CISSP - Glosario

3DES *Ver* Triple DES (3DES).

802.1X Un protocolo de acceso al puerto que protege las redes a través de la autenticación. Se utiliza ampliamente en entornos inalámbricos.

802.11a Un estándar de comunicación que opera en la frecuencia de 5 GHz con una velocidad máxima de 54 Mbps.

802.11ac Un estándar de comunicación que opera en la frecuencia de 5 GHz con una velocidad máxima de al menos 1 gigabit por segundo (Gbps) y un rendimiento de enlace único de 500 megabits por segundo (Mbps).

802.11b Un estándar de comunicación que opera en la frecuencia de 2.4 GHz con una velocidad máxima de 11 Mbps.

802.11f Un estándar para la comunicación entre puntos de acceso.

802.11g Un estándar de comunicación que opera en la frecuencia de 2,4 GHz con una velocidad máxima de 54 Mbps.

802.11n Un estándar de comunicación que opera tanto en las frecuencias de 2,4 GHz como en las de 5,0 GHz con una velocidad teórica máxima de 600 Mbps.

direccionamiento absoluto Direcciona todo el espacio de memoria principal.

abstracción El proceso de quitar o quitar características de algo para reducirlo a un conjunto de características esenciales.

pruebas de aceptación Pruebas para garantizar que el cliente (ya sea interno o externo) está satisfecho con la funcionalidad del software.

agregación de acceso Se produce cuando los usuarios obtienen más acceso en más sistemas. A menudo se usa como sinónimo de arrastramiento de privilegios.

control de acceso El medio por el cual se permite o deniega la capacidad de un sujeto para comunicarse con un objeto o acceder a un objeto en función de los requisitos de seguridad de una organización.

lista de control de acceso (ACL) Una tabla que consta de los derechos de acceso que los sujetos tienen a un objeto determinado. Una ACL es sobre el objeto.

matriz de control de acceso Una tabla que consta de una lista de sujetos, una lista de objetos y una lista de las acciones que un sujeto puede realizar en cada objeto.

directiva de control de acceso Una directiva de seguridad que define el método para identificar y autenticar a los usuarios y el nivel de acceso que se concede a los usuarios.

punto de acceso Un transmisor y receptor inalámbricos que se conecta a la parte cableada de la red y proporciona un punto de acceso a esta red para dispositivos inalámbricos.

administración de cuentas Implica la adición y eliminación de cuentas a las que se concede acceso a sistemas o redes. También implica cambiar los permisos o privilegios concedidos a esas cuentas.

contabilidad El proceso mediante el cual los resultados de la auditoría se utilizan para responsabilizar a los usuarios y las organizaciones por sus acciones o inacción.

acreditación La aceptación formal de la adecuación de la seguridad general de un sistema por parte de la dirección.

ACL *Consulte* la lista de control de acceso (ACL).

sistemas acústicos Sistemas de detección que utilizan micrófonos estratégicamente colocados para detectar cualquier sonido realizado durante una entrada forzada.

vidrio acrílico Un tipo de vidrio hecho de acrílico de policarbonato que es mucho más fuerte que el vidrio regular, pero produce humos tóxicos cuando se quema.

analizador de vulnerabilidades activo (AVS) Puede tomar medidas para bloquear un ataque, como bloquear una dirección IP peligrosa, mientras que un escáner pasivo solo puede recopilar información.

ActiveX Una tecnología de Microsoft que utiliza programación orientada a objetos (OOP) y se basa en COM y DCOM.

Modo ad hoc Una implementación inalámbrica en la que no hay AP y las estaciones se comunican directamente entre sí.

Protocolo de resolución de direcciones (ARP) Un protocolo que resuelve la dirección IP colocada en el paquete en una dirección física o de capa 2 (denominada dirección MAC en Ethernet).

control administrativo Un control de seguridad que se implementa para administrar los activos y el personal de la organización e incluye directivas, procedimientos, estándares y directrices de seguridad establecidos por la administración.

derecho administrativo Un tipo de ley donde las agencias gubernamentales establecen estándares de desempeño o conducta para que las organizaciones e industrias los sigan. Las áreas comunes que están cubiertas incluyen servicios públicos, comunicaciones, banca, protección del medio ambiente y atención médica.

ADSL *Ver* DSL asimétrico (ADSL).

amenaza persistente avanzada (APT) Un ataque en el que una persona no autorizada obtiene acceso a una red y permanece durante un largo período de tiempo con la intención de robar datos.

adware Software que rastrea el uso de Internet en un intento de adaptar los anuncios y correos electrónicos no deseados a los intereses de un usuario.

agregación El proceso de ensamblar o compilar unidades de información a un nivel de sensibilidad y tener la totalidad resultante de datos siendo de un nivel de sensibilidad más alto que los componentes individuales.

Ágil Un modelo de desarrollo que enfatiza la retroalimentación continua y el trabajo en equipo multifuncional.

AH, *consulte* Encabezado de autenticación (AH).

ALE *Ver* expectativa de pérdida anualizada.

algoritmo Una función matemática que cifra y descifra los datos. También se conoce como cifrado.

expectativa de pérdida anualizada El factor de riesgo esperado de un evento de amenaza anual. La ecuación utilizada es ALE = SLE × ARO.

tasa anualizada de ocurrencia Una estimación de la frecuencia con la que una amenaza determinada puede ocurrir anualmente. Este acrónimo significa tasa anualizada de ocurrencia.

aprobación/rechazo de aplicaciones Aprobar o rechazar una aplicación en función de los resultados de las pruebas; parte del proceso de investigación de la aplicación.

pruebas de aplicaciones Probar una aplicación para asegurarse de que cumple con los requisitos de seguridad de la organización; parte del proceso de investigación de la aplicación.

investigación de aplicaciones Una secuencia de actividades que tiene como objetivo determinar si una aplicación cumple con los requisitos de seguridad de la organización. Incluye dos actividades principales: pruebas de aplicaciones y aprobación/rechazo de aplicaciones.

Capa de aplicación (capa 7) La capa del modelo de referencia OSI donde comienza el proceso de encapsulación. Esta capa recibe los datos sin procesar de la aplicación en uso y proporciona servicios como la transferencia de archivos y el intercambio de mensajes a la aplicación (y, por lo tanto, al usuario).

proxy de nivel de aplicación Un tipo de firewall que realiza una inspección profunda de paquetes. Comprende los detalles del proceso de comunicación en la capa 7 para la aplicación de interés.

arquitectura La organización de un sistema, incluyendo sus componentes y sus interrelaciones, junto con los principios que guiaron el diseño y la evolución del sistema.

ARO *Ver* tasa anualizada de ocurrencia.

ARP *Consulte* Protocolo de resolución de direcciones (ARP).

idiomas ensamblados Lenguajes que utilizan símbolos o mnemotécnicos para representar secciones de código binario complicado. Por consiguiente, estos lenguajes utilizan un ensamblador para convertir el código a nivel de máquina.

activo Cualquier recurso, producto, proceso, sistema o entidad digital o física que tenga valor para una organización y deba protegerse.

valoración de activos El proceso de asignar un valor monetario a un activo en función de su valor para la organización.

memoria asociativa Memoria en la que se busca un valor de datos específico en lugar de utilizar una dirección de memoria específica.

DSL asimétrico (ADSL) Un tipo de DSL que normalmente proporciona cargas de 128 Kbps a 384 Kbps y descargas de hasta 768 Kbps.

cifrado asimétrico Un método de cifrado mediante el cual un par de claves, una clave privada y una clave pública, realiza el cifrado y descifrado. Una clave realiza el cifrado, mientras que la otra clave realiza el descifrado. También se conoce como cifrado de clave pública.

modo asimétrico Un modo en el que un procesador está dedicado a un proceso o aplicación específica y cuando se realiza el trabajo para ese proceso, siempre lo realiza el mismo procesador.

cifrado asíncrono Forma de cifrado en la que las solicitudes de cifrado o descifrado se procesan desde una cola.

Modo de transferencia asíncrono (ATM) Una tecnología de conmutación de celdas que transfiere celdas de tamaño fijo (53 bytes) en lugar de paquetes y, una vez establecida una ruta de acceso, utiliza la misma ruta para toda la comunicación.

transmisión asíncrona Tipo de transmisión en la que los bits de inicio y detención se comunican cuando cada byte se inicia y se detiene.

ATM *Vea el* Asynchronous Transfer Mode (ATM).

atomicidad Propiedad en la que se completan todas las operaciones o se revierten los cambios de la base de datos.

ataque Cualquier evento que viole las políticas de seguridad o privacidad de una organización.

vector de ataque Segmento de la ruta de comunicación que un ataque utiliza para tener acceso a una vulnerabilidad.

atenuación El debilitamiento de una señal a medida que viaja por el cable y encuentra resistencia.

control de acceso basado en atributos (ABAC) Modelo de control de acceso que concede o deniega solicitudes de usuario basándose en atributos arbitrarios del usuario y atributos arbitrarios del objeto, así como en condiciones de entorno que se pueden reconocer globalmente.

auditoría El proceso de proporcionar una evaluación técnica medible manual o sistemática de un sistema o aplicación.

servidor de autenticación El servidor de RADIUS, que trabaja con el cliente de RADIUS.

autenticación El acto de validar un usuario con un identificador único proporcionando las credenciales adecuadas.

Encabezado de autenticación (AH) Parte de IPsec que proporciona integridad de datos, autenticación de origen de datos y protección contra ataques de reproducción.

autenticador El componente en un entorno RADIUS al que un solicitante está intentando conectarse (AP, conmutador, servidor de acceso remoto).

autorización El punto después de la identificación y autenticación en el que se conceden a un usuario los derechos y permisos para los recursos.

Direccionamiento IP privado automático (APIPA) Asigna una dirección IP a un dispositivo si el dispositivo no puede comunicarse con el servidor DHCP y se implementa principalmente en

Windows. El intervalo de direcciones IP asignadas es de 169.254.0.1 a 169.254.255.254 con una máscara de subred de 255.255.0.0.

alarma de estación auxiliar Un mecanismo que hace que una alarma que se origina automáticamente en un centro de datos se transmita a través de los circuitos de alarma de incendios o policía municipales locales para su transmisión tanto a la policía / estación de bomberos local como a la sede correspondiente.

disponibilidad Un valor que describe qué porcentaje del tiempo que el recurso o los datos están disponibles. El principio de la tríada de la CIA que garantiza que los datos sean accesibles cuando y donde se necesiten.

efecto avalancha La condición en la que cualquier cambio en la clave o el texto sin formato, no importa cuán menor sea, cambiará significativamente el texto cifrado.

puerta trasera Mecanismo implementado en muchos dispositivos o aplicaciones que da al usuario que utiliza la puerta trasera acceso ilimitado al dispositivo o aplicación. Es una pieza de software instalada por un hacker que le permite volver más tarde y conectarse a la computadora sin pasar por el proceso de autenticación normal. También conocido como trampilla.

BACnet2 Un protocolo de sistema de control industrial maestro/esclavo que utiliza el puerto 47808.

relación base En SQL, una relación que realmente existe en la base de datos.

banda base A las transmisiones en las que se utiliza todo el medio para una sola transmisión y luego se asignan múltiples tipos de transmisión ranuras de tiempo para utilizar este único circuito.

Basilea II Recomendaciones de una asociación bancaria que afectan a las instituciones financieras. Abordan los requisitos mínimos de capital, la revisión supervisora y la disciplina de mercado con el propósito de proteger contra los riesgos que enfrentan los bancos y otras instituciones financieras.

línea de base Componente de gobierno de seguridad de la información que actúa como punto de referencia que se define y captura para ser utilizado como referencia futura. Se utilizan líneas de base de seguridad y rendimiento.

Isdn de la tarifa básica (BRI) Una solución de comunicaciones que proporciona tres canales: dos canales B que proporcionan 64 Kbps cada uno y un canal D que es de 16 Kbps para un total de 144 Kbps.

host bastión Un dispositivo expuesto directamente a Internet o a cualquier red que no sea de confianza.

BCP *Ver* plan de continuidad del negocio.

Modelo Bell-LaPadula El primer modelo matemático de un sistema multinivel que utilizaba tanto los conceptos de una máquina de estado como los de control del flujo de información.

regla de la mejor evidencia Una regla que establece que cuando se presentan pruebas, como un documento o una grabación, solo se aceptará el original a menos que exista una razón legítima para no usar el original.

BGP *Consulte* Border Gateway Protocol (BGP).

Modelo biba Un modelo de seguridad que se ocupa de la integridad de la información en lugar de la confidencialidad de esa información.

aceptabilidad biométrica La probabilidad de que los usuarios acepten y sigan el sistema.

precisión biométrica Qué tan correctas serán las lecturas biométricas generales.

rendimiento biométrico La velocidad a la que el sistema biométrico podrá escanear las características y completar el análisis para permitir o denegar el acceso.

ataque de cumpleaños Un ataque en el que los valores que tiene un atacante se comparan con un conjunto de hashes de contraseña para los que el atacante conoce las contraseñas.

pruebas de caja negra El equipo de pruebas no tiene conocimiento sobre la red o la aplicación de la organización. El equipo puede utilizar cualquier medio a su disposición para obtener información sobre la red o aplicación de la organización. Esto también se conoce como pruebas de conocimiento cero y pruebas cerradas. Este término se utiliza para referirse a las pruebas de seguridad de red, así como a las pruebas de aplicación.

listas negras Configurar direcciones de correo electrónico, direcciones de Internet, sitios web, aplicaciones o algunos otros identificadores inaceptables como remitentes incorrectos o denegados.

apagón Un corte de energía prolongado.

prueba ciega Una prueba en la que se proporciona al equipo de pruebas un conocimiento limitado de los sistemas y dispositivos de red utilizando información disponible públicamente. El equipo de seguridad de la organización sabe que se avecina un ataque. Esta prueba requiere más esfuerzo por parte del equipo de pruebas y el equipo de pruebas debe simular un ataque real.

cifrado de bloques Cifrado que realiza el cifrado dividiendo el mensaje en unidades de longitud fija.

Pez soplador Un cifrado de bloques que utiliza bloques de datos de 64 bits que utilizan claves de cifrado de 32 a 448 bits. Blowfish realiza 16 rondas de transformación.

Bluejacking Enviar un mensaje no solicitado a un dispositivo habilitado para Bluetooth.

Bluesnarfing Obtener acceso no autorizado a un dispositivo mediante la conexión Bluetooth.

