó una pérdida de ingresos. Por último, recientemente descubrió que varios sistemas cliente tienen instaladas versiones de SO sin licencia. Debe asegurarse de que se implementen los controles adecuados para mitigar estos riesgos.

En una auditoría reciente, descubrió que varios dispositivos móviles carecían de las actualizaciones adecuadas para sus sistemas operativos o aplicaciones. Además, los usuarios habían desactivado las funciones de limpieza remota y ubicación GPS en estos dispositivos y habían instalado varias aplicaciones no autorizadas. Necesita una solución para mitigar estos riesgos y controlar la configuración y las aplicaciones de los dispositivos móviles cuando esos dispositivos están conectados a la empresa.

Debido a varios contratos entre su empresa y terceros, debe asegurarse de que ciertos sistemas dentro de su infraestructura logren EAL7 en el modelo de evaluación Common Criteria.

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 devolver el servidor al estado operativo. Durante ese tiempo, el personal de la oficina principal no pudo acceder a la información importante de recursos humanos almacenada en el servidor afectado.

Se espera que los usuarios utilicen un cifrado simétrico y asimétrico para garantizar la confidencialidad de los datos. Debe implementar un sistema adecuado para administrar las claves de cifrado, los hash y los certificados digitales en todos los equipos cliente. También debe proteger las contraseñas, cifrar las unidades y administrar los derechos digitales para estas mismas computadoras.

La integridad de los datos se ha convertido en una preocupación cada vez más seria para los archivos creados y mantenidos por el departamento de investigación. Debe implementar la solución adecuada para estos archivos. Todos los archivos se encuentran en un único servidor al que solo pueden acceder los usuarios del departamento de investigación.

Nunca se completó formalmente un análisis de riesgos completo para toda la organización. Se le ha pedido que encabece este proyecto. Como parte de este proceso, debe identificar las amenazas geográficas para cada oficina individual.

Su organización desplegará dos oficinas internacionales a finales de este año. Se le ha invitado a participar en la selección de instalaciones y el proceso de seguridad interna del edificio para proporcionar información de seguridad particular.

¿Cuáles de las siguientes políticas y controles debería implementar para los sistemas cliente en función de sus riesgos identificados? (Elija todas las que correspondan).

A) Utilice el cifrado de unidades en todos los discos duros del sistema cliente.

B) Implemente software anti-malware y antivirus en todos los sistemas cliente.

C) Implemente solo sistemas operativos compatibles con licencia.

D) Implementar firewalls y sistemas de detección de intrusos basados en host en los sistemas cliente.

Pregunta # 81 de 193

ID de pregunta: 1105083

Su organización ha implementado una infraestructura de clave pública (PKI). Debe asegurarse de que el navegador de cada usuario verifique automáticamente el estado del certificado del usuario. ¿Qué deberías implementar?

A) CRL

B) OCSP

C) MÍMICA

D) PGP

Pregunta # 82 de 193

ID de pregunta: 1113931

¿Qué es un algoritmo de cifrado?

A) una clave de cifrado

B) una fórmula matemática

C) datos antes del cifrado

D) datos después del cifrado

Pregunta # 83 de 193

ID de pregunta: 1192936

Haga clic en cada uno de los títulos de los escenarios para expandir o contraer su contenido. Debe leer el escenario completo para responder la pregunta.

Fondo

Usted es un profesional de seguridad contratado recientemente por una institución financiera que cotiza en bolsa para ayudar a administrar la seguridad de la organización. La oficina principal de la empresa se encuentra en Nueva York, NY, y tiene sucursales adicionales en todo Estados Unidos.

Asuntos actuales

La infraestructura actual incluye servidores Windows, servidores UNIX, clientes Windows, clientes Mac, dispositivos móviles Windows y dispositivos móviles Mac implementados en todas las oficinas. El departamento de TI de la empresa tiene un gran personal ubicado en la oficina de Nueva York. Cada sucursal tiene un pequeño personal de TI local que solo se ocupa de los problemas de esa sucursal.

local que solo se ocupa de los problemas de esa sucursal.

Ha identificado varios casos en los que los ataques contra los sistemas cliente no se evitaron o no se detectaron a nivel de cliente porque no se implementaron controles para prevenir el ataque. Se robaron datos de algunos dispositivos. Toda una sucursal se infectó con malware y virus y requirió varios días de tiempo de recuperación, lo que significó una pérdida de ingresos. Por último, recientemente descubrió que varios sistemas cliente tienen instaladas versiones de SO sin licencia. Debe asegurarse de que se implementen los controles adecuados para mitigar estos riesgos.

En una auditoría reciente, descubrió que varios dispositivos móviles carecían de las actualizaciones adecuadas para sus sistemas operativos o aplicaciones. Además, los usuarios habían desactivado las funciones de limpieza remota y ubicación GPS en estos dispositivos y habían instalado varias aplicaciones no autorizadas. Necesita una solución para mitigar estos riesgos y controlar la configuración y las aplicaciones de los dispositivos móviles cuando esos dispositivos están conectados a la empresa.

Debido a varios contratos entre su empresa y terceros, debe asegurarse de que ciertos sistemas dentro de su infraestructura logren EAL7 en el modelo de evaluación Common Criteria.

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 devolver el servidor al estado operativo. Durante ese tiempo, el personal de la oficina principal no pudo acceder a la información importante de recursos humanos almacenada en el servidor afectado.

Se espera que los usuarios utilicen un cifrado simétrico y asimétrico para garantizar la confidencialidad de los datos. Debe implementar un sistema adecuado para administrar las claves de cifrado, los hash y los certificados digitales en todos los equipos cliente. También debe proteger las contraseñas, cifrar las unidades y administrar los derechos digitales para estas mismas computadoras.

La integridad de los datos se ha convertido en una preocupación cada vez más seria para los archivos creados y mantenidos por el departamento de investigación. Debe implementar la solución adecuada para estos archivos. Todos los archivos se encuentran en un único servidor al que solo pueden acceder los usuarios del departamento de investigación.

Nunca se completó formalmente un análisis de riesgos completo para toda la organización. Se le ha pedido que encabece este proyecto. Como parte de este proceso, debe identificar las amenazas geográficas para cada oficina individual.

Su organización desplegará dos oficinas internacionales a finales de este año. Se le ha invitado a participar en la selección de instalaciones y el proceso de seguridad interna del edificio para proporcionar información de seguridad particular.

¿Qué debería implementar para los archivos del departamento de investigación?

A) RC6

B) Diffie-Hellman

C) SHA-3

D) 3DES

Pregunta # 84 de 193

ID de pregunta: 1104979

Se le ha pedido que se asegure de que los datos en reposo en las computadoras de la organización permanezcan confidenciales. ¿Qué control de seguridad debería implementar?

A) cifrado de enlace

B) listas de control de acceso

C) líneas de base

D) cifrado de unidad

Pregunta # 85 de 193

ID de pregunta: 1111718

¿Qué característica de PGP es diferente del uso de certificados formales de confianza?