Bluetooth Una tecnología inalámbrica que se utiliza para crear redes de área personal (PANs).

bolardos Postes verticales cortos colocados en las entradas a los edificios y las aceras que bordean las aceras que ayudan a proporcionar protección contra los vehículos que podrían chocar intencionalmente o no, o entrar en el edificio o lesionar a los peatones.

virus del sector de inicio Virus que infecta el sector de arranque de un equipo y sobrescribe archivos o instala código en el sector para que el virus se inicie en el inicio.

Protocolo de puerta de enlace fronteriza (BGP) Un protocolo de ruteo exterior considerado como un protocolo de vector de trayecto.

botnet Colección de equipos que actúan juntos en un ataque; las computadoras individuales se llaman zombis.

incumplimiento Un ataque que ha logrado alcanzar su objetivo.

Modelo Brewer-Nash (Muralla China) Un modelo de seguridad que introdujo el concepto de permitir que los controles de acceso cambien dinámicamente en función de las acciones anteriores de un usuario. También llamado el modelo de la Muralla China.

BRI *Ver* Tipo Básico ISDN (BRI).

banda ancha Una transmisión de datos de ancho de banda amplio que tiene la capacidad de transportar simultáneamente múltiples señales y tipos de tráfico.

difusión Una transmisión enviada por un único sistema a todos los sistemas de la red. Se considera uno a todos.

brownout Una caída prolongada de potencia que está por debajo del voltaje normal.

ataque de fuerza bruta Un ataque de contraseña que implica probar todas las combinaciones posibles de números y caracteres. También se conoce como un ataque exhaustivo.

BSI *Consulte* Seguridad de compilación en (BSI).

desbordamiento de búfer Un problema que se produce cuando se aceptan demasiados datos como entrada para un proceso específico. Los hackers pueden aprovecharse de este fenómeno enviando demasiados datos, lo que puede causar un error, o en algunos casos ejecutando comandos en la máquina si pueden localizar un área donde se pueden ejecutar los comandos.

Construir y corregir Un método de desarrollo que ha sido desacreditado en gran medida y ahora se utiliza como una plantilla para cómo *no* gestionar un proyecto de desarrollo. En pocas palabras, utilizando este método, el software se desarrolla lo más rápido posible y se libera.

Generar seguridad en (BSI) Una iniciativa que promueve un enfoque independiente de los procesos para hacer recomendaciones de seguridad con respecto a arquitecturas, métodos de prueba, revisiones de código y procesos de administración.

topología de bus La topología Ethernet más antigua utilizada. En esta topología, todos los dispositivos están conectados a una sola línea que tenga dos puntos finales definitivos.

caso de negocio Un documento formal que da las razones detrás de un proyecto o iniciativa organizacional.

plan de continuidad del negocio (BCP) Un plan que se centra en mantener la misión de una organización o los procesos de negocio durante y después de una interrupción.

CA *Consulte* entidad de certificación (CA).

bloqueo de cable Un cable de acero recubierto de vinilo que se conecta a una computadora portátil y luego se bloquea alrededor de un objeto.

módems de cable Una solución de acceso a Internet que puede proporcionar hasta más de 50 Mbps a través del cableado coaxial utilizado para la televisión por cable.

caché Una cantidad relativamente pequeña (en comparación con la memoria primaria) de RAM de muy alta velocidad, que contiene las instrucciones y los datos de la memoria primaria, que tiene una alta probabilidad de que se acceda durante la parte actualmente en ejecución de un programa.

CALEA *Ver* Communications Assistance for Law Enforcement Act (CALEA) de 1994.

red de área de campus (CAN) Incluye varias LAN, pero es más pequeño que un MAN. Un CAN podría implementarse en un hospital o campus de negocios local.

clave candidata Atributo de una relación que tiene valores que coinciden con la clave principal de otra relación.

Integración del modelo de madurez de capacidad (CMMI) Un conjunto completo de directrices que aborda todas las fases del ciclo de vida del desarrollo de software. Describe una serie de etapas o niveles de madurez que un proceso de desarrollo puede avanzar a medida que pasa del modelo ad hoc (construir y corregir) a un modelo que incorpora un plan presupuestado para la mejora continua.

tabla de capacidades Tabla que enumera los derechos de acceso que tiene un sujeto determinado a los objetos.

detector de capacitancia Un dispositivo que emite un campo magnético y monitorea ese campo. Si el campo se interrumpe, lo que ocurre cuando una persona entra en el área, suena una alarma.

cardinalidad Número de filas de una relación.

Acceso múltiple/prevención de colisiones con detección de portadora (CSMA/CA) Un método de contención utilizado en redes inalámbricas 802.11.

Detección de múltiples accesos/colisiones con detección de portadora (CSMA/CD) Un método de contención utilizado en redes 802.3.

REPARTO-128 Cifrado de bloques que utiliza una clave de 40 a 128 bits que realizará 12 o 16 rondas de transformación en bloques de 64 bits.

REPARTO-256 Cifrado de bloques que utiliza una clave de 128, 160, 192, 224 o 256 bits que realizará 48 rondas de transformación en bloques de 128 bits.

CBC *Consulte* Cipher Block Chaining (CBC).

CBC-MAC *Consulte* Cifrado de encadenamiento de bloques MAC (CBC-MAC).

CCTV *Ver* circuito cerrado de televisión (CCTV) sistema.

CDMA *Consulte* Acceso múltiple por división de código (CDMA).

CDN *Consulte* red de distribución de contenido (CDN).

control de acceso centralizado Un tipo de control de acceso en el que un departamento central o personal supervisa el acceso a todos los recursos de la organización.

lista de revocación de certificados (CRL) Una lista de certificados digitales que una CA ha revocado.

certificación La evaluación técnica de un sistema. El proceso de evaluación del software para su eficacia de seguridad con respecto a las necesidades del cliente.

entidad de certificación (CA) La entidad que crea y firma certificados digitales, mantiene los certificados y los revoca cuando es necesario.

CFAA *Ver* Ley de Fraude y Abuso Informático de 1986.

CFB *Consulte* Comentarios de cifrado (CFB).

cadena de custodia Una lista que muestra quién controló la evidencia, quién aseguró la evidencia y quién la obtuvo.

Protocolo de autenticación por desafío mutuo (CHAP) Un protocolo para validar una contraseña sin enviar la contraseña a través de una red que no es de confianza, donde el servidor envía al cliente un conjunto de texto aleatorio denominado desafío. El cliente cifra el texto con la contraseña y lo devuelve. A continuación, el servidor lo descifra con la misma contraseña y compara el resultado con lo que se envió originalmente. Si los resultados coinciden, el servidor puede estar seguro de que el usuario o sistema posee la contraseña correcta sin necesidad de enviarla a través de la red que no es de confianza.

proceso de gestión de cambios El proceso de TI que garantiza que todos los cambios sean aprobados y documentados.

unidad de servicio de canal/unidad de servicio de datos (CSU/DSU) Dispositivo utilizado para conectar una LAN a una WAN.

CHAP *Consulte* Protocolo de autenticación por desafío mutuo (CHAP).

factores característicos Factores que son algo que una persona es, como una huella digital o geometría facial.

Modelo de la pared china *Vea* el modelo de Brewer-Nash (pared china).

ataque de texto cifrado elegido Ataque que se produce cuando un atacante elige el texto cifrado que se va a descifrar para obtener el texto no cifrado.

ataque de texto sin formato elegido Un ataque que se produce cuando un atacante elige el texto no cifrado para obtener el texto cifrado.

Tríada de la CIA Los tres fundamentos de la seguridad: confidencialidad, integridad y disponibilidad.

Plan CIP *Ver* plan de protección de infraestructuras críticas.

cifrado *Ver* algoritmo.

Encadenamiento de bloques cifrado (CBC) Un modo DES en el que cada bloque de 64 bits se encadena porque cada bloque de texto cifrado de 64 bits resultante se aplica al bloque siguiente. Por lo tanto, el bloque de mensajes de texto plano uno es procesado por el algoritmo utilizando un vector de inicialización (IV). El bloque de mensajes de texto cifrado resultante uno es XORed con el bloque de mensajes de texto no cifrado dos, lo que resulta en el mensaje de texto cifrado dos. Este proceso continúa hasta que se completa el mensaje.

Cifrado de encadenamiento de bloques MAC (CBC-MAC) Un MAC de cifrado de bloques que funciona en modo CBC.

Comentarios cifrados (CFB) Un modo DES que funciona con bloques de 8 bits (o más pequeños) y utiliza una combinación de cifrado de secuencias y cifrado de bloques. Al igual que CBC, el primer bloque de 8 bits del mensaje de texto sin formato es XORed por el algoritmo que utiliza un flujo de claves, que es el resultado de un IV y la clave. El mensaje de texto cifrado resultante se aplica al siguiente bloque de mensajes de texto no cifrado.

bloqueos de cifrado Un bloqueo que se abre escribiendo el código correcto en un teclado.

texto cifrado Forma modificada de un mensaje que es ilegible sin conocer la clave y el sistema de cifrado utilizado. También se conoce como criptograma.

ataque de sólo texto cifrado Ataque que se produce cuando un atacante utiliza varios mensajes cifrados (texto cifrado) para averiguar la clave utilizada en el proceso de cifrado.

proxy a nivel de circuito Un firewall que funciona en la capa Session (capa 5) del modelo OSI.

red de conmutación de circuitos Una red en la que hay una ruta de acceso establecida al destino que es la única ruta de acceso para toda la comunicación.

evidencia circunstancial Evidencia que proporciona inferencia de información de otros hechos relevantes intermedios.

ley del código civil Un tipo de ley basada en leyes escritas. Es una ley basada en reglas y no se basa en la precedencia de ninguna manera.

desobediencia civil La negativa intencional a obedecer ciertas leyes, demandas y órdenes de un gobierno y comúnmente, aunque no siempre, se define como resistencia no violenta.

investigación civil Una investigación que ocurre cuando una organización o parte sospecha que otra organización está incurriendo en actos civiles.

ley civil/agravio Un tipo de ley donde la parte responsable debe un deber legal a la víctima. Se ocupa de los agravios que se han cometido contra un individuo u organización.

Modelo de integridad de Clark-Wilson Desarrollado después del modelo Biba, un modelo de seguridad que también se preocupa por la integridad de los datos.

Puerta de clase 1 Una puerta apta para uso residencial.

Puerta de clase 2 Una puerta adecuada para uso comercial.

Puerta de clase 3 Una puerta adecuada para uso industrial.

Puerta de clase 4 Una puerta que se utiliza para un área restringida.

Extintor clase A Un extintor de incendios utilizado para combustibles ordinarios.

Extintor clase B Un extintor de incendios utilizado para líquidos inflamables y gases inflamables.

Extintor clase C Un extintor de incendios utilizado para equipos eléctricos.

Extintor clase D Un extintor de incendios utilizado para metales combustibles.

Extintor clase K Un extintor de incendios utilizado para el aceite de cocina o la grasa.

Sala blanca Un modelo de desarrollo que se adhiere estrictamente a los pasos formales y un método más estructurado. Intenta prevenir errores y equivocaciones a través de pruebas exhaustivas.

texto no cifrado *Consulte* texto sin formato.

niveles de recorte Establezca una línea base para los errores normales del usuario y las infracciones que superen ese umbral se registrarán para analizar por qué se produjeron las infracciones.

sistema de circuito cerrado de televisión (CCTV) Un sistema que utiliza conjuntos de cámaras que se pueden supervisar en tiempo real o registrar días de actividad que se pueden ver según sea necesario en un momento posterior.

sistema cerrado Un sistema propietario que está diseñado para trabajar con una gama limitada de otros sistemas.

computación en la nube La centralización de datos en un entorno web al que se puede acceder desde cualquier lugar y en cualquier momento. Enfoque que hace que los recursos estén

disponibles en un centro de datos basado en web para que se pueda acceder a los recursos desde cualquier lugar.

servicios de identidad en la nube Servicios de identidad proporcionados por una solución en la nube.

CMMI *Consulte* Integración del modelo de madurez de capacidad (CMMI).

coaxial Uno de los primeros tipos de cable que se utilizaron para redes, el mismo tipo básico de cable que llevó la televisión por cable a millones de hogares.

Acceso múltiple por división de código (CDMA) Una técnica de modulación utilizada en la tecnología inalámbrica móvil.

repositorio de código Un lugar donde se almacena el código, normalmente en un servidor o en la nube.

revisión y pruebas de código Se utiliza para identificar patrones de programación incorrectos, configuraciones incorrectas de seguridad, errores funcionales y errores lógicos.

cohesión Término utilizado para describir cuántas tareas diferentes puede llevar a cabo un módulo. Si un módulo está limitado a un número pequeño o una sola función, se dice que tiene alta cohesión.

sitio frío Una instalación arrendada que contiene solo cableado eléctrico y de comunicaciones, aire acondicionado, plomería y pisos elevados.

colisión Evento que se produce cuando una función hash genera el mismo valor hash en mensajes diferentes. Se produce cuando dos empleados trabajan juntos para lograr un robo de algún tipo que no se podría lograr sin sus conocimientos o responsabilidades combinados.

columna o atributo Una columna de una tabla.

COM *Vea* Modelo de objetos componentes (COM).

bloqueo de combinación Un bloqueo que se abre girando el bloqueo en un patrón hasta que los vasos se alinean.

Criterios comunes Un sistema que utiliza niveles de garantía de evaluación (EALs) para calificar los sistemas, con cada EAL que representa un nivel sucesivamente más alto de pruebas de seguridad y diseño en un sistema.

common law Un tipo de ley basada en costumbres y precedentes porque no se disponía de leyes escritas. El common law reflexiona sobre la moral del pueblo y se basa en gran medida en la precedencia.

Arquitectura de agente de solicitud de objetos comunes (CORBA) Un estándar abierto orientado a objetos desarrollado por el Object Management Group (OMG).

Ley de asistencia en materia de comunicaciones para la aplicación de la ley (CALEA) de 1994 Una ley estadounidense que afecta a las agencias de inteligencia y aplicación de la ley. Requiere que los operadores de telecomunicaciones y los fabricantes de equipos de telecomunicaciones modifiquen y diseñen sus equipos, instalaciones y servicios para asegurarse de que tienen capacidades de vigilancia incorporadas.

nube de la comunidad Una solución de implementación en la nube propiedad y administrada por un grupo de organizaciones que crean la nube para un propósito común, quizás para abordar una preocupación común, como el cumplimiento de la regularidad.

control compensativo Un control de seguridad que sustituye a un control de acceso primario y actúa principalmente como mitigación de riesgos.

Modelo de objetos componentes (COM) Un modelo para la comunicación entre procesos en el mismo equipo.

Ley de Fraude y Abuso Informático (CFAA) de 1986 Una ley estadounidense que afecta a cualquier entidad que pueda participar en la piratería de "computadoras protegidas" como se define en la ley.

delitos informáticos de prevalencia Un delito que se produce debido a que las computadoras son tan ampliamente utilizadas en el mundo de hoy. Este tipo de delito se produce sólo porque existen equipos.

Ley de Seguridad Informática de 1987 Una ley estadounidense que fue la primera ley escrita para exigir un plan formal de seguridad informática. Fue escrito para proteger y defender cualquiera de la información sensible en los sistemas del gobierno federal y proporcionar seguridad para esa información.

delitos asistidos por computadora Un delito que se produce cuando un equipo se utiliza como una herramienta para ayudar a cometer un delito.

delitos dirigidos por computadoras Un delito que se produce cuando un ordenador es víctima de un ataque cuyo único propósito es dañar el ordenador y a su propietario.

cifrado de ocultación Un cifrado que intercalaba texto plano en algún lugar dentro de otro material escrito. También se conoce como cifrado nulo.

círculo concéntrico Una forma de seguridad física dentro de un edificio que se basa en la creación de capas de barreras físicas a la información.

pruebas concluyentes Evidencia que no requiere otra corroboración.

confidencialidad El principio de la tríada de la CIA que garantiza que los datos estén protegidos de la divulgación no autorizada. Una característica proporcionada si los datos no se pueden leer.

confinamiento Cuando un proceso solo puede leer y escribir en determinadas ubicaciones y recursos de memoria.

confusión El proceso de cambiar un valor de clave durante cada ronda de cifrado. La confusión se lleva a cabo a menudo por sustitución.

coherencia El grado en que una transacción sigue un proceso de integridad que garantiza que los datos sean consistentes en todos los lugares donde existen.

contaminación La mezcla o mezcla de datos de un nivel de sensibilidad o necesidad de saber con el de otro.

análisis de contenido Análisis del contenido de una unidad o software. El análisis de contenido de la unidad proporciona un informe que detalla los tipos de datos por porcentaje. El análisis de contenido del software determina el propósito del software.

red de distribución de contenido (CDN) Una red distribuida de servidores que normalmente se encuentra en varios centros de datos conectados a través de Internet.

control de acceso dependiente del contexto Tipo de acceso que se basa en atributos de sujeto u objeto o en características del medio ambiente. Basa el acceso a los datos en varios factores para ayudar a evitar la inferencia.

plan de continuidad de operaciones (COOP) Un plan que se centra en restaurar las funciones esenciales de misión (MEF) de una organización en un sitio alternativo y realizar esas funciones durante un hasta 30 días antes de volver a las operaciones normales.

COOP *Ver* plan de continuidad de operaciones.

copia de seguridad Una copia de seguridad que realiza una copia de seguridad de todos los archivos, al igual que en una copia de seguridad completa, pero no restablece el bit de almacenamiento del archivo.

derechos de autor Un tipo de propiedad intelectual que garantiza que una obra de autor está protegida para cualquier forma de reproducción o uso sin el consentimiento del titular de los derechos de autor, generalmente el autor o artista que creó la obra original.

CORBA *Consulte* Common Object Request Broker Architecture (CORBA).

control correctivo Control de seguridad que reduce el efecto de un ataque u otro evento no deseado.

evidencia corroborativa Evidencia que apoya otra pieza de evidencia.

Modo de contador (CTR) Un modo DES similar al modo OFB que utiliza un contador IV de incremento para asegurarse de que cada bloque se cifra con una secuencia de claves única. Además, el texto cifrado no se está encadenando en el proceso de cifrado. Dado que este encadenamiento no se produce, el rendimiento de CTR es mucho mejor que los otros modos.

countermeasure A control that is implemented to reduce potential risk.

acoplamiento Hace referencia a la cantidad de interacción que un módulo requiere de otro módulo para hacer su trabajo. El acoplamiento bajo o suelto indica que un módulo no necesita mucha ayuda de otros módulos, mientras que el acoplamiento alto indica lo contrario.

CPTED *Ver* Prevención del Delito a través del Diseño Ambiental (CPTED).

Prevención del delito a través del diseño ambiental (CPTED) Diseño de instalaciones desde cero para apoyar la seguridad.

escena del crimen El entorno en el que existe evidencia potencial.

investigación criminal Una investigación que se lleva a cabo porque se ha violado una ley federal, estatal o local.

derecho penal Un tipo de ley que cubre cualquier acción que se considere perjudicial para otros. Se trata de conductas que violan las leyes de protección pública.

plan de comunicaciones de crisis Un plan que documenta los procedimientos estándar para las comunicaciones internas y externas en caso de una interrupción utilizando un plan de comunicaciones de crisis. También proporciona varios formatos para las comunicaciones adecuadas al incidente.

plan de protección de infraestructuras críticas (CIP) Un conjunto de políticas y procedimientos que sirven para proteger y recuperar estos activos y mitigar riesgos y vulnerabilidades.

criticidad *Consulte* Criticidad de los datos.

CRL Consulte lista de revocación de certificados (CRL).

modelo de identidad federada de certificación cruzada Un modelo de identidad federada en el que cada organización certifica que todas las demás organizaciones son de confianza.

tasa de error cruzado El punto en un sistema biométrico en el que FRR es igual a FAR.

diafonía Un problema que ocurre cuando las señales de los dos cables (o más) interfieren entre sí y distorsionan la transmisión.

criptoanálisis La ciencia de descifrar el texto cifrado sin conocimiento previo de la clave o criptosistema utilizado. El propósito del criptoanálisis es forjar señales o mensajes codificados que serán aceptados como auténticos.

criptograma *Ver* texto cifrado.

criptografía Una ciencia que oculta los datos o los hace ilegibles transformándolos.

criptología La ciencia que estudia la comunicación y los datos cifrados.

criptosistema Todo el proceso criptográfico, incluido el algoritmo, la clave y las funciones de administración de claves. La seguridad de un criptosistema se mide por el tamaño del espacio de claves y la potencia computacional disponible.

cryptovariable *Consulte* la clave.

CSMA/CA *Vea el* acceso múltiple del detección portador/la evitación de la colisión (CSMA/CA).

CSMA/CD *Vea el* acceso múltiple del detección portadora/la detección de la colisión (CSMA/CD).

CSU/DSU *Véase* unidad de servicio de canal/unidad de servicio de datos (CSU/DSU).

CTR *Consulte* Modo de contador (CTR).

derecho consuetudinario Un tipo de ley basada en las costumbres de un país o región.

delitos cibernéticos Cualquier actividad delictiva que se lleve a cabo por medio de ordenadores o internet.

plan de respuesta a incidentes cibernéticos Un plan que establece procedimientos para abordar los ataques cibernéticos contra los sistemas de información de una organización.

ciberocupación Registrar nombres de dominio sin intención de usarlos, pero con la intención de mantenerlos como rehenes.

DAC *Consulte* control de acceso discrecional (DAC).

copia de seguridad diaria Copia de seguridad en la que se utiliza la marca de tiempo de un archivo para determinar si es necesario archivarlo.

violación de datos Cualquier incidente en el que la información que se considera privada o confidencial se divulga a partes no autorizadas.

borrado de datos Un ataque que hace que la información sea irrecuperable mediante un teclado. Este tipo de ataque extrae información de los medios de almacenamiento de datos mediante la ejecución de utilidades de software, pulsaciones de teclas u otros recursos del sistema desde un teclado.

criticidad de los datos Una medida de la importancia de los datos.

custodio de datos La persona que asigna permisos a los datos en función de las directrices del propietario de los datos.

ocultar datos El principio por el cual los datos sobre una entidad conocida no son accesibles para ciertos procesos o usuarios.

Capa de vínculo de datos (capa 2) La capa del modelo de referencia OSI responsable de determinar qué direcciones MAC deben estar en cada salto y agregarlas a parte del paquete.

software de prevención de pérdida de datos (DLP) Software que intenta evitar la fuga de datos.

minería de datos Un proceso de uso de herramientas especiales para organizar los datos en un formato aún más utilizable. Analiza grandes conjuntos de datos en un almacén de datos para encontrar patrones no obvios.

Especificaciones de la interfaz de servicio de datos sobre cable (DOCSIS) Un estándar para las comunicaciones de módem de cable.

titular de los datos El individuo que realmente posee ciertos datos y decide sobre el nivel de acceso otorgado a individuos o grupos.

procesadores de datos Cualquier personal dentro de una organización que procese los datos que se han recopilado a lo largo de todo el ciclo de vida de los datos.

purga de datos Un proceso hace que la información sea irrecuperable contra ataques de laboratorio (forenses). Se puede hacer utilizando un método como la desgasificación para hacer que los datos antiguos no estén disponibles incluso con forenses.

calidad de los datos La idoneidad de los datos para su uso.

sensibilidad de datos Una medida de la libertad con la que se pueden manejar los datos.

estructura de datos La relación lógica entre los elementos de datos. Describe la medida en que los elementos, los métodos de acceso y las alternativas de procesamiento están asociados y la organización de los elementos de datos.

almacén de datos Un repositorio de información de bases de datos heterogéneas.

almacenamiento de datos Proceso de combinación de datos de varias bases de datos u orígenes de datos en una ubicación central denominada almacén. El almacén se utiliza para realizar análisis. Los datos no se combinan simplemente, sino que se procesan y presentan de una manera más útil y comprensible.

bloqueos de base de datos Se utiliza cuando un usuario tiene acceso a un registro que impide que otro usuario tenga acceso al registro al mismo tiempo para evitar las ediciones hasta que finalice el primer usuario.

vistas de base de datos El conjunto de datos dado que un usuario o grupo de usuarios puede ver cuando tienen acceso a la base de datos.

DCOM *vea* Modelo de objetos componentes distribuido (DCOM).

Ataque DDoS *Consulte* ataque de denegación de servicio distribuido (DDoS).

control de acceso descentralizado Un tipo de control de acceso en el que el personal más cercano a los recursos, como los jefes de departamento y los propietarios de datos, supervisan el control de acceso para los recursos individuales.

decodificación El proceso de volver a cambiar un mensaje codificado a su formato original.

descifrado El proceso de convertir datos de texto cifrado a texto no cifrado. También se conoce como desciframiento.

postura de seguridad predeterminada La postura de seguridad predeterminada que usa una organización. Una postura permitir-por-abandono permite el acceso a cualquier dato a menos que exista una necesidad de restringir el acceso. Una postura de denegación por defecto es mucho más estricta porque deniega cualquier acceso que no se permita explícitamente.

defensa en profundidad Un enfoque de seguridad que hace referencia a la implementación de capas de protección.

grado Número de columnas de una tabla.

extintor de diluvios Un extintor de incendios que permite que se liberen grandes cantidades de agua en una habitación, lo que no es una buena opción para donde se encuentra el equipo de computación.

zona desmilitarizada (DMZ) Una red donde se colocan los sistemas a los que se accederá regularmente desde la red que no es de confianza.

demultiplexor Un dispositivo que toma una sola señal de entrada que lleva muchos canales y los separa en múltiples señales de salida.

desaprovisionamiento El acto de quitar o deshabilitar una cuenta de acceso.

DES *Vea* el estándar de encripción digital (DES).

DES-X Una variante de DES que utiliza varias claves de 64 bits además de la clave DES de 56 bits. La primera clave de 64 bits es XORed para el texto no cifrado, que luego se cifra con DES. La segunda clave de 64 bits es XORed para el cifrado resultante.

control detectivesco Un control de seguridad que detecta un ataque mientras se está produciendo para alertar al personal adecuado.

control disuasorio Un control de seguridad que disuade posibles ataques.

autenticación de dispositivos Una forma de autenticación que se basa en la identidad del dispositivo como parte del proceso de autenticación.

DHCP *Consulte* Protocolo de configuración dinámica de host (DHCP).

conexión de acceso telefónico Una conexión de comunicación que utiliza la RTC. Si se inicia a través de una línea telefónica analógica, requiere un módem que convierta los datos digitales a analógicos en el extremo emisor y un módem en el extremo receptor para convertirlos de nuevo a digital.

Ataque de diccionario Un tipo de ataque de contraseña en el que los atacantes utilizan un diccionario de palabras comunes para detectar contraseñas.

copia de seguridad diferencial Una copia de seguridad en la que se realiza una copia de seguridad de todos los archivos que se han cambiado desde la última copia de seguridad completa y no se borra el bit de archivo de cada archivo.

difusión El proceso de cambiar la ubicación del texto no cifrado dentro del texto cifrado. La difusión se lleva a cabo a menudo mediante transposición.

digital Señalización utilizada en la mayoría de las transmisiones de computadora, que tiene sólo dos valores posibles: encendido y apagado.

certificado digital Documento electrónico que identifica al titular del certificado.

Estándar de cifrado digital (DES) Un algoritmo simétrico que utiliza una clave de 64 bits, 8 bits de los cuales se utilizan para la paridad. La longitud de clave efectiva para DES es de 56 bits. DES divide el mensaje en bloques de 64 bits. Dieciséis rondas de transposición y sustitución se realizan en cada bloque, lo que resulta en un bloque de 64 bits de texto cifrado.

gestión de derechos digitales Un enfoque utilizado por los fabricantes de hardware, editores, titulares de derechos de autor e individuos para controlar el uso del contenido digital. A menudo también implica controles de dispositivo.

firma digital Un método para proporcionar autenticación de remitente e integridad de mensaje. El mensaje actúa como entrada para una función hash y la clave privada del remitente cifra el valor hash. El receptor puede realizar un cálculo hash en el mensaje recibido para determinar la validez del mensaje.

Estándar de firma digital (DSS) Un estándar federal de seguridad digital que rige el algoritmo de seguridad digital (DSA).

Línea de suscriptor digital (DSL) Una opción de transmisión de banda ancha que proporciona una conexión de alta velocidad desde un hogar u oficina pequeña al ISP. Si bien utiliza las líneas telefónicas existentes, es una conexión siempre en línea.

evidencia directa Evidencia que prueba o refuta un hecho a través del testimonio oral, basado en información recopilada a través de los sentidos del testigo.