A) el uso de dominios de confianza por parte de los servidores y los clientes

B) el uso de servidores de autoridad de certificación

C) el despliegue de claves privadas para autenticación y cifrado

D) el establecimiento de una web de confianza entre los usuarios

Pregunta # 86 de 193

ID de pregunta: 1105072

¿Qué tarea realiza un sistema de revocación de claves?

A) generación de claves

B) invalidación de clave

C) protección de clave privada

D) validación de claves

Pregunta # 87 de 193

ID de pregunta: 1104954

¿A qué se refiere la norma ISO 15408?

A) ITSEC

B) Criterios comunes

C) TCSEC

D) politica de seguridad

Pregunta # 88 de 193

ID de pregunta: 1114709

Una nueva política de seguridad implementada por su organización establece que todos los mensajes de correo electrónico oficiales deben estar firmados con firmas digitales. ¿Qué elementos se proporcionan cuando se utilizan?

una. integridad

B. disponibilidad

C. cifrado

D. autenticación

es. no repudio

A) opción c

B) opciones c, d y e

C) opción d

D) opción b

MI) opciones a, d y e

F) opción a

GRAMO) opción e

H) opciones a, byc

Pregunta # 89 de 193

ID de pregunta: 1114691

¿Cuáles de las siguientes entidades NO son sujetos?

una. usuario

B. proceso

C. expediente

D. grupo

mi. directorio

F. ordenador

A) opción d
B) opción c
C) todas las opciones
D) opción f
MI) opción b
F) opción a
GRAMO) opción e
H) solo opciones c, e y f
I) solo opciones a, byd

Pregunta # 90 de 193

ID de pregunta: 1192933

Haga clic en cada uno de los títulos de los escenarios para expandir o contraer su contenido. Debe leer el escenario completo para responder la pregunta.

Fondo

Usted es un profesional de seguridad contratado recientemente por una institución financiera que cotiza en bolsa para ayudar a administrar la seguridad de la organización. La oficina principal de la empresa se encuentra en Nueva York, NY, y tiene sucursales adicionales en todo Estados Unidos.

Asuntos actuales

La infraestructura actual incluye servidores Windows, servidores UNIX, clientes Windows, clientes Mac, dispositivos móviles Windows y dispositivos móviles Mac implementados en todas las oficinas. El departamento de TI de la empresa tiene un gran personal ubicado en la oficina de Nueva York. Cada sucursal tiene un pequeño personal de TI local que solo se ocupa de los problemas de esa sucursal.

Ha identificado varios casos en los que los ataques contra los sistemas cliente no se evitaron o no se detectaron a

nivel de cliente porque no se implementaron controles para prevenir el ataque. Se robaron datos de algunos dispositivos. Toda una sucursal se infectó con malware y virus y requirió varios días de tiempo de recuperación, lo que significó una pérdida de ingresos. Por último, recientemente descubrió que varios sistemas cliente tienen instaladas versiones de SO sin licencia. Debe asegurarse de que se implementen los controles adecuados para mitigar estos riesgos.

En una auditoría reciente, descubrió que varios dispositivos móviles carecían de las actualizaciones adecuadas para sus sistemas operativos o aplicaciones. Además, los usuarios habían desactivado las funciones de limpieza remota y ubicación GPS en estos dispositivos y habían instalado varias aplicaciones no autorizadas. Necesita una solución para mitigar estos riesgos y controlar la configuración y las aplicaciones de los dispositivos móviles cuando esos dispositivos están conectados a la empresa.

Debido a varios contratos entre su empresa y terceros, debe asegurarse de que ciertos sistemas dentro de su infraestructura logren EAL7 en el modelo de evaluación Common Criteria.

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 devolver el servidor al estado operativo. Durante ese tiempo, el personal de la oficina principal no pudo acceder a la información importante de recursos humanos almacenada en el servidor afectado.

Se espera que los usuarios utilicen un cifrado simétrico y asimétrico para garantizar la confidencialidad de los datos. Debe implementar un sistema adecuado para administrar las claves de cifrado, los hash y los certificados digitales en todos los equipos cliente. También debe proteger las contraseñas, cifrar las unidades y administrar los derechos digitales para estas mismas computadoras.

La integridad de los datos se ha convertido en una preocupación cada vez más seria para los archivos creados y mantenidos por el departamento de investigación. Debe implementar la solución adecuada para estos archivos. Todos los archivos se encuentran en un único servidor al que solo pueden acceder los usuarios del departamento de investigación.

Nunca se completó formalmente un análisis de riesgos completo para toda la organización. Se le ha pedido que encabece este proyecto. Como parte de este proceso, debe identificar las amenazas geográficas para cada oficina individual.

Su organización desplegará dos oficinas internacionales a finales de este año. Se le ha invitado a participar en la selección de instalaciones y el proceso de seguridad interna del edificio para proporcionar información de seguridad particular.

Se le ha pedido que identifique cualquier amenaza natural que pueda afectar a todas y cada una de las oficinas en los Estados Unidos. ¿Cuál de los siguientes debería incluir?

A) cortes eléctricos, de comunicaciones y de servicios públicos

B) huelgas, disturbios y actos terroristas

C) explosiones, vandalismo y fraude

D) tornados, inundaciones y terremotos

Pregunta # 91 de 193

ID de pregunta: 1192924

¿Qué modelo de control de acceso utiliza la regla de seguridad simple, la regla de propiedad de estrella y la regla de propiedad de estrella fuerte?

A) Modelo Biba

B) Modelo Bell-LaPadula

C) Modelo de Clark-Wilson

D) Modelo de pared chino

Pregunta # 92 de 193

ID de pregunta: 1105101

Como parte del plan de seguridad de su organización, se colocan guardias de seguridad en cada entrada de acceso público a las instalaciones. En el contexto de la seguridad física, ¿qué afirmación sobre el personal de los guardias de seguridad es la más apropiada?

A) El personal de los guardias de seguridad es uno de los controles administrativos en una arquitectura de seguridad en capas.

B) El personal de los guardias de seguridad actúa como la última línea de defensa para asegurar la infraestructura de la instalación.

C) El personal de los guardias de seguridad es una contramedida rentable para reducir el riesgo de seguridad física.

D) El personal de los guardias de seguridad es la contramedida más cara para reducir el riesgo de seguridad física.

Pregunta # 93 de 193

ID de pregunta: 1105084

Al desarrollar el sitio web de su organización, el desarrollador web debe asegurarse de que ciertos mensajes se transmitan de forma segura. ¿Qué tecnología sería la mejor opción para este propósito?

A) S-HTTP

B) HTTP

C) COLOCAR

D) HTTPS

Pregunta # 94 de 193

ID de pregunta: 1105094

Su organización ha decidido construir una nueva instalación. Durante la fase de diseño, se le pide que considere la combustibilidad de los materiales de construcción. ¿Qué elementos NO debería considerar para este problema?