Espectro ensanchado de secuencia directa (DSSS) Una de las dos tecnologías de modulación (junto con el SFSS) que formaban parte de la norma 802.11 original.

control de directivas Control de seguridad que especifica una práctica aceptable dentro de una organización.

desastre Un evento que ocurre repentinamente y que tiene un impacto negativo a largo plazo en la vida.

plan de recuperación ante desastres (DRP) Un plan centrado en el sistema de información diseñado para restaurar la operatividad del sistema de destino, la aplicación o la infraestructura de la instalación informática en un sitio alternativo después de una emergencia.

control de acceso discrecional (DAC) Un modelo de control de acceso en el que el propietario del objeto especifica qué sujetos pueden tener acceso al recurso.

imágenes de disco El proceso de creación de una imagen exacta del contenido de un disco duro.

interrupción Cualquier evento no planificado que resulte en la interrupción temporal de cualquier activo de la organización, incluidos procesos, funciones y dispositivos.

protocolos de vectores de distancia Protocolos de ruteo que comparten toda su tabla de ruteo con sus routers vecinos según una programación, creando así la mayor parte del tráfico de las tres categorías. También utilizan una métrica llamada recuento de saltos, que es simplemente el número de enrutadores atravesados para llegar a una red.

Modelo de objetos componentes distribuido (DCOM) Un modelo de comunicación entre procesos en diferentes partes de una red.

ataque de denegación de servicio distribuido (DDoS) Un ataque DoS en el que el perpetrador solicita la ayuda de otras máquinas.

Protocolo de red distribuida versión 3 (DNP3) Un protocolo multicapa que se utiliza entre componentes en sistemas de automatización de procesos de empresas eléctricas y de agua. Fue desarrollado para las comunicaciones entre varios tipos de adquisición de datos y equipos de control. Funciona en modo maestro/esclavo usando el puerto 19999 cuando se usa TLS y el puerto 20000 cuando no se usa TLS.

sistemas distribuidos orientados a objetos Sistemas cuyos componentes deben ser capaces de localizarse entre sí y comunicarse en una red. Cuando una aplicación funciona en un marco cliente/servidor, como muchos, la solución está realizando computación distribuida.

Software DLP *Ver* software de prevención de pérdida de datos (DLP).

ZONA DESMILITARIZADA *Véase* zona desmilitarizada (DMZ).

DNP3 *Consulte* Protocolo de red distribuida versión 3 (DNP3).

DNS *Consulte* Sistema de nombres de dominio (DNS).

Ataque de envenenamiento de caché de DNS Un ataque en el que el atacante intenta actualizar o actualizar un registro cuando expira con una dirección diferente de la dirección correcta.

DNSSEC *Consulte* Extensiones de seguridad del Sistema de nombres de dominio (DNSSEC).

EL DOCSIS *ve las* especificaciones de la interfaz de servicio del Data-Over-Cable (DOCSIS).

dominio Conjunto de valores permitidos que puede tomar un atributo.

acaparamiento de dominios Registrar un nombre de dominio de una empresa conocida antes de que la propia empresa tenga la oportunidad de hacerlo.

Sistema de nombres de dominio (DNS) Un sistema que resuelve un nombre de equipo (o, en el caso de la web, un nombre de dominio) en una dirección IP.

Extensiones de seguridad del Sistema de nombres de dominio (DNSSEC) Uno de los enfoques más recientes para prevenir ataques DNS. Muchas implementaciones actuales de software DNS contienen esta funcionalidad, que utiliza firmas digitales para validar el origen de todos los mensajes para asegurarse de que no se suplantan.

prueba de doble anonimato Una prueba a ciegas en la que el equipo de seguridad de la organización no sabe que se avecina un ataque. Solo unas pocas personas de la organización conocen el ataque y no comparten esta información con el equipo de seguridad. Esta prueba normalmente requiere el mismo esfuerzo tanto para el equipo de pruebas como para el equipo de seguridad de la organización.

Doble DES Una versión de DES que utiliza una longitud de clave de 112 bits.

DRM *Consulte* gestión de derechos digitales.

DRP *Consulte plan* de recuperación ante desastres.

extintor de tubería seca Un sistema en el que el agua no se mantiene en las tuberías, sino en un tanque de retención. Las tuberías contienen aire presurizado, que se reduce cuando se detecta fuego, lo que permite que el agua entre en la tubería y los aspersores. Esto minimiza la posibilidad de una descarga accidental.

DSL *Vea* línea de suscriptor digital (DSL).

DSS *Véase* Estándar de firma digital (DSS).

DSSS *véase* Espectro ensanchado de secuencia directa (DSSS).

control dual Una medida de seguridad que requiere que dos empleados estén disponibles para completar una tarea específica. Esta medida de seguridad forma parte de la separación de funciones.

firewall de doble hogar Un firewall que tiene dos interfaces de red, una que apunta a la red interna y otra conectada a la red que no es de confianza.

atención debida Un término legal que se utiliza cuando una organización tomó todas las medidas razonables para evitar infracciones de seguridad y también tomó medidas para mitigar los daños causados por infracciones exitosas.

diligencia debida Término legal que se usa cuando una organización investiga todas las vulnerabilidades.

buceo en contenedores de basura Un ataque de ingeniería social que se produce cuando los atacantes examinan el contenido de la basura para obtener información confidencial.

durabilidad Una propiedad en la que, una vez comprobada, la transacción se confirma y no se puede revertir.

coacción Una situación que se produce cuando un empleado es obligado a cometer una acción por otra parte. Esta es una preocupación particular para la administración de alto nivel y los empleados con autorizaciones de alta seguridad porque tienen acceso a activos adicionales.

Protocolo de configuración dinámica de host (DHCP) Un servicio que se puede utilizar para automatizar el proceso de asignación de una configuración IP a los dispositivos de una red.

NAT dinámica Varias direcciones IP privadas internas tienen acceso a varias direcciones IP públicas externas. Se trata de una asignación de varios a varios.

servidor de seguridad de filtrado dinámico de paquetes Un firewall que realiza un seguimiento del puerto de origen y agrega dinámicamente una regla a la lista para permitir el tráfico de retorno a ese puerto.

pruebas dinámicas Analiza la seguridad del software en el entorno de tiempo de ejecución. Con esta prueba, el evaluador no debe tener acceso al código fuente de la aplicación.

EAP *Consulte* Protocolo de autenticación extensible (EAP).

E-transportistas En Europa, una tecnología similar a las líneas T-carrier.

BCE *Véase* el Libro electrónico de códigos (BCE).

Ley de espionaje económico de 1996 Una ley estadounidense que afecta a las empresas que tienen secretos comerciales y a cualquier persona que planee usar la tecnología de cifrado para actividades delictivas.

ECPA *Véase* la Ley de Privacidad de las Comunicaciones Electrónicas (ECPA) de 1986.

Exhibición de documentos electrónicos *Vea* detección electrónica (exhibición de documentos electrónicos).

EF *Ver* factor de exposición.

supervisión de salida Supervisión que se produce cuando una organización supervisa el flujo saliente de información de una red a otra.

EIGRP *Vea* el IGRP aumentado (EIGRP).

interferencia electromagnética (EMI) Interferencia de líneas eléctricas y otras fuentes de alimentación.

sistemas electromecánicos Sistemas de detección que funcionan detectando una rotura en un circuito eléctrico. Por ejemplo, el circuito puede cruzar una ventana o puerta, y cuando se abre la ventana o puerta, el circuito se rompe, activando una alarma de algún tipo.

Libro electrónico de códigos (BCE) Una versión de DES en la que el algoritmo procesa bloques de datos de 64 bits mediante la clave. El texto cifrado producido se puede rellenar para asegurarse de que el resultado es un bloque de 64 bits.

Ley de Privacidad de las Comunicaciones Electrónicas (ECPA) de 1986 Una ley estadounidense que afecta a las agencias de inteligencia y aplicación de la ley. Amplió las restricciones gubernamentales a las escuchas telefónicas de llamadas telefónicas para incluir las transmisiones de datos electrónicos por computadora y prohibió el acceso a las comunicaciones electrónicas almacenadas.

detección electrónica (exhibición de documentos electrónicos) Litigios o investigaciones gubernamentales que tratan con el intercambio de información en formato electrónico como parte del proceso de descubrimiento.

bóveda electrónica Copiar archivos en una ubicación de copia de seguridad a medida que se producen modificaciones en tiempo real.

suplantación de correo electrónico El proceso de enviar un correo electrónico que parece provenir de una fuente cuando realmente proviene de otra.

sistema embebido Una pieza de software integrada en una pieza más grande de software que está a cargo de realizar alguna función específica en nombre del sistema más grande.

iluminación de emergencia Sistemas de iluminación con su propia fuente de alimentación para usar cuando la energía está fuera.

EMI *Ver* interferencia electromagnética (EMI).

Carga de seguridad encapsuladora (ESP) Parte de IPsec que proporciona integridad de datos, autenticación de origen de datos, protección contra reproducción y cifrado.

encapsulación Un proceso en el que se agrega información al encabezado en cada capa y luego se coloca un remolque en el paquete antes de la transmisión.

codificación El proceso de cambiar los datos a otro formulario, mediante código.

cifrado El proceso de convertir datos de texto no cifrado a texto cifrado. También se conoce como cifrado.

seguridad de punto final Un campo de seguridad que intenta proteger sistemas individuales en una red manteniéndose en contacto constante con estos sistemas individuales desde una ubicación central.

IGRP mejorado (EIGRP) Un protocolo de ruteo propietario de Cisco sin clases que se considera un híbrido o un protocolo avanzado del vector de la distancia.

inscripción El proceso de solicitud de un certificado de la CA.

error ambiental Error que hace que un sistema sea vulnerable debido al entorno en el que está instalado.

EPHI Información de salud electrónica protegida. *Consulte* información de salud protegida.

ESP *Consulte* Encapsulating Security Payload (ESP).

Ethernet Un protocolo de capa 2 ampliamente utilizado descrito en el estándar 802.3.

evento Un cambio de estado que se produce.

exposición Una condición que se produce cuando un activo de la organización está expuesto a pérdidas.

factor de exposición El valor porcentual o la funcionalidad de un activo que se perderá cuando se produzca un evento de amenaza.

Protocolo de autenticación extensible (EAP) No un solo protocolo, sino un marco para el control de acceso basado en puertos que utiliza los mismos tres componentes que RADIUS.

Lenguaje de marcado extensible (XML) El lenguaje web más utilizado.

amenazas externas Amenazas de seguridad perimetral o acceso a un edificio o habitación.

extranet Una red que es lógicamente independiente de una intranet. Se trata de un ámbito en el que se ponen a disposición recursos a los que se accederá desde el mundo exterior.

estado a prueba de fallos Dejar los procesos y componentes del sistema en un estado seguro cuando se produce un error o se detecta en el sistema.

Estado de error suave La terminación del procesamiento no crítico seleccionado cuando se produce un error de hardware o software.

conmutación por error La capacidad de un sistema para cambiar a un sistema de copia de seguridad si se produce un error en el sistema primario.

failsoft La capacidad de un sistema para terminar procesos no críticos cuando se produce un error.

tasa de aceptación falsa (FAR) Una medida del porcentaje de usuarios no válidos que serán falsamente aceptados por el sistema. Esto se denomina error de tipo II.

tasa de rechazo falso (FRR) Una medición de usuarios válidos que serán rechazados falsamente por un sistema biométrico. Esto se denomina error de tipo I.

FAR *Ver* tasa de aceptación falsa (FAR).

error Un apagón momentánea.

tolerancia a fallos Un concepto que incluye redundancia pero que se refiere a cualquier proceso que permita a un sistema seguir poniendo a disposición activos de información en caso de fallo.

FCoE *Consulte* Fibre Channel a través de Ethernet (FCoE).

FDDI *Consulte* Interfaz de datos distribuidos por fibra (FDDI).

FDM *Consulte* Multiplexación por división de frecuencia (FDM).

AMDF *Consulte* Acceso múltiple por división de frecuencia (AMDF).

Ley Federal de Gestión de la Seguridad de la Información (FISMA) de 2002 Una ley estadounidense que afecta a todas las agencias federales. Requiere que las agencias federales desarrollen, documenten e implementen un programa de seguridad de la información en toda la agencia.

Ley Federal de Vigilancia de Inteligencia (FISA) de 1978 Una ley estadounidense que afecta a las agencias de inteligencia y aplicación de la ley. Establece procedimientos para la vigilancia física y electrónica y la recopilación de "información de inteligencia extranjera" entre "potencias extranjeras" y "agentes de potencias extranjeras" y sólo se aplica al tráfico dentro de los Estados Unidos.

Ley Federal de Privacidad de 1974 Una ley estadounidense que afecta a cualquier computadora que contenga registros utilizados por una agencia federal. Proporciona pautas para la recopilación, el mantenimiento, el uso y la difusión de información de identificación personal (PII) sobre individuos que las agencias federales mantienen en sistemas de registros sobre la recopilación, el mantenimiento, el uso y la distribución de pii que se mantiene en sistemas de registros por parte de agencias federales.

identidad federada Una identidad portátil que se puede usar en empresas y dominios.

gestión de identidades federadas (FIM) *Consulte* servicios de identidad federada.

servicios de identidad federada Servicios de identidad que participan en una estructura federada con otras organizaciones. Cada organización que se une a la federación acepta aplicar un conjunto común de directivas y estándares.

pies de iluminación Una medida de la iluminación.

obtención El proceso de una CPU que recibe instrucciones de la memoria.

FHSS *Ver* Espectro ensanchado de salto de frecuencia (FHSS).

Interfaz de datos distribuidos por fibra (FDDI) Un protocolo de capa 2 que utiliza una topología en anillo y una infraestructura de fibra.

fibra óptica Cableado que utiliza una fuente de luz que derriba un núcleo interior de vidrio o plástico.

Fibre Channel a través de Ethernet (FCoE) Protocolo que encapsula tramas Fibre Channel a través de redes Ethernet, lo que permite a Fibre Channel utilizar redes Ethernet de 10 Gigabits o superiores, al tiempo que preserva el protocolo Fibre Channel.

Matriz de puertas programable en campo (FPGA) Un tipo de dispositivo lógico programable (PLD) que se programa soplando conexiones de fusibles en el chip o utilizando un antifusible que realiza una conexión cuando se aplica un alto voltaje a la unión.

Protocolo de transferencia de archivos (FTP) Protocolo utilizado para transferir archivos de un sistema a otro.

cortafuegos Un dispositivo físico o de software que inspecciona y controla el tipo de tráfico permitido.

firmware Tipo de ROM donde se almacena un programa.

primero en entre, primero en salir (FIFO) Esquema de rotación de copia de seguridad donde la copia de seguridad más reciente se guarda en el medio más antiguo. Aunque este es el esquema de rotación más simple, no protege contra errores de datos.

FISA *Ver* Ley Federal de Vigilancia de Inteligencia (FISA) de 1978.

FISMA *Véase* la Ley Federal de Gestión de la Seguridad de la Información (FISMA) de 2002.

sensor accionado por llama Un dispositivo óptico que "mira" el área protegida. Generalmente reacciona más rápido a un incendio que los dispositivos no ópticos.

memoria flash Un tipo de ROM eléctricamente programable.

fluorescente Un sistema de iluminación que utiliza una lámpara de descarga de gas y vapor de mercurio de muy baja presión con fluorescencia para producir luz visible.

clave externa Atributo de una relación que tiene valores que coinciden con la clave principal de otra relación. Las coincidencias entre la clave externa y la clave principal son importantes porque representan referencias de una relación con otra y establecen la conexión entre estas relaciones.

FPGA *Consulte* Field-Programmable Gate Array (FPGA).

T1 fraccionario Una parte de un T1.

Acceso múltiple por división de frecuencia (FDMA) Una técnica de modulación utilizada en redes inalámbricas celulares.

Multiplexación por división de frecuencia (FDM) Proceso utilizado en la multiplexación que divide el medio en una serie de subbandas de frecuencia no superpuestas, cada una de las cuales se utiliza para transportar una señal separada.

Espectro ensanchado de salto de frecuencia (FHSS) Una de las dos tecnologías (junto con DSSS) que formaban parte del estándar 802.11 original. Es único en que cambia las frecuencias o canales cada pocos segundos en un patrón establecido que tanto el transmisor como el receptor conocen.

FRR *Ver* tasa de rechazo falso (FRR).

FTP *Consulte* Protocolo de transferencia de archivos (FTP).

FTPS FTP que incluye compatibilidad adicional para los protocolos criptográficos Seguridad de la capa de transporte (TLS) y Capa de sockets seguros (SSL).

copia de seguridad completa Una copia de seguridad en la que se realiza una copia de seguridad de todos los datos y se borra el bit de archivo de cada archivo.

prueba de interrupción completa Una prueba que implica apagar la instalación primaria y llevar la instalación alternativa a la operación completa.

prueba de conocimiento completo Una prueba en la que se proporciona al equipo de pruebas todo el conocimiento disponible sobre la red de la organización. Esta prueba se centra más en qué ataques se pueden llevar a cabo.

pruebas de exploración no aproximada Una herramienta de prueba dinámica que proporciona entrada al software para probar los límites del software y descubrir defectos. La entrada proporcionada puede ser generada aleatoriamente por la herramienta o creada especialmente para probar vulnerabilidades conocidas.

puerta de enlace Dispositivo que realiza algún tipo de traslación o actúa como punto de control de entrada y salida.

GLBA *Véase* la Ley Gramm-Leach-Bliley (GLBA) de 1999.

Sistema Mundial de Comunicaciones Móviles (GSM) Un estándar para redes celulares digitales.

Modelo de Graham-Denning Un modelo de seguridad que se ocupa de la delegación y cesión de derechos.

Ley Gramm-Leach-Bliley (GLBA) de 1999 Una ley estadounidense que afecta a todas las instituciones financieras, incluidos bancos, compañías de préstamos, compañías de seguros, compañías de inversión y proveedores de tarjetas de crédito. Proporciona directrices para asegurar toda la información financiera y prohíbe compartir información financiera con terceros.

abuelo/padre/hijo (GFS) Esquema de rotación de copia de seguridad donde se definen tres conjuntos de copias de seguridad. La mayoría de las veces, estas tres definiciones son diarias, semanales y mensuales. Las copias de seguridad diarias son los hijos, las copias de seguridad semanales son los padres, y las copias de seguridad mensuales son los abuelos. Cada semana, un hijo avanza al conjunto paterno. Cada mes, un padre avanza al conjunto del abuelo.

pruebas de caja gris Al equipo de pruebas se le proporciona más información que en las pruebas de caja negra, mientras que no tanto como en las pruebas de caja blanca. Las pruebas de caja gris tienen la ventaja de no ser intrusivas mientras se mantiene el límite entre el desarrollador y el probador. Este término se utiliza para referirse a las pruebas de seguridad de red, así como a las pruebas de aplicación.

computación en red El proceso de aprovechar la potencia de CPU de varias máquinas físicas para realizar un trabajo.

GSM *Véase* Sistema Mundial de Comunicaciones Móviles (GSM).

guía Un componente de gobierno de seguridad de la información que proporciona acciones recomendadas que son mucho más flexibles que los estándares, lo que proporciona una asignación para las circunstancias que pueden ocurrir.

Modelo de Harrison-Ruzzo-Ullman Un modelo de seguridad que se ocupa de los derechos de acceso y restringe el conjunto de operaciones que se pueden realizar en un objeto a un conjunto finito para garantizar la integridad.

hash Función unidireccional que reduce un mensaje a un valor hash. Si el valor hash del remitente se compara con el valor hash del receptor, se determina la integridad del mensaje. Si los valores hash resultantes son diferentes, el mensaje se ha modificado de alguna manera, siempre que tanto el remitente como el receptor hayan utilizado la misma función hash.

MAC hash (HMAC) Un MAC con hash con clave que implica una función hash con clave simétrica.

HAVAL Una función unidireccional que genera valores hash de longitud variable, incluidos 128 bits, 160 bits, 192 bits, 224 bits y 256 bits, y utiliza bloques de 1.024 bits.

HDSL *consulte* DSL de alta velocidad de datos de bits (HDSL).

Ley de conciliación de la atención de la salud y la educación de 2010 Una ley estadounidense que afecta a las organizaciones de salud y educación. Aumentó algunas de las medidas de seguridad que se deben tomar para proteger la información de atención médica.

Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA) Una ley estadounidense que afecta a todos los centros de atención médica, compañías de seguros de salud y centros de compensación de atención médica. Proporciona estándares y procedimientos para almacenar, usar y transmitir información médica y datos de atención médica.

pruebas de oídas Evidencia que es de segunda mano, donde el testigo no tiene conocimiento directo del hecho afirmado sino que lo conoce solo a partir de ser contado por alguien.

sensor activado por calor Un sensor que funciona mediante la detección de cambios de temperatura, que puede alertar cuando se cumple una temperatura predefinida o alertar cuando la tasa de aumento es un valor determinado.

base de datos jerárquica Modelo en el que los datos se organizan en una jerarquía. Un objeto puede tener un elemento secundario (un objeto que es un subconjunto del objeto primario), varios elementos secundarios o ningún elemento secundario.

sistema de administración jerárquica de almacenamiento (HSM) Un tipo de sistema de administración de backup que proporciona un backup en línea continuo mediante el uso de "jukeboxes" ópticos o de cinta.

alta disponibilidad Un nivel de disponibilidad que garantiza que los datos estén siempre disponibles, utilizando redundancia y tolerancia a errores.

DSL de alta velocidad de datos de bits (HDSL) Una forma de DSL que proporciona velocidades T1.

idiomas de alto nivel Lenguajes cuyas instrucciones utilizan sentencias abstractas (por ejemplo, IF–THEN–ELSE) y son independientes del procesador. Son fáciles de trabajar, y su sintaxis es similar al lenguaje humano.

Interfaz serie de alta velocidad (HSSI) Una interfaz en el Routers y los multiplexores que proporciona una conexión a los servicios como el Frame Relay y la atmósfera. Funciona a velocidades de hasta 52 Mbps.

HIPAA *Ver* Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA, por sus, por sus).

Marco común de seguridad (CSF) de HITRUST Un marco que pueden usar todas las organizaciones que crean, acceden, almacenan o intercambian datos confidenciales y/o regulados.

HMAC *Consulte* hash MAC.

honeynet Una red que está configurada para ser atractiva para los hackers.

honeypot Un sistema que está configurado para ser atractivo para los hackers y atraerlos a pasar tiempo atacándolos mientras se recopila información sobre el ataque.

sitio caliente Una instalación arrendada que contiene todos los recursos necesarios para el funcionamiento completo.

HSM *Consulte* sistema de administración jerárquica de almacenamiento (HSM).

HSSI *consulte* Interfaz serie de alta velocidad (HSSI).

HTTP *Consulte* Protocolo de transferencia de hipertexto (HTTP).

HTTP-S *Consulte* HTTP-Seguro (HTTP-S).

HTTP-Seguro (HTTP-S) La implementación de HTTP que se ejecuta sobre el protocolo SSL/TLS, que establece una sesión segura utilizando el certificado digital del servidor.

concentrador Un dispositivo físico (capa 1) que funciona como un punto de unión para los dispositivos en una topología en estrella. Se considera físico en el sentido de que no tiene inteligencia.

desastres causados por el hombre Desastres que ocurren a través de la intención o error humano.

amenazas causadas por humanos Amenazas físicas debidas a humanos maliciosos y descuidados.

híbrido Una combinación de topologías de red, incluyendo bus, estrella y anillo.

protocolos de vectores de distancia híbridos o avanzados Protocolos que exhiben características de los protocolos de enrutamiento de estado de enlace y vector de distancia.

nube híbrida Alguna combinación de implementación de nube privada y pública.

higrómetro Un sistema de alerta que monitoriza la humedad.

Protocolo de transferencia de hipertexto (HTTP) Protocolo que se utiliza para ver y transferir páginas web o contenido web.

IaaS *Consulte* la infraestructura como servicio (IaaS).

ICMP *Consulte* Protocolo de mensajes de control de mensajes de Internet (ICMP).

IDaaS *Ver* identidad como servicio (IDaaS).

IDEA *Ver* Algoritmo Internacional de Cifrado de Datos (IDEA).

Modelo IDEAL Modelo desarrollado por el Software Engineering Institute para proporcionar orientación sobre el desarrollo de software. Su nombre es un acrónimo que representa las cinco fases: Iniciar, Diagnosticar, Establecer, Actuar y Aprender.

identificación Proceso en el que un usuario profesa una identidad a un sistema de control de acceso.

Identidad como servicio (IDaaS) Un servicio basado en la nube que proporciona un conjunto de funciones de administración de identidad y acceso a los sistemas de destino en las instalaciones de los clientes o en la nube.

IGMP *Consulte* Protocolo de administración de grupos de Internet (IGMP).

IGP *Consulte* Protocolo de puerta de enlace interior (IGP).

IKE *Consulte* Intercambio de claves de Internet (IKE).

IMAP *Consulte* Protocolo de acceso a mensajes de Internet (IMAP).

direccionamiento implícito Un tipo de direccionamiento de memoria que hace referencia a los registros normalmente contenidos dentro de la CPU.

incidente Una serie de eventos que afectan negativamente a las operaciones y la seguridad de una organización.

delitos informáticos incidentales Un delito informático que se produce en el que el equipo no es la víctima del ataque o el atacante.

Incrementales Un refinamiento al modelo básico de Waterfall, que establece que el software debe desarrollarse en incrementos de la capacidad funcional.

backup incremental Una copia de seguridad en la que se realiza una copia de seguridad de todos los archivos que se han cambiado desde la última copia de seguridad completa o incremental y se borra el bit de almacenamiento de cada archivo.

direccionamiento indirecto Tipo de direccionamiento de memoria donde la ubicación de dirección que se especifica en la instrucción de programa contiene la dirección de la ubicación final deseada.

inferencia Proceso que se produce cuando alguien tiene acceso a información en un nivel que le permite inferir información sobre otro nivel.

activos de información Recetas, procesos, secretos comerciales, planes de producto y cualquier otro tipo de información que permita a la empresa mantener la competitividad dentro de su industria.

modelo de flujo de información Modelo que se centra en controlar los flujos que relacionan dos versiones del mismo objeto.

supervisión continua de la seguridad de la información (ISCM) Un programa que implica mantener un conocimiento continuo de la seguridad de la información, vulnerabilidades y amenazas para apoyar las decisiones de administración de riesgos de la organización.

plan de contingencia del sistema de información (ISCP) Proporciona procedimientos establecidos para la evaluación y recuperación de un sistema después de una interrupción del sistema.

Criterios de evaluación de la seguridad de la tecnología de la información (ITSEC) Un modelo que aborda la integridad y la disponibilidad, así como la confidencialidad.

Infrarrojos Un proceso inalámbrico de corta distancia que utiliza luz, en este caso luz infrarroja, en lugar de ondas de radio.

infraestructura como servicio (IaaS) Un servicio de computación en la nube que involucra al proveedor que proporciona la plataforma de hardware o centro de datos y la empresa instalando y administrando sus propios sistemas operativos y sistemas de aplicaciones. El proveedor simplemente proporciona acceso al centro de datos y mantiene ese acceso.

Modo de infraestructura Un modo en el cual todas las transmisiones entre las estaciones pasan con el AP, y ninguna comunicación directa entre las estaciones ocurre.

validación de entrada Proceso mediante el cual se comprueba el formato y la longitud de la entrada antes de que se utilice.

activos intangibles Activos como la propiedad intelectual, los datos y la reputación de la organización que son vitales y tienen valor para una empresa, pero que no se pueden tocar.

Red Digital de Servicios Integrados (ISDN) A veces se conoce como acceso telefónico digital, un método de comunicaciones que ahora sólo se utiliza como una conexión de copia de seguridad.

integridad Una característica proporcionada si puede estar seguro de que los datos no han cambiado de ninguna manera. El principio de la tríada de la CIA que garantiza que los datos sean precisos y fiables.

pruebas de interfaz Evalúa si los sistemas o componentes de una aplicación se pasan correctamente datos y controles entre sí. Comprueba si las interacciones del módulo funcionan correctamente y los errores se controlan correctamente.

Protocolo de puerta de enlace interior (IGP) Un protocolo de ruteo propietario de Cisco con clase obsoleto.

sistema intermedio a sistema intermedio (IS-IS) Un protocolo de enrutamiento interior complejo que se basa en protocolos OSI en lugar de IP.

amenazas internas Amenazas de aquellos que podrían tener algún acceso a la habitación o edificio.

Algoritmo internacional de cifrado de datos (IDEA) Un cifrado de bloques que utiliza bloques de 64 bits, que se dividen en 16 bloques más pequeños. Utiliza una clave de 128 bits y realiza ocho rondas de transformaciones en cada uno de los 16 bloques más pequeños.

Organización Internacional de Normalización (ISO) y comisión electrotécnica internacional (IEC) *Véase* ISO/IEC 27000.

Protocolo de mensajes de control de Internet (ICMP) Protocolo utilizado por los dispositivos de red para enviar un mensaje sobre el éxito o el fracaso de las comunicaciones y utilizado por los seres humanos para solucionar problemas. Cuando se utilizan los programas PING o TRACEROUTE, se utiliza ICMP.