A) techos

B) puertas

C) paredes

D) ventanas

Pregunta # 95 de 193

ID de pregunta: 1105075

¿Qué contiene una CRL X.509?

A) claves privadas

B) números seriales

C) Certificados digitales

D) claves públicas

Pregunta # 96 de 193

ID de pregunta: 1113943

Su organización protege su centro de datos mediante un candado inteligente. Cada usuario tiene un código único para ingresar en la cerradura inteligente para acceder al centro de datos. El código está configurado para permitir el acceso solo durante ciertas horas y días. ¿Qué tipo de bloqueo se implementa?

A) cerradura de combinación

B) bloqueo de cifrado

C) cerradura de vaso

D) cerradura mecanica

Pregunta # 97 de 193

ID de pregunta: 1113934

Su organización está trabajando con un socio internacional en un producto nuevo e innovador. Toda la comunicación relacionada con esto debe cifrarse utilizando un algoritmo simétrico de dominio público. ¿Qué algoritmo debería utilizar?

A) DESDE

B) OCURRENCIA

C) 3DES

D) Pez globo

Pregunta # 98 de 193

ID de pregunta: 1114712

¿Cuál es el primer paso para diseñar un programa de seguridad física eficaz?

A) Determine las líneas de base de desempeño a partir de niveles de riesgo aceptables.

B) Realice el análisis de riesgos de seguridad física.

C) Identifique el equipo del programa de seguridad física.

D) Defina un nivel de riesgo aceptable para cada amenaza a la seguridad física.

Pregunta # 99 de 193

ID de pregunta: 1104956

¿Qué libro de la serie Rainbow cubre problemas de seguridad para redes y componentes de red?

A) el libro rojo

B) el libro negro

B) el libro negro

C) el libro naranja

D) el libro verde

Pregunta # 100 de 193

ID de pregunta: 1113940

Recientemente, la gerencia se ha preocupado de que RFI esté causando problemas en las instalaciones de su organización. ¿Qué puede provocar este tipo de interferencias?

A) motor electrico

B) cableado eléctrico

C) iluminación fluorescente

D) relámpago

Pregunta # 101 de 193

ID de pregunta: 1105031

Recientemente ha implementado una infraestructura de clave pública en una red de Windows Server 2008. Se emitirán certificados digitales a todos los usuarios y ordenadores válidos. ¿Qué afirmación NO es cierta sobre los certificados digitales?

A) La garantía de nivel 1 para un certificado digital solo requiere una dirección de correo electrónico.

B) X.509 es un estándar de certificado digital.

C) Los certificados digitales proporcionan autenticación antes de enviar información de forma segura a un servidor web.

D) La garantía de nivel 2 para un certificado digital solo verifica el nombre y la dirección de correo electrónico de un usuario.

Pregunta # 102 de 193

ID de pregunta: 1113923

¿Qué enunciado es verdadero para las computadoras con conjuntos de instrucciones complejos (CISC)?

A) Las llamadas de acceso a la memoria principal son menores en comparación

con RISC.

B) Se requiere explícitamente que el programador llame a las funciones de carga y almacenamiento.

C) Un conjunto de instrucciones ejecuta una única operación de bajo nivel.

D) El conjunto de instrucciones admite todos los lenguajes de programación de bajo nivel.

Pregunta # 103 de 193

ID de pregunta: 1105054

¿Qué es la agrupación de claves?

A) el acto de transformar datos en un formato legible

B) la práctica de romper sistemas criptográficos

C) cuando dos claves diferentes cifran un mensaje de texto sin formato en el mismo texto cifrado

D) el tiempo, el esfuerzo y los recursos estimados necesarios para romper un sistema criptográfico

Pregunta # 104 de 193

ID de pregunta: 1104993

¿En qué situación representa el mayor peligro el cross-site scripting (XSS)?

A) Un usuario accede a un sitio web de contenido estático.

B) Un usuario accede a un sitio web de acceso público.

C) Un usuario accede al sitio de una organización financiera utilizando sus credenciales de inicio de sesión.

D) Un usuario accede a un sitio basado en conocimientos utilizando sus credenciales de inicio de sesión.

Pregunta # 105 de 193

ID de pregunta: 1192932

Haga clic en cada uno de los títulos de los escenarios para expandir o contraer su contenido. Debe leer el escenario

completo para responder la pregunta.

Fondo

Usted es un profesional de seguridad contratado recientemente por una institución financiera que cotiza en bolsa para ayudar a administrar la seguridad de la organización. La oficina principal de la empresa se encuentra en Nueva York, NY, y tiene sucursales adicionales en todo Estados Unidos.

Asuntos actuales

La infraestructura actual incluye servidores Windows, servidores UNIX, clientes Windows, clientes Mac, dispositivos móviles Windows y dispositivos móviles Mac implementados en todas las oficinas. El departamento de TI de la empresa tiene un gran personal ubicado en la oficina de Nueva York. Cada sucursal tiene un pequeño personal de TI local que solo se ocupa de los problemas de esa sucursal.

Ha identificado varios casos en los que los ataques contra los sistemas cliente no se evitaron o no se detectaron a nivel de cliente porque no se implementaron controles para prevenir el ataque. Se robaron datos de algunos dispositivos. Toda una sucursal se infectó con malware y virus y requirió varios días de tiempo de recuperación, lo que significó una pérdida de ingresos. Por último, recientemente descubrió que varios sistemas cliente tienen instaladas versiones de SO sin licencia. Debe asegurarse de que se implementen los controles adecuados para mitigar estos riesgos.

En una auditoría reciente, descubrió que varios dispositivos móviles carecían de las actualizaciones adecuadas para sus sistemas operativos o aplicaciones. Además, los usuarios habían desactivado las funciones de limpieza remota y ubicación GPS en estos dispositivos y habían instalado varias aplicaciones no autorizadas. Necesita una solución para mitigar estos riesgos y controlar la configuración y las aplicaciones de los dispositivos móviles cuando esos dispositivos están conectados a la empresa.

Debido a varios contratos entre su empresa y terceros, debe asegurarse de que ciertos sistemas dentro de su infraestructura logren EAL7 en el modelo de evaluación Common Criteria.

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 devolver el servidor al estado operativo. Durante ese tiempo, el personal de la oficina principal no pudo acceder a la información importante de recursos humanos almacenada en el servidor afectado.

Se espera que los usuarios utilicen un cifrado simétrico y asimétrico para garantizar la confidencialidad de los datos. Debe implementar un sistema adecuado para administrar las claves de cifrado, los hash y los certificados digitales en todos los equipos cliente. También debe proteger las contraseñas, cifrar las unidades y administrar los derechos digitales para estas mismas computadoras.

La integridad de los datos se ha convertido en una preocupación cada vez más seria para los archivos creados y mantenidos por el departamento de investigación. Debe implementar la solución adecuada para estos archivos. Todos los archivos se encuentran en un único servidor al que solo pueden acceder los usuarios del departamento de investigación.

Nunca se completó formalmente un análisis de riesgos completo para toda la organización. Se le ha pedido que

Nunca se completó formalmente un análisis de riesgos completo para toda la organización. Se le ha pedido que encabece este proyecto. Como parte de este proceso, debe identificar las amenazas geográficas para cada oficina individual.

Su organización desplegará dos oficinas internacionales a finales de este año. Se le ha invitado a participar en la selección de instalaciones y el proceso de seguridad interna del edificio para proporcionar información de seguridad particular.

¿Qué debería implementar para ayudar con los problemas del dispositivo móvil?

A) políticas de grupo
B) Kerberos
C) MDM
D) Directorio Activo

Pregunta # 106 de 193

ID de pregunta: 1132519

¿Qué tecnología web ofrece el mayor nivel de seguridad?

A) ActiveX
B) JavaScript
C) HTTPS
D) S-HTTP

Pregunta # 107 de 193

ID de pregunta: 1105028

¿Cuál es el problema principal de la criptografía simétrica?

A) implementación de hardware y software
B) gestión de claves
C) diferentes claves para cifrado y descifrado
D) alto procesamiento

Pregunta # 108 de 193

ID de pregunta: 1105059

Su organización ha decidido implementar el algoritmo asimétrico Diffie-Hellman. ¿Qué afirmación es verdadera sobre el intercambio de claves de este algoritmo?

A) Los usuarios autorizados no necesitan intercambiar claves secretas.

B) Los usuarios autorizados intercambian claves públicas a través de un medio seguro.

C) Los usuarios no autorizados intercambian claves públicas a través de un medio no seguro.

D) Los usuarios autorizados intercambian claves secretas a través de un medio no seguro.

Pregunta # 109 de 193

ID de pregunta: 1105009

¿Qué son los servicios de confidencialidad?

A) firmas digitales

B) esquemas de autenticación

C) Matrices RAID

D) tecnologías de encriptación

Pregunta # 110 de 193

ID de pregunta: 1114708

Su organización implementa cifrado híbrido para brindar un alto nivel de protección de sus datos. ¿Qué afirmaciones son ciertas sobre este tipo de cifrado?

una. La clave secreta protege las claves de cifrado.

B. Las claves públicas descifran la clave secreta para su distribución.

C. La criptografía asimétrica se utiliza para la distribución segura de claves.

D. El algoritmo simétrico genera claves públicas y privadas.

mi. La criptografía simétrica se utiliza para el cifrado y descifrado de datos.

A) opción b

B) opción d

C) opción e

D) opción a

MI) opciones c y d

F) opciones ayb

GRAMO) opciones c y e

H) opción c

Pregunta # 111 de 193

ID de pregunta: 1113944

¿Obtener acceso no autorizado al centro de datos mediante el uso de las credenciales de otro usuario al seguirlo al interior del edificio es un ejemplo de qué opción?

A) torniquete

B) cepo

C) intrusión

D) llevar a cuestas

Pregunta # 112 de 193

ID de pregunta: 1114707

¿Qué opción es un algoritmo de cifrado de clave pública?

A) OCURRENCIA

B) Barrilete

C) RSA

D) RC5

Pregunta # 113 de 193

ID de pregunta: 1113939

¿Qué elemento puede representar una amenaza para los sistemas eléctricos en una instalación de procesamiento de información?

A) un hundimiento

B) un destructor de picos

C) una fuente de alimentación ininterrumpida (UPS)

D) un acondicionador de línea eléctrica

Pregunta # 114 de 193

ID de pregunta: 1105073

¿Qué entidad debe certificar el par de claves públicas de una CA raíz?

A) una CA externa

B) una CA subordinada

C) un servidor Kerberos

D) la CA raíz

Pregunta # 115 de 193

ID de pregunta: 1105038

¿Qué cifrado se basa en las pistas de los factores físicos en lugar del criptosistema de hardware o software?

A) un cifrado de transposición

B) un cifrado de ocultación

C) un cifrado DES

D) un cifrado 3DES

Pregunta # 116 de 193

ID de pregunta: 1113919

¿Qué dos factores aseguran que la información esté compartimentada en el modelo de flujo de información?

A) clasificación y flujo

A) clasificación y flujo

B) clasificación y rol

C) clasificación y necesidad de saber

D) papel y necesidad de saber

Pregunta # 117 de 193

ID de pregunta: 1111705

¿Qué nivel del Libro Naranja se considera protecciones obligatorias y se basa en el modelo de seguridad de Bell-LaPadula?

A) D

B) B

C) A

D) C

Pregunta # 118 de 193

ID de pregunta: 1104962

¿Qué sección del documento Requisitos mínimos de seguridad para el sistema operativo multiusuario (NISTIR 5153) aborda la responsabilidad del usuario de un extremo a otro?

A) control de acceso

B) integridad de los datos

C) integridad del sistema

D) auditoría

Pregunta # 119 de 193

ID de pregunta: 1105127

Se le ha pedido que implemente un plan mediante el cual la sala de servidores de su empresa permanecerá en línea durante tres horas después de un corte de energía. Esto le dará a su departamento de TI el tiempo suficiente para implementar el sitio alternativo. ¿Qué tecnología sería la mejor en este escenario?

A) REDADA

B) generador de respaldo

C) UPS

D) agrupamiento

Pregunta # 120 de 193

Pregunta ID: 1105025

Todo lo siguiente afecta la fuerza del cifrado, EXCEPTO:

A) la longitud de los datos que se cifran

B) el secreto de la llave

C) el algoritmo

D) la longitud de la llave

Pregunta # 121 de 193

Pregunta ID: 1105085

Debe asegurarse de que un solo documento transmitido desde su servidor web esté cifrado. Debe implementar esta solución de la manera más sencilla posible.

¿Qué deberías hacer?

A) Utilice JavaScript.

B) Utilice HTTPS.

C) Utilice ActiveX.

D) Utilice S-HTTP.

Pregunta # 122 de 193

ID de pregunta: 1113935

¿Cuál es el propósito de la autenticación en un criptosistema?

A) verificar la identidad del usuario o del sistema

B) convertir la información en datos ininteligibles

C) Asegurarse de que el remitente de los datos no pueda negar haber enviado los

datos.

D) Asegurarse de que los datos no hayan sido modificados por un usuario no autorizado.

Pregunta # 123 de 193

ID de pregunta: 1113920

¿Qué modelo de seguridad garantiza que las actividades realizadas en un nivel de seguridad superior no afecten a las actividades en un nivel de seguridad inferior?

A) Modelo Brewer y Nash

B) modelo de flujo de información

C) Modelo Biba

D) modelo de no interferencia

Pregunta # 124 de 193

ID de pregunta: 1105125

Se le ha pedido a un usuario de TI que reemplace un disco duro en un servidor. Sin embargo, cuando el usuario abre la caja, se da cuenta de que el disco duro actual está conectado a la abertura del disco duro mediante un cable de acero. Indica que no sabe dónde está la llave. ¿Qué tipo de cerradura se describe?