Protocolo de administración de grupos de Internet (IGMP) Un protocolo utilizado para la multidifusión, que es una forma de comunicación mediante la cual un host envía a un grupo de hosts de destino en lugar de un solo host (llamado transmisión de unidifusión) o a todos los hosts (llamado transmisión de difusión).

Intercambio de claves de Internet (IKE) Un método de intercambio de claves que proporciona el material autenticado utilizado para crear las claves intercambiadas por ISAKMP utilizado para realizar la autenticación del mismo nivel. También se conoce a veces como intercambio de claves IPsec.

Protocolo de acceso a mensajes de Internet (IMAP) Un protocolo de capa de aplicación para la recuperación de correo electrónico.

Protocolo de Internet (IP) Un protocolo que es responsable de colocar las direcciones IP de origen y destino en el paquete y de enrutar el paquete a su destino.

Protocolo de seguridad de Internet (IPsec) Un conjunto de protocolos que establece un canal seguro entre dos dispositivos. Puede proporcionar cifrado, integridad de datos y autenticación basada en el sistema, lo que lo convierte en una opción flexible para proteger las transmisiones.

Internet Security Association and Key Management Protocol (ISAKMP) Protocolo que controla la creación de una asociación de seguridad para la sesión y el intercambio de claves.

Interfaz de sistema de equipos pequeños de Internet (iSCSI) Una tecnología que permite que los comandos SCSI se envíen de extremo a extremo a través de LAN, WAN o Internet a través de TCP.

Internet de las cosas (IoT) Un sistema de dispositivos informáticos interrelacionados, máquinas mecánicas y digitales, y objetos que se proporcionan con identificadores únicos y la capacidad

de transferir datos a través de una red sin necesidad de interacción de persona a persona o de persona a computadora.

interrumpir Una señal utilizada por un dispositivo de entrada/salida cuando requiere que la CPU realice alguna acción.

intranet La red interna de una empresa.

IoT *Ver* Internet de las Cosas.

IP *Consulte* Protocolo de Internet (IP).

Suplantación de direcciones IP Una técnica que utilizan los hackers para ocultar su rastro o para hacerse pasar por otro ordenador en el que alteran la dirección IP tal y como aparece en el paquete.

Convergencia de P.I. Implica llevar diferentes tipos de tráfico a través de una red. El tráfico incluye voz, vídeo, datos e imágenes. Se basa en el Protocolo de Internet (IP) y soporta aplicaciones multimedia.

IPsec *Consulte* Seguridad del protocolo de Internet (IPsec).

IS-IS *Ver* sistema intermedio a sistema intermedio (IS-IS).

ISAKMP *Consulte* Internet Security Association and Key Management Protocol (ISAKMP).

ISCM *Ver* monitoreo continuo de seguridad de la información (ISCM).

ISCP *Ver* plan de contingencia del sistema de información.

iSCSI *Consulte* Interfaz de sistema de equipos pequeños de Internet.

ISDN *Véase* Red Digital de Servicios Integrados (ISDN).

ISO/IEC 27000 Estándares que proporcionan orientación a las organizaciones sobre la integración de la seguridad en el desarrollo y mantenimiento de aplicaciones de software. Estas normas forman parte de una serie que establece normas de seguridad de la información y es publicada conjuntamente por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (CEI).

aislamiento Una situación en la que las transacciones no interactúan con otras transacciones hasta su finalización.

Directiva de seguridad específica del problema Una directiva de seguridad que aborda problemas de seguridad específicos.

ITSEC *Consulte* Criterios de evaluación de la seguridad de las tecnologías de la información (ITSEC).

JAD *Ver* modelo de Desarrollo de Análisis Conjunto (JAD).

Applet de Java Un pequeño componente creado con Java que se ejecuta en un navegador web. Es independiente de la plataforma y crea código intermedio denominado código de bytes que no es específico del procesador.

Conectividad de base de datos Java (JDBC) Una API que permite que las aplicaciones Java se comuniquen con una base de datos.

Java Platform, Enterprise Edition (J2EE) Un modelo de componentes distribuidos que se basa en el lenguaje de programación Java. Es un marco utilizado para desarrollar software que proporciona API para servicios de red y utiliza un proceso de comunicación entre procesos que se basa en CORBA.

JDBC *Consulte* Java Database Connectivity (JDBC).

rotación de trabajos Una medida de seguridad que garantiza que más de una persona cumpla con las tareas laborales de un solo puesto dentro de una organización. Se refiere a la capacitación de varios usuarios para realizar las tareas de un puesto para ayudar a prevenir el fraude por parte de cualquier empleado individual.

Modelo de desarrollo de análisis conjunto (JAD) También denominado desarrollo de aplicaciones conjuntas (JAD), un modelo de desarrollo que utiliza un enfoque de equipo tanto para acordar los requisitos como para resolver las diferencias. La teoría es que al reunir a todas las partes en todas las etapas, surgirá un producto más satisfactorio al final del proceso.

Ley Kennedy-Kassebaum *Ver* Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA, por sus, por sus).

Kerberos Un protocolo de autenticación que utiliza un modelo cliente/servidor desarrollado por el Proyecto Athena del MIT. Es el modelo de autenticación predeterminado en las últimas ediciones de Windows Server y también se usa en los sistemas operativos Apple, Sun y Linux.

firewall de proxy del núcleo Un ejemplo de un firewall de quinta generación que inspecciona un paquete en cada capa del modelo OSI pero no introduce el impacto en el rendimiento que un firewall de capa de aplicación lo hará porque lo hace en la capa de kernel.

clave Parámetro que controla la transformación de texto no cifrado en texto cifrado o viceversa. Determinar los datos de texto no cifrado originales sin la clave es imposible. También se conoce como criptovariable.

agrupación en clústeres de claves El proceso que se produce cuando diferentes claves de cifrado generan el mismo texto cifrado a partir del mismo mensaje de texto no cifrado.

espacio de teclas Todos los valores de clave posibles cuando se utiliza un algoritmo determinado u otra medida de seguridad. Una clave de 40 bits tendría 240 valores posibles, mientras que una clave de 128 bits tendría 2.128 valores posibles.

factores de conocimiento Factores que son algo que una persona conoce.

ataque de texto sin formato conocido Ataque que se produce cuando un atacante utiliza las versiones de texto no cifrado y texto cifrado de un mensaje para detectar la clave utilizada.

L2TP *Consulte* el Protocolo de túnel de capa 2 (L2TP).

Protocolo de distribución de etiquetas (LDP) Permite que el Routers capaz del Multiprotocol Label Switching (MPLS) intercambie la información de la asignación de la escritura de la etiqueta.

vidrio laminado Dos láminas de vidrio con una película de plástico entre las que hace que sea más difícil de romper.

LAN *Consulte* red de área local (LAN).

Protocolo de túnel de capa 2 (L2TP) Protocolo que funciona en la capa 2 del modelo OSI. Puede utilizar varios mecanismos de autenticación como PPTP puede, pero no proporciona ningún cifrado. Normalmente se utiliza con IPsec, un mecanismo de cifrado muy fuerte.

conmutador de capa 3 Un conmutador que tiene funcionalidad de enrutamiento también integrada.

conmutador de capa 4 Un conmutador que proporciona enrutamiento adicional por encima de la capa 3 mediante el uso de los números de puerto que se encuentran en el encabezado de la capa de transporte para tomar decisiones de enrutamiento.

modelo de defensa en capas Un modelo en el que la confianza no se basa en un único concepto de seguridad física, sino en el uso de múltiples enfoques que se apoyan entre sí.

LDAP *Consulte* Protocolo ligero de acceso a directorios (LDAP).

privilegio mínimo Un principio de seguridad que requiere que a un usuario o proceso se le otorgue solo el privilegio de acceso mínimo necesario para realizar una tarea determinada. También conocido como necesidad de saber.

responsabilidad El estado de ser legalmente responsable ante otra entidad debido a sus acciones o negligencia.

Protocolo ligero de acceso a directorios (LDAP) Un protocolo de acceso a directorios (DAP) que se basa en DAP de X.500 y es más simple que X.500.

Protocolo de estado de vínculos Un protocolo de enrutamiento que solo comparte los cambios de red (interrupciones y recuperaciones de vínculos) con los vecinos, lo que reduce en gran medida la cantidad de tráfico generado. Este tipo de protocolo también utiliza una métrica sofisticada que se basa en muchos factores, tales como el ancho de banda de cada link en el trayecto y la congestión en cada link.

Modelo de Lipner Un modelo de seguridad que comparte características con el modelo de Clark-Wilson en el que separa los objetos en datos y programas.

red de área local (LAN) Un grupo de sistemas que están conectados con una conexión de red rápida. Para los propósitos de esta discusión, es decir cualquier conexión sobre el 10 Mbps y generalmente en una sola ubicación.

factores de ubicación Factores para autenticar a un usuario en función de la ubicación desde la que se autentica el usuario.

registro Un registro de eventos que se producen en un activo de la organización, incluidos sistemas, redes, dispositivos e instalaciones. Cada entrada de un registro cubre un único evento que se produce en el activo.

revisión de registros Una práctica importante para garantizar que los problemas se detectan antes de que se conviertan en problemas importantes. Los registros de seguridad informática son especialmente importantes porque pueden ayudar a una organización a identificar incidentes de seguridad, infracciones de directivas y fraudes.

bomba lógica Tipo de malware que se ejecuta cuando tiene lugar un evento.

control lógico Componentes de software o hardware utilizados para restringir el acceso.

LonWorks/LonTalk3 Un protocolo de sistema de control industrial punto a punto que utiliza el puerto 1679.

MAC *Consulte* control de acceso obligatorio (MAC).

Dirección MAC *Consulte* dirección de control de acceso a medios (MAC).

lenguajes de máquina Idiomas que entregan instrucciones directamente al procesador.

virus de macro Virus que infectan programas escritos en Word, Basic, Visual Basic o VBScript que se utilizan para automatizar funciones. Estos virus infectan archivos de Microsoft Office y son fáciles de crear porque el lenguaje subyacente es simple e intuitivo de aplicar. Estos virus son especialmente peligrosos en el que infectan el propio sistema operativo. También se pueden transportar entre diferentes sistemas operativos, ya que los lenguajes son independientes de la plataforma.

gancho de mantenimiento Un conjunto de instrucciones integradas en el código que permite a alguien que conoce la "puerta trasera" utilizar las instrucciones para conectarse para ver y editar el código sin utilizar los controles de acceso normales.

el malware Cualquier software que dañe un equipo, elimine datos o realice acciones que el usuario no autorizó.

MAN *Ver* red de área metropolitana (MAN).

control de gestión *Ver* control administrativo.

control de acceso obligatorio (MAC) Un modelo de control de acceso en el que la autorización del sujeto se basa en etiquetas de seguridad.

mantrap Una serie de dos puertas con una pequeña habitación entre ellas.

modelo basado en matrices Un modelo de seguridad que organiza tablas de sujetos y objetos que indica qué acciones pueden realizar los sujetos individuales sobre objetos individuales.

MD2 Un algoritmo de síntesis de mensaje que genera un valor hash de 128 bits y realiza 18 rondas de cálculos.

MD4 Un algoritmo de síntesis de mensaje que genera un valor hash de 128 bits y realiza solo 3 rondas de cálculos.

MD5 Un algoritmo de síntesis de mensaje que genera un valor hash de 128 bits y realiza 4 rondas de cálculos.

MD6 Un algoritmo de síntesis de mensaje que genera un valor hash variable, realizando un número variable de cálculos.

tiempo medio entre fallos (MTBF) La cantidad estimada de tiempo que un dispositivo funcionará antes de que se produzca un error. Describe la frecuencia con la que se produce un error en un componente en promedio.

tiempo medio de reparación (MTTR) El tiempo medio necesario para reparar un único recurso o función cuando se produce un desastre o una interrupción. Describe la cantidad media de tiempo que se tardará en arreglar un dispositivo y volver a estar en línea.

medias Cómo un sospechoso llevó a cabo un crimen.

Dirección de control de acceso a medios (MAC) En Ethernet, una dirección física de 48 bits expresada en hexadecimal que se asigna permanentemente a un dispositivo.

vapor de mercurio Un sistema de iluminación que utiliza un arco eléctrico a través de mercurio vaporizado para producir luz.

topología de malla La topología de red más tolerante a errores y más costosa de implementar. En él, todos los dispositivos están conectados a todos los demás dispositivos.

Metro Ethernet El uso de la tecnología Ethernet en un área amplia.

red de área metropolitana (MAN) Un tipo de LAN que abarca un área grande, como el centro de una ciudad.

MIMO *Ver* entrada múltiple, salida múltiple (MIMO).

pruebas de casos de mal uso Tipo de prueba que prueba una aplicación para asegurarse de que la aplicación puede controlar la entrada no válida o el comportamiento inesperado. También conocido como prueba negativa.

ley mixta Un tipo de ley que combina dos o más de los otros tipos de ley. La ley más a menudo mixta utiliza el derecho civil y el derecho consuetudinario.

código móvil Las instrucciones se pasan a través de una red y se ejecutan en un sistema remoto. Un tipo de código que se puede transferir a través de una red y, a continuación, ejecutar en un sistema o dispositivo remoto.

IPv6 móvil (MIPv6) Un protocolo mejorado que admite la itinerancia para un nodo móvil, de modo que pueda moverse de una red a otra sin perder la conectividad de la capa IP (como se define en RFC 3775).

Modbus Un protocolo de sistema de control industrial maestro/esclavo que utiliza el puerto 50.

cifrado mono-alfabético de subestaciones Un cifrado que utiliza un solo alfabeto.

motivo Por qué se cometió un delito y quién cometió el delito. MOM significa motivo, oportunidad y medios.

iluminación móvil Iluminación que se puede reposicionar según sea necesario.

MPLS *Consulte* Multiprotocol Label Switching (MPLS).

MTBF *Ver* tiempo medio entre fallos (MTBF).

MTD *Ver* tiempo de inactividad máximo tolerable.

MTTR *Ver* tiempo medio de reparación (MTTR).

MU MIMO *Ver* entrada múltiple multiusuario, salida múltiple (MU MIMO).

multidifusión Una señal recibida por todos los demás en un grupo de multidifusión. Se considera uno a muchos.

autenticación multifactor Un tipo de autenticación que incluye dos o más tipos de factores de autenticación. Agregar más tipos de factores aumenta la seguridad de la autenticación.

modelo de celosía multinivel Un modelo desarrollado principalmente para tratar cuestiones de confidencialidad que se centra principalmente en el flujo de información.

multimodo Cable de fibra óptica que utiliza varios haces de luz al mismo tiempo y utiliza LED como fuente de luz.

virus multipartito Un virus que puede infectar tanto archivos de programa como sectores de arranque.

entrada múltiple, salida múltiple (MIMO) Uso de múltiples antenas, que permiten hasta cuatro flujos espaciales a la vez.

multiplexador Un dispositivo físico (capa 1) que combina varias señales de información de entrada en una señal de salida, que lleva varios canales de comunicación, mediante alguna técnica múltiplex.