A) trampa de cable

B) bloqueo de ranura

C) control del interruptor

D) control de puertos

Pregunta # 125 de 193

ID de pregunta: 1111723

Su organización ha decidido utilizar blocs de notas de una sola vez para asegurarse de que ciertos datos confidenciales estén protegidos. Todas las siguientes afirmaciones son verdaderas con respecto a este tipo de criptosistema, EXCEPTO:

A) Cada almohadilla de un solo uso se puede usar solo una vez.

B) La almohadilla debe distribuirse y almacenarse de manera segura.

C) El bloc debe ser tan largo como el mensaje.

D) El pad debe estar formado por valores secuenciales.

Pregunta # 126 de 193

ID de pregunta: 1114702

¿Qué ataques se consideran ataques de control de acceso comunes?

una. suplantación

B. phreaking

C. Inundación SYN

D. ataques de diccionario

mi. ataques de fuerza bruta

A) opción b

B) todas las opciones

C) opción a

D) opción d

MI) opción e

F) opciones a, d y e solamente

GRAMO) Todas las opciones byc

H) opción c

Pregunta # 127 de 193

ID de pregunta: 1104944

¿Qué procesos definen el modo supervisor?

A) procesos que se ejecutan en los anillos exteriores de protección

B) procesos sin mecanismo de protección

C) Procesos en el anillo de protección exterior que tienen más privilegios.

D) procesos que se ejecutan en los anillos de protección internos

Pregunta # 128 de 193

ID de pregunta: 1154292

¿Qué declaraciones NO definen los requisitos de un kernel de seguridad?

una. Se debe verificar que el monitor de referencia sea correcto.

B. El monitor de referencia debe proporcionar aislamiento de proceso.

C. El kernel de seguridad debe verificarse de manera integral.

D. El monitor de referencia debe implementar un método para eludir la seguridad.

A) opción c
B) opciones by d
C) opción a
D) opciones ayc
MI) opción b
F) opción d

Pregunta # 129 de 193

ID de pregunta: 1192930

Usted es responsable de administrar las computadoras virtuales en su red. ¿Qué pauta es importante al administrar computadoras virtuales?

A) Implemente un firewall solo en la computadora host.
B) Aísle la computadora host y cada computadora virtual entre sí.
C) Actualice el sistema operativo y las aplicaciones solo en la computadora host.
D) Instale y actualice el programa antivirus solo en la computadora host.

Pregunta # 130 de 193

ID de pregunta: 1104945

¿Qué sucede cuando se produce una falla de la base informática confiable (TCB) como resultado de un proceso con menos privilegios que intenta acceder a segmentos de memoria restringidos?

A) Se requiere la reinstalación del sistema operativo.

B) El sistema entra en modo de mantenimiento.

C) Se requiere la intervención del administrador.

D) El sistema se reinicia inmediatamente.

Pregunta # 131 de 193

ID de pregunta: 1105080

Su organización ha firmado recientemente un contrato con una agencia gubernamental. El contrato requiere que implemente el estándar X.509. ¿Qué rige este estándar?

A) IPSec

B) HTTP

C) PKI

D) IKE

Pregunta # 132 de 193

ID de pregunta: 1105033

¿Qué afirmación NO es verdadera para un algoritmo RSA?

A) RSA puede prevenir ataques man-in-the-middle.

B) RSA es un algoritmo de clave pública que realiza tanto el cifrado como la autenticación.

C) Un algoritmo RSA es un ejemplo de criptografía simétrica.

D) Los algoritmos de cifrado RSA no tratan con logaritmos discretos.

MI) RSA utiliza firmas de claves públicas y privadas para la verificación de la integridad.

Pregunta # 133 de 193

ID de pregunta: 1114701

La gerencia de su organización se ha dado cuenta recientemente de que el movimiento de Internet de las cosas (IoT) ha dado lugar a muchos problemas de seguridad. Le han pedido que identifique algunas de las vulnerabilidades presentadas por IoT de la siguiente lista:

A. interfaz web de gestión insegura

B. Autenticación insuficiente o inexistente

C. falta de cifrado de transporte

D. software / firmware inseguro

E. seguridad física insuficiente o inexistente

¿Cuál aplicaría?

A) A, B, C y D
B) Todo lo anterior
C) Solo A y B
D) Solo C y D
MI) Solo D y E
F) Solo B y C

Pregunta # 134 de 193

ID de pregunta: 1111711

¿Qué término es una evaluación de los componentes de seguridad y su cumplimiento antes de la aceptación formal?

A) control de seguridad
B) acreditación
C) Certificación
D) control del sistema de información

Pregunta # 135 de 193

ID de pregunta: 1105128

Debe asegurarse de que los datos de los equipos de su organización no se pierdan cuando se produce un corte de energía. Los usuarios deben tener suficiente tiempo para guardar sus datos si ocurre un corte de energía. ¿Qué deberías usar?

A) un aspersor
B) una cerradura de puerta
C) un UPS

D) un aire acondicionado

Pregunta # 136 de 193

ID de pregunta: 1105012

Mientras investiga la seguridad del protocolo de Internet (IPSec), descubre que utiliza el intercambio de claves de Internet (IKE). ¿Cuál es el objetivo principal de IKE?

A) para cifrar los datos a través de la red

B) para gestionar las asociaciones de seguridad (SA) en la red

C) para reproducir los datos en la red

D) para autenticar los datos a través de la red

Pregunta # 137 de 193

ID de pregunta: 1105107

Varias habitaciones de sus instalaciones tienen ruido de modo transversal. ¿Qué factor influye en la generación de este ruido?

A) presurización positiva

B) diferencia entre cables calientes y de tierra

C) diferencia entre cables vivos y neutros

D) fuente de poder ininterrumpible

Pregunta # 138 de 193

ID de pregunta: 1105026

La gerencia le ha pedido que investigue el cifrado y haga una recomendación sobre qué técnica de cifrado utilizar. Durante esta investigación, examinará varios criptosistemas diferentes. ¿Qué parámetro determina su fuerza?

A) la longitud de la llave

B) la infraestructura de gestión de claves

C) el marco de seguridad

D) el código de autenticación del mensaje (MAC)

Pregunta # 139 de 193

ID de pregunta: 1111722

Está preparando una propuesta de gestión sobre el valor de utilizar la criptografía para proteger su red. ¿Qué afirmación es verdadera sobre la criptografía?

A) La disponibilidad es una de las principales preocupaciones de la criptografía.

B) La criptografía se utiliza para detectar divulgaciones fraudulentas.

C) Las claves en criptografía pueden hacerse públicas.

D) La gestión de claves es una de las principales preocupaciones de la criptografía.

Pregunta # 140 de 193

ID de pregunta: 1105056

¿Cuál es el propósito de la tecnología BitLocker?

A) Bloquea su computadora para que no se pueda iniciar.

B) Cifra los datos a medida que se transmiten a través de una red.

C) Bloquea su disco duro para que no se pueda iniciar.

D) Cifra el contenido de la unidad para que no se puedan robar datos.

Pregunta # 141 de 193

ID de pregunta: 1105002

La dirección de su organización ha dedicado tiempo recientemente a analizar los ataques contra las empresas y su infraestructura. Durante la reunión, se discutió el ataque Stuxnet. ¿Contra qué tipo de sistema ocurrió este ataque?

A) Kerberos

B) disminución

C) VoIP

D) RADIO

Pregunta # 142 de 193

ID de pregunta: 1105076

¿Qué entidad emite certificados digitales?

A) BDC

B) QUE

C) corriente continua

D) EFS

Pregunta # 143 de 193

ID de pregunta: 1105052

¿Cuál de las siguientes fue una máquina de rotor alemana utilizada en la Segunda Guerra Mundial?

A) Lucifer

B) Proyecto Ultra

C) Enigma

D) Máquina púrpura

Pregunta # 144 de 193

ID de pregunta: 1105068

¿Qué afirmación NO es cierta sobre el criptoanálisis?

A) Es una herramienta que se utiliza para desarrollar un criptosistema seguro.

B) Se utiliza para probar la fuerza de un algoritmo.

C) Es un proceso de intentar la ingeniería inversa de un criptosistema.

D) Se utiliza para falsificar señales codificadas que serán aceptadas como auténticas.

Pregunta # 145 de 193

ID de pregunta: 1114694

¿Qué opciones son componentes del kernel de seguridad?

una. software

B. hardware

C. monitor de referencia

D. base informática confiable

A) opciones ayb

B) opciones c y d

C) opción d

D) opción a

MI) opción b

F) opción c

Pregunta # 146 de 193

ID de pregunta: 1111729

¿Qué control incluye mantraps y torniquetes?

A) control ambiental

B) control administrativo

C) control tecnico

D) Control físico

Pregunta # 147 de 193

ID de pregunta: 1104960

¿Qué entidad puede operar como sujeto y como objeto?

A) programa

B) grupo

C) expediente

D) usuario

Pregunta # 148 de 193

ID de pregunta: 1113938

Su organización ha identificado varios sitios como opciones para la reubicación. Una de las ubicaciones tiene un sistema de drenaje positivo. ¿Qué asegura este sistema con referencia a la seguridad física?

A) el aire sale de la habitación tan pronto como se abre la puerta

B) el contenido de las tuberías de agua, gas y vapor fluye hacia el edificio

C) el suministro limpio y constante de energía desde las cajas de distribución eléctrica hasta los dispositivos eléctricos

D) el contenido de las tuberías de agua, gas y vapor sale del edificio

Pregunta # 149 de 193

ID de pregunta: 1104950

¿Qué diferencia a ITSEC de TCSEC?

A) La funcionalidad y la seguridad son evaluadas por separado por ITSEC.

B) Las prácticas de desarrollo y la documentación se evalúan como parte de la funcionalidad del sistema.

C) Los servicios de auditoría y autenticación no son proporcionados a los usuarios por ITSEC.

D) Las calificaciones de ITSEC no se asignan al Libro Naranja.

Pregunta # 150 de 193

ID de pregunta: 1114697

¿Cuál es la mejor descripción de la informática de conjuntos de instrucciones reducidos (RISC)?

A) computación usando instrucciones que realizan muchas operaciones por instrucción

B) procesamiento que ejecuta una instrucción a la vez

C) procesamiento que permite la ejecución concurrente de múltiples instrucciones

D) Computación usando instrucciones que son más simples y requieren menos reloj.
ciclos para ejecutar

Pregunta # 151 de 193

ID de pregunta: 1114717

¿Qué afirmaciones son verdaderas sobre el halón como agente de extinción de incendios?

una. El halón es seguro para los humanos.

B. El halón se ocupa de la categoría de fuego de Clase A.

C. El gas halón suprime el fuego mediante una reacción química.

D. FM-200 es un sustituto del halón aprobado por la EPA.

mi. Actualmente, el halón está aprobado por la Agencia de Protección Ambiental (EPA).

A) opción a

B) opción d

C) opción b

D) opción e

MI) opciones b, c y d

F) opción c

GRAMO) opciones c y d

H) opciones ayb

Pregunta # 152 de 193

ID de pregunta: 1114710

Usted es parte del equipo de diseño de las instalaciones de procesamiento de información de una organización. ¿Qué opción u opciones representan posibles riesgos de seguridad física para el diseño?

una. suplantación

B. robo fisico

C. fallo de alimentación

D. daño de hardware

mi. ataque de denegación de servicio (DoS)

A) opción b

B) opción e

C) opción d

D) opciones a, byc

MI) opciones b, c y d

F) opción c

GRAMO) opciones c, d y e

H) opción a

Pregunta # 153 de 193

ID de pregunta: 1192935

Eres el administrador de seguridad de una organización. La gerencia decide que todas las comunicaciones en la red deben cifrarse utilizando el algoritmo estándar de cifrado de datos (DES). ¿Qué afirmación es verdadera de este algoritmo?

A) El tamaño de clave efectivo de DES es de 64 bits.

B) Un cifrado DES de 56 bits es 256 veces más seguro que un cifrado DES de 40 bits.

C) Un algoritmo DES utiliza 32 rondas de cálculo.

D) Un algoritmo Triple DES (3DES) utiliza 48 rondas de cálculo.

Pregunta # 154 de 193

ID de pregunta: 1111717

¿Qué afirmación es verdadera de FIPS 140?

A) FIPS se ocupa de productos de hardware.

B) FIPS solo se ocupa de software criptográfico.

C) FIPS no valida el software para que lo utilicen agencias gubernamentales.

D) FIPS especifica los requisitos de seguridad para los módulos criptográficos de hardware y software.

Pregunta # 155 de 193

ID de pregunta: 1111730

¿Qué práctica de seguridad NO aborda la protección física y ambiental de una instalación?

¿Qué práctica de seguridad NO aborda la protección física y ambiental de una instalación?

A) Los sistemas de alerta de inundaciones se actualizan una vez al año.

B) Los códigos de entrada en la instalación se cambian a intervalos regulares.

C) La entrada y salida de la instalación son monitoreadas continuamente por CCTV.

D) Se toman medidas para evitar el robo de información por parte de personas no autorizadas.

Pregunta # 156 de 193

ID de pregunta: 1105055

¿Qué tecnología requiere hardware Trusted Platform Module (TPM)?

A) IPSec

B) NTFS

C) BitLocker

D) EFS

Pregunta # 157 de 193

ID de pregunta: 1104989

Su organización ha decidido implementar la computación en la nube y ha configurado la plataforma como servicio (PaaS) con un proveedor de la nube. ¿Cuál es el enfoque principal de este tipo de implementación en la nube?