Conmutación de etiquetas multiprotocolo (MPLS) Protocolo que enruta los datos de un nodo al siguiente basándose en etiquetas de ruta de acceso corta en lugar de direcciones de red largas, lo que evita búsquedas complejas en una tabla de enrutamiento. Incluye la capacidad de controlar cómo y dónde se enruta el tráfico, ofrece servicios de transporte de datos a través de la misma red y mejora la resistencia de la red a través de MPLS Fast Reroute.

multitarea El proceso de llevar a cabo más de una tarea a la vez.

subprocesamiento múltiple Una característica que permite realizar varias tareas dentro de un único proceso.

entrada múltiple multiusuario, salida múltiple (MU MIMO) Un conjunto de tecnologías MIMO para la comunicación inalámbrica en el que los usuarios o puntos de acceso inalámbricos, cada uno con una o más antenas, se comunican entre sí.

NAS *Consulte* almacenamiento conectado en red (NAS) o servidor de acceso a la red (NAS).

NAT *Consulte* traducción de direcciones de red (NAT).

control de acceso natural Un concepto que se aplica a las entradas de la instalación y abarca la colocación de las puertas, luces, vallas e incluso paisajismo. Su objetivo es satisfacer los objetivos de seguridad de la manera menos molesta y estéticamente atractiva.

lenguajes naturales Lenguajes cuyo objetivo es crear software que pueda resolver problemas por sí solo en lugar de requerir que un programador cree código para tratar el problema. Aunque no se realiza completamente, es un objetivo que vale la pena perseguir utilizando el procesamiento basado en el conocimiento y la inteligencia artificial.

vigilancia natural El uso de características ambientales físicas para promover la visibilidad de todas las zonas y así desalentar la delincuencia en esas zonas. La idea es fomentar el flujo de personas de tal manera que el mayor porcentaje posible del edificio esté siempre poblado, porque la gente de una zona desalienta la delincuencia.

refuerzo de los territoriales naturales Crear un sentimiento de comunidad en un área extendiendo el sentido de propiedad a los empleados.

amenazas naturales Amenazas físicas que deben abordarse y mitigarse y que son causadas por las fuerzas de la naturaleza.

comunicación de campo cercano (NFC) Un conjunto de protocolos de comunicación que permiten que dos dispositivos electrónicos, uno de los cuales suele ser un dispositivo móvil, establezcan la comunicación llevándolos a menos de 2 pulgadas el uno del otro.

necesidad de saber El concepto de que los usuarios solo deben tener acceso a los recursos necesarios para realizar su trabajo. Define cuáles son los privilegios mínimos reales para cada trabajo o función empresarial.

pruebas negativas *Ver* prueba de casos de mal uso.

control de acceso a la red (NAC) Un servicio que va más allá de la autenticación del usuario e incluye un examen del estado del equipo que el usuario está introduciendo en la red al realizar un acceso remoto o una conexión VPN a la red.

servidor de acceso a la red (NAS) Dispositivo que controla el acceso a una red.

traducción de direcciones de red (NAT) Un servicio que cambia una dirección IP privada a una dirección pública que se puede enrutar en Internet. Cuando la respuesta se devuelve desde la web, el servicio NAT la recibe y traduce la dirección a la dirección IP privada original y la devuelve al originador.

análisis de detección de red Examina un intervalo de direcciones IP para determinar qué puertos están abiertos. Este tipo de análisis sólo muestra una lista de los sistemas de la red y los puertos en uso en la red.

Capa de red (capa 3) La capa del modelo de referencia OSI en la que se agrega la información necesaria para enrutar un paquete en forma de dirección lógica de origen y destino.

almacenamiento de información conectado en red (NAS) Una forma de almacenamiento de red que utiliza la red LAN existente para el acceso mediante protocolos de acceso a archivos como NFS o SMB.

análisis de vulnerabilidad de red Sondea un sistema o red de destino para identificar vulnerabilidades. Es un análisis más complejo de la red que un análisis de detección de red.

NIST SP 800-92 Una guía para la administración de registros de seguridad informática.

NIST SP 800-137 Una guía para el monitoreo continuo de seguridad de la información (ISCM) para sistemas de información y organizaciones federales.

ruido Interferencia que se puede introducir en el cable que causa problemas.

nonce Un número aleatorio que se utiliza una sola vez y actúa como una variable de marcador de posición en las funciones.

modelo de no intervención Un modelo menos preocupado por el flujo de información que por el conocimiento de un sujeto del estado del sistema en un momento dado; se concentra en evitar que las acciones que tienen lugar en un nivel alteren el Estado presentado a otro nivel.

no repudio La garantía de que un usuario no puede denegar una acción.

memoria no volátil Almacenamiento persistente a largo plazo que permanece incluso cuando el dispositivo se apaga.

cifrado nulo *Véase* cifrado de ocultación.

objeto Recurso al que un usuario o proceso desea tener acceso.

vinculación e incrustación de objetos (OLE) Método para compartir objetos en un equipo local que utiliza COM como base.

base de datos de vinculación e incrustación de objetos (OLE DB) Reemplazo de ODBC que extiende la funcionalidad de ODBC a bases de datos no relacionales.

base de datos orientada a objetos (OODB) Un modelo que tiene la capacidad de controlar una variedad de tipos de datos y es más dinámico que una base de datos relacional. Los sistemas OODB son útiles para almacenar y manipular datos complejos, como imágenes y gráficos.

programación orientada a objetos (OOP) Tipo de programación en el que los objetos se organizan en una jerarquía en clases con características denominadas atributos asociados a cada uno. OOP hace hincapié en el empleo de objetos y métodos en lugar de tipos o transformaciones como en otros enfoques de software.

base de datos relacional de objetos Un modelo que es un matrimonio de tecnologías orientadas a objetos y relacionales, combinando los atributos de ambas.

plan de emergencia para ocupantes (OEP) Un plan que describe los procedimientos de primera respuesta para los ocupantes de una instalación en caso de una amenaza o incidente para la salud y la seguridad del personal, el medio ambiente o la propiedad.

OCSP *Consulte* Protocolo de estado de certificados en línea (OCSP).

ODBC *Consulte* Conectividad abierta de bases de datos (ODBC).

OEP *Ver* plan de emergencia para ocupantes.

OFB *Consulte* Retroalimentación de salida (OFB).

MDFO *Véase* Multiplexación por división de frecuencia ortogonal (MDFO).

OLE *Vea* vinculación e incrustación de objetos (OLE).

OLE DB *Vea Base* de datos de vinculación e incrustación de objetos (OLE DB).

Prueba ACID oltp Prueba en la que se utiliza un sistema de procesamiento de transacciones en línea para supervisar problemas como los procesos que dejan de funcionar. Su objetivo principal es evitar que las transacciones que no ocurren correctamente o no están completas surtan efecto. Una prueba ACID garantiza que cada transacción tiene ciertas propiedades antes de que se confirma.

servicios de identidad locales Servicios de identidad proporcionados dentro de una empresa.

almohadilla de un solo uso El esquema de cifrado más seguro que se puede utilizar. Funciona como un cifrado en ejecución en el que el valor de clave se agrega al valor de las letras. Sin embargo, utiliza una clave que tiene la misma longitud que el mensaje de texto no cifrado.

función unidireccional Una función matemática que se puede realizar más fácilmente en una dirección que en la otra.

Protocolo de estado de certificados en línea (OCSP) Protocolo de Internet que obtiene el estado de revocación de un certificado digital X.509.

Sistema de procesamiento de transacciones en línea *Consulte* la prueba OLTP ACID.

OODB *Consulte* base de datos orientada a objetos (OODB).

OOP *Ver* programación orientada a objetos (OOP).

conectividad abierta de bases de datos (ODBC) Una API que permite la comunicación con bases de datos de forma local o remota.

Abrir primero la ruta más corta (OSPF) Un protocolo de estado de enlace basado en estándares.

sistema abierto Un sistema que se ajusta a los estándares de la industria y puede trabajar con sistemas que admiten el mismo estándar.

Modelo de interconexión de sistemas abiertos (OSI) Un modelo creado en la década de 1980 por la Organización Internacional de Normalización (ISO) como parte de su misión de crear un conjunto de protocolos para ser utilizado como estándar para todos los proveedores.

Abrir proyecto de seguridad de aplicaciones web (OWASP) Un proyecto de seguridad de aplicaciones de código abierto. Este grupo crea directrices, procedimientos de prueba y herramientas para ayudar con la seguridad web. Un grupo que monitorea los ataques, específicamente los ataques web. OWASP mantiene una lista de los 10 principales ataques de forma continua.

huellas digitales del sistema operativo El proceso de utilizar algún método para determinar el sistema operativo que se ejecuta en un host o un servidor.

investigación de operaciones Una investigación sobre un evento o incidente que no resulte en ningún problema penal, civil o regulatorio.

seguridad de las operaciones Las actividades que apoyan el mantenimiento continuo de la seguridad de un sistema sobre una base diaria.

evidencia de opinión Evidencia que se basa en lo que el testigo piensa, siente o infiere con respecto a los hechos.

oportunidad Dónde y cuándo ocurrió un delito.

Libro naranja Colección de criterios basados en el modelo Bell-LaPadula que se utiliza para calificar o calificar la seguridad que ofrece un producto de sistema informático.

directiva de seguridad de la organización La directiva de seguridad de más alto nivel adoptada por una organización que describe los objetivos de seguridad.

Multiplexación por división de frecuencia ortogonal (MDFO) Una técnica más avanzada de modulación en la que se utiliza un gran número de señales de subportadora ortogonal estrechamente espaciadas para transportar los datos en varios flujos de datos paralelos. Se utiliza en 802.11a, 802.11ac y 802.11g y hace posible una velocidad de hasta 54 Mbps.

OSI *Ver* Modelo de Interconexión de Sistemas Abiertos (OSI).

OSPF *vea* el Open Shortest Path First (OSPF).

Retroalimentación de salida (OFB) Un modo DES que funciona con bloques de 8 bits (o más pequeños) que utiliza una combinación de cifrado de secuencias y cifrado de bloques. Sin embargo, OFB utiliza la secuencia de claves anterior con la clave para crear la siguiente secuencia de claves.

OWASP *Vea* Open Web Application Security Project (OWASP).

factores de propiedad Factores que son algo que una persona posee, como una contraseña.

PaaS *Ver* plataforma como servicio (PaaS).

servidor de seguridad de filtrado de paquetes Un firewall que solo inspecciona el encabezado de un paquete en busca de direcciones IP o números de puerto permitidos.

red de conmutación de paquetes Una red que agrupa todos los bloques de datos transmitidos, llamados paquetes. Cada paquete se trata individualmente con respecto a la encaminamiento.

PAP *Consulte* Protocolo de autenticación de contraseña (PAP).

prueba paralela Una prueba que implica llevar un sitio de recuperación a un estado de preparación operativa pero mantener las operaciones en el sitio primario.

virus parásito Un virus que se adhiere a un archivo, normalmente un archivo ejecutable, y luego entrega la carga útil cuando se utiliza el programa.

prueba de conocimiento parcial Una prueba en la que se proporciona al equipo de pruebas un conocimiento público sobre la red de la organización. Se pueden establecer límites para este tipo de prueba.

sistema de infrarrojo pasivo (PIR) Un sistema de detección que funciona mediante la identificación de cambios en las olas de calor en un área.

escáner de vulnerabilidad pasiva (PVS) Supervisa el tráfico de red en la capa de paquetes para determinar la topología, los servicios y las vulnerabilidades.

Protocolo de autenticación de contraseña (PAP) Protocolo que proporciona autenticación pero en el que las credenciales se envían en texto no cifrado y se pueden leer con un rastreador.

enmascaramiento de contraseñas Una medida que evita que una contraseña se aprenda a través del shoulder surfeando oscureciendo los caracteres introducidos a excepción del último.

PAT *Consulte* traducción de direcciones de puerto (PAT).

panel de parches Un panel que opera en la capa física del modelo OSI y simplemente funciona como un punto de terminación central para todos los cables que atraviesan las paredes de los enchufes de pared, que a su vez están conectados a computadoras con cables.

patente Un tipo de propiedad intelectual que abarca una invención descrita en una solicitud de patente y se concede a una persona o empresa.

Estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS) Se aplica a todas las entidades que almacenan, procesan y/o transmiten datos de titulares de tarjetas. Cubre los componentes técnicos y operativos del sistema incluidos en los datos del titular de la tarjeta o conectados a ellos. Si una organización acepta o procesa tarjetas de pago, PCI DSS se aplica a esa organización.

PBX *Consulte* Central de conmutación (PBX).

Informática punto a punto Una solución cliente/servidor en la que cualquier plataforma puede actuar como cliente o servidor o ambos.

prueba de penetración Una prueba que simula un ataque para identificar cualquier riesgo que pueda derivarse de las vulnerabilidades de un sistema o dispositivo.

permutación *Ver* transposición.

red de área personal (PAN) Incluye dispositivos, como ordenadores, teléfonos, tabletas y teléfonos móviles, que están muy cerca entre sí. Los PANs generalmente se implementan usando Bluetooth, Z-Wave, Zigbee y Infrared Data Association (IrDA).

Ley de Protección de Información Personal y Documentos Electrónicos (PIPEDA) Una ley de Canadá que afecta la forma en que las organizaciones del sector privado recopilan, usan y divulgan información personal en el curso de negocios comerciales. La ley fue escrita para abordar las preocupaciones de la Unión Europea sobre la seguridad de la PII.

información de identificación personal (PII) Cualquier dato que se pueda utilizar solo o con otra información para identificar a una sola persona.

pharming Un ataque de ingeniería social, similar a la suplantación de identidad (phishing), que en realidad contamina el contenido de la caché dns de un equipo para que las solicitudes a un sitio legítimo se enruten realmente a un sitio alternativo.