A) gestión de máquinas virtuales

B) control de acceso

C) protección de Datos

D) gestión de acceso a aplicaciones

Pregunta # 158 de 193

ID de pregunta: 1104998

¿Cuál de las siguientes NO es una contramedida para mitigar los ganchos de mantenimiento?

A) Cifre toda la información confidencial contenida en el sistema.

B) Utilice un IDS basado en host para registrar cualquier intento de acceder al sistema mediante uno de estos ganchos.

C) Implementar auditorías para complementar el IDS.

D) Asegúrese de que, si los conjuntos de instrucciones críticos no se ejecutan en orden y en su totalidad, los cambios que realicen se reviertan o se evitan.

Pregunta # 159 de 193

ID de pregunta: 1105024

¿Cuál es otro término para la fuerza de la criptografía?

A) vector de inicialización

B) Llave pública

C) factor de trabajo

D) llave privada

Pregunta # 160 de 193

ID de pregunta: 1105096

Su organización está utilizando el enfoque de Prevención del Crimen a través del Diseño Ambiental (CPTED) para asegurarse de que su sitio esté diseñado correctamente. ¿Qué faceta de este enfoque incluye la colocación de puertas, cercas, iluminación y jardinería?

A) endurecimiento del objetivo

B) vigilancia natural

C) refuerzo territorial

D) control de acceso natural

Pregunta # 161 de 193

ID de pregunta: 1105042

¿Qué produce sumas de comprobación de 160 bits?

A) AES

B) DESDE

C) MD5

D) SHA

Pregunta # 162 de 193

ID de pregunta: 1132516

¿Qué ataque envía mensajes no solicitados a través de una conexión Bluetooth?

A) gato azul

B) spam

C) bluesnarfing

D) conducción de guerra

Pregunta # 163 de 193

ID de pregunta: 1113942

¿Qué NO es un componente de una tarjeta de detección de sistema de transpondedor?

A) espectro ensanchado

B) transmisor

C) batería

D) receptor

Pregunta # 164 de 193

ID de pregunta: 1105051

Dados dos mensajes, M1 y M2, ¿cuál es el resultado MENOS probable cuando se usa la misma función hash unidireccional, H, para cifrar los mensajes?

A) H (M1)> H (M2)

B) H (M1) no es igual a H (M2)

C) H (M1) = H (M2)

D) H (M1) <H (M2)

Pregunta # 165 de 193

ID de pregunta: 1192927

Usted es responsable de administrar el entorno de virtualización de su empresa. ¿Qué función NO debería permitirse en un host de virtualización?

A) implementando IPsec

B) implementando un firewall

C) monitorear los registros de eventos

D) navegando en Internet

Pregunta # 166 de 193

ID de pregunta: 1192938

¿Qué métodos de extinción se recomiendan cuando el papel, los laminados y los muebles de madera son los elementos de un incendio en la instalación?

una. Halón

B. Agua

c. Ácido de soda

D. Polvo seco

A) opciones c y d

B) opción b

C) opción d

D) opciones ayb

MI) opciones byc

F) opción a

GRAMO) opción c

Pregunta # 167 de 193

ID de pregunta: 1105062

¿Qué algoritmo de hash se diseñó para usarse con el Estándar de firma digital (DSS)?

A) Resumen de mensajes 5 (MD5)

B) HAVAL

C) Algoritmo hash seguro (SHA)

D) Tigre

Pregunta # 168 de 193

ID de pregunta: 1104990

Su empresa aloja varios sitios web públicos en su servidor web. Algunos de los sitios implementan el protocolo de capa de sockets seguros (SSL). ¿Qué afirmación NO es cierta sobre este protocolo?

A) SSL opera en la capa de red del modelo OSI.

B) SSL versión 2 proporciona autenticación del lado del cliente.

C) SSL se utiliza para proteger las transacciones de Internet.

D) SSL tiene dos posibles longitudes de clave de sesión: 40 bits y 128 bits.

MI) SSL con TLS admite la autenticación tanto del servidor como del cliente.

Pregunta # 169 de 193

ID de pregunta: 1114706

Ha sido contratado como administrador de seguridad. La gerencia le informa que la red utiliza el cifrado SKIP. ¿Qué afirmación es verdadera de este protocolo?

A) SKIP es un protocolo de distribución de claves.

B) SKIP funciona respuesta por sesión.

C) SKIP es solo un protocolo de almacenamiento de claves.

D) SKIP implementa IKE para la distribución y administración de claves.

Pregunta # 170 de 193

ID de pregunta: 1105048

¿Cuál de las siguientes opciones NO se basa en el cifrado de Feistel?

A) CAST-128

D) Diffie-Hellman

B) Diffie-Hellman

C) Pez globo

D) Barrilete

Pregunta # 171 de 193

ID de pregunta: 1105093

La nueva instalación de su organización debe estar construida con material resistente al fuego. ¿Qué material se debe utilizar en la construcción de su marco?

A) acero

B) Madera pesada con una clasificación de fuego de una hora.

C) varillas de acero encajadas en muros de hormigón

D) madera aserrada sin tratar

Pregunta # 172 de 193

ID de pregunta: 1105021

¿Qué servicio proporcionado por un criptosistema es más importante para los militares?

A) integridad

B) no repudio

C) confidencialidad

D) autenticación

Pregunta # 173 de 193

ID de pregunta: 1114711

Su equipo tiene la tarea de identificar un sitio seguro para la infraestructura de las instalaciones de una organización. ¿Qué opción representa las consideraciones de visibilidad involucradas en este proceso?

una. Encendiendo

B. tipos de vecinos

C. controles ambientales

D. construcción de marcas y letreros

mi. televisión de circuito cerrado (CCTV)

A) opción e

B) opciones ayc

C) opción a

D) opción b

MI) opciones bye

F) opción d

GRAMO) opción c

H) opciones by d

Pregunta # 174 de 193

ID de pregunta: 1111734

El centro de datos secundario de su empresa experimentó un incendio recientemente. El equipo electrónico del centro de datos ha estado expuesto tanto al agua como al humo. Debe asegurarse de que todo el equipo se limpie correctamente. Todo el equipo se ha apagado. También ha abierto todos los gabinetes, paneles y cubiertas para permitir que el agua fluya. ¿Que deberías hacer después?

A) Limpie con alcohol o soluciones de alcohol freón, o rocíe con aerosoles de desplazamiento de agua.

B) Utilice disolventes de freón o alcohol de freón para rociar conectores, placas posteriores y placas de circuito impreso.

C) Rocíe un aerosol inhibidor de la corrosión para estabilizar las superficies de contacto de metal.

D) Mueva todo el equipo a un ambiente con controles adecuados de temperatura y humedad.

Pregunta # 175 de 193

ID de pregunta: 1104964

¿Qué afirmación es verdadera sobre el direccionamiento de memoria indirecto?

A) El campo de dirección apunta a una celda de memoria que contiene la dirección del operando.

del operando.

B) El campo de dirección contiene la dirección del operando.

C) Se utiliza un único acceso a la memoria para encontrar el operando.

D) No tiene referencia de memoria para recuperar datos.

Pregunta # 176 de 193

ID de pregunta: 1104996

¿Qué es un rootkit?

A) una aplicación que utiliza cookies de seguimiento para recopilar e informar las actividades de un usuario

B) una aplicación de software que muestra anuncios mientras se ejecuta la aplicación

C) un programa que se propaga a través de conexiones de red

D) una colección de programas que otorga a un pirata informático acceso administrativo a una computadora o red

Pregunta # 177 de 193

ID de pregunta: 1105036

¿Qué función binaria es la base del funcionamiento de un pad de un solo uso?

A) Y

B) XOR

C) XAND

D) O

Pregunta # 178 de 193

ID de pregunta: 1113930

Un cliente ha solicitado una computadora con un chip Clipper. ¿Qué es un chip Clipper?

A) Es un chip de módem.

B) Es un chip de encriptación.

C) Es un número de serie único en el chip de la computadora.

C) Es un número de serie único en el chip de la computadora.

D) Es un algoritmo de encriptación.

Pregunta # 179 de 193

ID de pregunta: 1114713

¿Qué métodos se pueden utilizar para reducir la electricidad estática?

una. aerosoles antiestáticos

B. menor humedad

C. pavimento antiestático

D. acondicionamiento de línea eléctrica

A) opción d

B) opción b

C) opción a

D) opciones by d

MI) opción c

F) opciones ayc

Pregunta # 180 de 193

ID de pregunta: 1111699

Su empresa tiene un sitio de comercio electrónico al que se puede acceder públicamente a través de Internet. El sitio de comercio electrónico acepta la información de la tarjeta de crédito de un cliente y luego procesa la transacción del cliente. ¿Qué norma o ley se aplicaría a este tipo de datos?

A) Basilea II

B) La Ley de Espionaje Económico de 1996

C) PCI DSS

D) SOX

Pregunta # 181 de 193

ID de pregunta: 1104970

¿Qué se entiende por el término a prueba de fallas?

A) la capacidad de un sistema para recuperarse automáticamente mediante un reinicio

B) la capacidad de un sistema para cambiar a un sistema de respaldo en caso de falla

C) la capacidad de un sistema para preservar un estado seguro antes y después de la falla

D) la capacidad de un sistema para terminar procesos cuando se identifica una falla

Pregunta # 182 de 193

ID de pregunta: 1104952

¿Qué componente NO forma parte de la información del perfil de protección utilizada por los Criterios Comunes para evaluar productos?

A) Calificación EAL

B) requisitos de aseguramiento

C) requisitos de funcionalidad

D) resultados de la prueba del producto

Pregunta # 183 de 193

ID de pregunta: 1105049

¿Qué chip implementa el estándar de cifrado en custodia de EE. UU. Y fue desarrollado por la Agencia de Seguridad Nacional (NSA)?

A) HSM

B) TPM

C) piedra angular

D) Chip de clipper

Pregunta # 184 de 193

ID de pregunta: 1114693

¿Cuál es la mejor descripción de un dominio de ejecución?

A) un área aislada que es utilizada por procesos confiables cuando se ejecutan en estado privilegiado

B) espacio de memoria aislado de otros procesos en ejecución en un multiprocesamiento
sistema

C) componentes que quedan fuera del perímetro de seguridad de la TCB

D) un canal de comunicación entre una aplicación y el kernel en la TCB

Pregunta # 185 de 193

ID de pregunta: 1132511

¿Qué enunciado es verdadero sobre la ingeniería inversa?

A) Se utiliza para ocultar los detalles de la funcionalidad de un objeto.

B) Elimina las fallas de seguridad del código objeto.

C) Implica la compilación de códigos de objeto de proveedor.

D) Analiza el funcionamiento de una aplicación.

Pregunta # 186 de 193

ID de pregunta: 1105088

¿Qué opción tendrá el menor efecto sobre la confidencialidad, integridad y disponibilidad de los recursos dentro de la organización?

A) llaves perdidas de la puerta

B) disco duro dañado

C) falla de energía primaria

D) computadora robada

Pregunta # 187 de 193

ID de pregunta: 1105004

Durante un reciente ataque a la red, un pirata informático utilizó tablas de arco iris para adivinar las contraseñas de la

red. ¿Qué tipo de ataque ocurrió?

A) escalada de privilegios

B) ataque de denegación de servicio

C) ataque de contraseña de fuerza bruta

D) ataque de ingeniería social

Pregunta # 188 de 193

ID de pregunta: 1104982

¿Qué tipos de computadoras son el objetivo de los ataques RedPill y Scooby Doo?

A) maquinas virtuales

B) Clientes de Windows Vista

C) servidores terminales

D) Computadoras con Windows Server 2008

Pregunta # 189 de 193

ID de pregunta: 1104980

¿Qué riesgo de seguridad representa el archivo /etc/hosts.equiv en un sistema UNIX?

A) Permite a todos los usuarios conectarse de forma remota sin autenticarse.

B) Permite a todos los usuarios editar localmente la configuración de DNS.

C) Permite que todos los usuarios se conecten localmente sin autenticarse.

D) Permite a todos los usuarios editar de forma remota la configuración de DNS.

Pregunta # 190 de 193

ID de pregunta: 1114704

Su organización debe asegurarse de que los mensajes estén protegidos de los piratas informáticos mediante cifrado. La gerencia decide implementar el algoritmo de hash seguro (SHA-1). ¿Qué afirmaciones NO son ciertas de este algoritmo?

una. SHA-1 produce un valor hash de 128 bits.

B. SHA-1 fue diseñado por NIST y NSA.

C. SHA-1 es una función hash bidireccional de longitud variable.

D. SHA-1 fue diseñado para su uso en firmas digitales.

A) opción a
B) opción c
C) opciones by d
D) opción d
MI) opción b
F) opciones ayc

Pregunta # 191 de 193

ID de pregunta: 1114690

¿Qué características de un sistema son evaluadas por los criterios de evaluación de sistemas informáticos de confianza (TCSEC)?

una. garantía

B. autenticidad

C. funcionalidad

D. tiempo de respuesta

A) opciones by d
B) opción b
C) opción c
D) opción d
MI) opciones ayc
F) opción a
GRAMO) opciones ayb

Pregunta # 192 de 193

Pregunta ID: 1105043

¿Qué asegura el código de autenticación de mensajes (MAC)?

A) repetición del mensaje

B) Integridad del mensaje

C) confidencialidad del mensaje

D) disponibilidad de mensajes

Pregunta # 193 de 193

ID de pregunta: 1105089

¿Por qué los archivos de controladores de dispositivo deben estar firmados digitalmente?

A) para asegurarse de que los instale un usuario de confianza

B) para asegurarse de que no se modifiquen después de la instalación

C) para asegurarse de que son de un editor de confianza

D) para registrar la marca de tiempo de instalación