PHI *Consulte la* información de salud protegida.

phishing Un ataque de ingeniería social en el que los atacantes intentan obtener información personal, incluida la información de tarjetas de crédito y datos financieros. Por ejemplo, un ataque en el que un destinatario está convencido de hacer clic en un enlace en un correo electrónico que parece ir a un sitio de confianza, pero en realidad va al sitio del hacker.

clonación de teléfonos Un proceso en el que se realizan copias de un chip SIM, permitiendo a otro usuario realizar llamadas como el usuario original.

sistema fotométrico Un sistema de detección que funciona mediante la detección de cambios en la luz y por lo tanto se utiliza en áreas sin ventanas. Envía un haz de luz a través del área, y si el haz es interrumpido (por una persona, por ejemplo), se activa la alarma.

activos físicos Activos que se pueden tocar, incluidos equipos o computadoras.

control físico Un control de seguridad, como un guardia, que protege las instalaciones y el personal de una organización.

Capa física (capa 1) La capa del modelo de referencia OSI responsable de convertir la información en bits (unos y ceros) y enviarla al medio.

PII *Ver* información de identificación personal (PII).

ping de ataque a muerte Un ataque que implica el envío de varios paquetes de gran tamaño, lo que puede hacer que el sistema de la víctima sea inestable al menos y posiblemente se congele.

análisis de ping Un ataque que básicamente hace ping a cada dirección IP y realiza un seguimiento de qué direcciones IP responden al ping.

PIPEDA *Ver* Ley de Protección de Información Personal y Documentos Electrónicos (PIPEDA).

procesador canalizadas Un procesador que se superpone a los pasos de diferentes instrucciones, a diferencia de un procesador escalar, que ejecuta una instrucción a la vez.

texto sin formato Un mensaje en su formato original. También se conoce como texto no cifrado.

plataforma como servicio (PaaS) Un servicio de computación en la nube que involucra al proveedor que proporciona la plataforma de hardware o el centro de datos y el software que se ejecuta en la plataforma. La empresa sigue implicada en la gestión del sistema.

Protocolo punto a punto (PPP) Un protocolo de capa 2 que realiza la trama y encapsulación de datos a través de conexiones punto a punto.

Protocolo de túnel punto a punto (PPTP) Un protocolo de Microsoft basado en PPP. Usa el cifrado punto a punto integrado de Microsoft y puede usar varios métodos de autenticación, incluidos CHAP, MS-CHAP y EAP-TLS.

política Un componente de gobierno de seguridad de la información que describe los objetivos, pero no proporciona ninguna forma específica de lograr los objetivos establecidos.

sondeo Método de contención donde un dispositivo primario sondea entre sí para ver si necesita transmitir.

cifrado de subestación polialfábética Cifrado que utiliza varios alfabetos.

poliinstanciación Proceso utilizado para evitar infracciones de inferencia de datos. Para ello, permite que una relación contenga varias tuplas con las mismas claves principales con cada instancia distinguiéndose por un nivel de seguridad. Impide que los usuarios de bases de datos de bajo nivel deduzca la existencia de datos de nivel superior. El desarrollo de una versión detallada de un objeto a partir de otro objeto utilizando valores diferentes en el nuevo objeto.

virus polimórfico Un virus que hace copias de sí mismo y, a continuación, realiza cambios en esas copias. Lo hace con la esperanza de evitar la detección por el software antivirus.

polimorfismo La capacidad de diferentes objetos con un nombre común para reaccionar al mismo mensaje o entrada con una salida diferente.

POP *Consulte* Protocolo de oficina de correos (POP).

Traducción de direcciones de puerto (PAT) Una versión específica de NAT que utiliza una sola dirección IP pública para representar varias direcciones IP privadas.

aislamiento de puertos Una VLAN privada que es sólo para acceder a un sistema invitado.

análisis de puertos Un ataque que básicamente hace ping a cada combinación de dirección y número de puerto y realiza un seguimiento de qué puertos están abiertos en cada dispositivo, ya que los pings son respondidos por puertos abiertos con servicios de escucha y no respondidos por puertos cerrados.

Protocolo de oficina de correos (POP) Un protocolo de recuperación de correo electrónico de la capa de aplicación.

POTS (Plain Old Telephone Service) *Ver* red telefónica conmutada pública (RTC).

acondicionador de energía Un dispositivo que va entre una toma de corriente y un dispositivo electrónico y suaviza las fluctuaciones de la energía entregada al dispositivo electrónico, protegiendo contra hundidos y sobretensiones.

PPP *Consulte* Protocolo punto a punto (PPP).

PPTP *Consulte* Protocolo de túnel punto a punto (PPTP).

extintor de preacción Un extintor que funciona como un sistema de tuberías secas, excepto que el cabezal del aspersor tiene un enlace térmico-fusible que debe fundirse antes de que se libere el agua. Este es actualmente el sistema recomendado para una sala de computadoras.

Capa de presentación (capa 6) La capa de modelo de referencia OSI responsable de la manera en que los datos de la capa de aplicación se representan (o se presentan) a la capa de aplicación en el dispositivo de destino. Si se requiere alguna traducción entre formatos, esta capa se encarga de ello.

control preventivo Un control de seguridad que impide que se produzca un ataque.

PRI ISDN *Ver* Tasa Primaria ISDN (PRI).

Isdn de la tarifa primaria (PRI) Una solución que proporciona hasta 23 canales B y un canal D para un total de 1,544 Mbps.

Central de conmutación (PBX) Un conmutador telefónico privado que reside en las instalaciones de un cliente. Tiene una conexión directa al conmutador del proveedor de telecomunicaciones y realiza el enrutamiento de llamadas dentro del sistema telefónico interno.

nube privada Una solución de implementación en la nube propiedad y administrada por una empresa únicamente para el uso de esa empresa.

direcciones IP privadas Tres intervalos de direcciones IPv4 reservados para ser utilizados *sólo* dentro de redes privadas y *no* en Internet.

cifrado de clave privada *Consulte* cifrado simétrico.

arrastramiento de privilegios *Consulte* agregación de acceso.

elevación de privilegios El proceso de explotar un error o debilidad en un sistema operativo para permitir a los usuarios recibir privilegios a los que no tienen derecho.

procedimiento Un componente de gobierno de seguridad de la información que incluye todas las acciones detalladas que el personal debe seguir.

proceso Conjunto de acciones, pasos o subprocesos que forman parte de la misma pieza de trabajo más grande realizada para una aplicación específica o para lograr un fin determinado.

información médica protegida (PHI) Cualquier información de salud identificable individualmente.

creación de prototipos Usar un ejemplo de código para explorar un enfoque específico para resolver un problema antes de invertir mucho tiempo y dinero en el enfoque.

aprovisionamiento El acto de crear una cuenta de acceso.

ciclo de vida del aprovisionamiento Un proceso formal para crear, cambiar y quitar usuarios.

dispositivo de autenticación de proximidad Una tarjeta programable utilizada para entregar un código de acceso al dispositivo, ya sea deslizando la tarjeta o, en algunos casos, simplemente estando en las proximidades del lector.

servidor de seguridad proxy Un firewall que crea una conexión web entre sistemas en su nombre normalmente permite a los sistemas permitir y no permitir el tráfico de forma más granular. Los firewalls proxy realmente se interponen entre cada conexión desde el exterior hasta el interior y realizan la conexión en nombre de los extremos.

RTC *Consulte* Red telefónica conmutada (RTC).

nube pública Una solución de implementación en la nube proporcionada por un tercero que descarga los detalles a ese tercero, pero renuncia a cierto control y puede introducir problemas de seguridad.

cifrado de clave pública *Consulte* cifrado asimétrico.

red telefónica conmutada (RTC) También conocido como el Plain Old Telephone Service (POTS), la red de conmutación de circuitos que se ha utilizado para el servicio telefónico analógico durante años y ahora es principalmente una operación digital.

QoS *Vea* la calidad de servicio (QoS).

análisis cualitativo de riesgos Un método de análisis del riesgo mediante el cual se utilizan técnicas de intuición, experiencia y mejores prácticas para determinar el riesgo.

calidad de servicio (QoS) Una tecnología que administra los recursos de red para garantizar un nivel de servicio predefinido. Asigna prioridades de tráfico a los diferentes tipos de tráfico en una red.

análisis cuantitativo de riesgos Un método de análisis de riesgos que asigna valores monetarios y numéricos a todas las facetas del proceso de análisis de riesgos, incluido el valor de los activos, la frecuencia de las amenazas, la gravedad de la vulnerabilidad, el impacto, los costos de protección, etc.

lámpara de cuarzo Una lámpara que consiste en una fuente de luz ultravioleta, como el vapor de mercurio, contenida en una bombilla de sílice fundida que transmite luz ultravioleta con poca absorción.

RA *Ver* autoridad de registro (RA).

RAD *Ver* Desarrollo Rápido de Aplicaciones (RAD).

interferencia de radiofrecuencia (RFI) Interferencias de fuentes de radio en la zona.

RADIUS *Consulte* Servicio de usuario de acceso telefónico local (RADIUS).

RAID 0 También se denomina creación de bandas de disco, un método que escribe los datos en varias unidades, pero aunque mejora el rendimiento, no proporciona tolerancia a errores.

RAID 1 También denominado creación de reflejo de disco, un método que utiliza dos discos y escribe una copia de los datos en ambos discos, lo que proporciona tolerancia a errores en caso de un error de una sola unidad.

RAID 2 Un sistema en el que los datos se dividen en bandas en todas las unidades a nivel de bits y utiliza un código de hamming para la detección de errores. Los códigos de Hamming pueden detectar errores de hasta dos bits o corregir errores de un bit sin detectar errores no corregidos.

RAID 3 Un método que requiere al menos tres unidades. Los datos se escriben en todas las unidades, como la creación de bandas, y luego la información de paridad se escribe en una sola unidad dedicada; la información de paridad se utiliza para regenerar los datos en el caso de una falla de una sola unidad.

RAID 5 Un método que requiere al menos tres unidades. Los datos se escriben en todas las unidades, como la creación de bandas y, a continuación, la información de paridad también se distribuye en todas las unidades. La información de paridad se utiliza para regenerar los datos en el caso de un fallo de una sola unidad.

RAID 7 Aunque no es un estándar, sino una implementación propietaria, un sistema que incorpora los mismos principios que RAID 5, pero que permite que la matriz de unidades siga funcionando si falla cualquier disco o cualquier ruta de acceso a cualquier disco. Los múltiples discos del arreglo de discos funcionan como un solo disco virtual.

RAID 10 También se denomina creación de bandas de disco con duplicación, un método que requiere al menos cuatro unidades y es una combinación de RAID 0 y RAID 1. En primer lugar, se crea un volumen RAID 1 duplicando dos unidades juntas. A continuación, se crea un conjunto de bandas RAID 0 en cada par reflejado.

ataque de tabla arco iris Un ataque en el que se utilizan comparaciones con valores hash conocidos. Sin embargo, en un ataque de arco iris, se utiliza una tabla de arco iris que contiene los hashes criptográficos de las contraseñas.

ransomware Malware que impide o limita el acceso de los usuarios a su sistema o dispositivo. Por lo general, obliga a las víctimas a pagar el rescate por la devolución del acceso al sistema.

Desarrollo rápido de aplicaciones (RAD) Un modelo de desarrollo en el que se dedica menos tiempo al diseño, mientras que se hace hincapié en la producción rápida de prototipos, con la suposición de que el conocimiento crucial sólo se puede obtener a través de ensayo y error.

RBAC *Consulte* Control de acceso basado en roles (RBAC).

RC4 Cifrado de secuencias que utiliza un tamaño de clave variable de 40 a 2.048 bits y hasta 256 rondas de transformación.

RC5 Cifrado por bloques que utiliza un tamaño de clave de hasta 2.048 bits y hasta 255 rondas de transformación. Los tamaños de bloque admitidos son de 32, 64 o 128 bits.

RC6 Un cifrado de bloques basado en RC5 que utiliza el mismo tamaño de clave, redondeos y tamaño de bloque.

RC7 Un cifrado de bloques basado en RC6 que utiliza el mismo tamaño de clave y redondea pero tiene un tamaño de bloque de 256 bits. Además, utiliza seis registros de trabajo en lugar de cuatro. Como resultado, es mucho más rápido que RC6.

prueba de lectura a través Una prueba en la que participan los equipos que forman parte de cualquier plan de recuperación. Estos equipos leen el plan que se ha desarrollado e intentan identificar cualquier inexactitud u omisión en el plan.

monitoreo de usuario real (RUM) Un tipo de monitorización pasiva que captura y analiza cada transacción de cada usuario de aplicación o sitio web.

acuerdo recíproco Un acuerdo entre dos organizaciones que tienen necesidades tecnológicas e infraestructuras similares.

registro Colección de elementos de datos relacionados.

control de recuperación Control de seguridad que recupera un sistema o dispositivo después de que se haya producido un ataque.

objetivo de punto de recuperación El punto en el tiempo al que se debe devolver el recurso o la función interrumpidos.

objetivo de tiempo de recuperación El período de tiempo más corto después de un desastre o evento disruptivo dentro del cual se debe restaurar un recurso o función para evitar consecuencias inaceptables.

Libro Rojo Colección de criterios basados en el modelo bell-lapadula que aborda la seguridad de la red.

redundancia Hace referencia a proporcionar varias instancias de un componente físico o lógico de forma que un segundo componente esté disponible si se produce un error en el primero.

sitio redundante Un sitio que está configurado de forma idéntica al sitio primario.

monitor de referencia Componente del sistema que aplica controles de acceso en un objeto.

integridad referencial Una característica que requiere que para cualquier atributo de clave externa, la relación a la que se hace referencia debe tener una tupla con el mismo valor para su clave principal.

autoridad de registro La entidad en una PKI que comprueba la identidad del solicitante y registra al solicitante.

investigación regulatoria Una investigación que ocurre cuando un organismo regulador investiga a una organización por una infracción regulatoria.

derecho reglamentario *Véase* el derecho administrativo.

política de seguridad reglamentaria Una política de seguridad que aborda las regulaciones específicas de la industria, incluidas las normas obligatorias.

relación Una entidad fundamental en una base de datos relacional en forma de tabla.

base de datos relacional Base de datos que utiliza atributos (columnas) y tuplas (filas) para organizar los datos en tablas bidimensionales.

fiabilidad La capacidad de una función o sistema para funcionar consistentemente de acuerdo con las especificaciones.

ley religiosa Un tipo de ley basada en creencias religiosas.

remanencia Cualquier dato que quede después de que los medios de comunicación hayan sido borrados.

acceso remoto Permite a los usuarios tener acceso a los recursos de una organización desde una conexión remota. Estas conexiones remotas pueden ser conexiones de acceso telefónico directo, pero más comúnmente utilizan Internet como la red a través de la cual se transmiten los datos.

Servicio de usuario de acceso telefónico de acceso remoto (RADIUS) Un estándar de autenticación remota definido en RFC 2138. RADIUS se diseña para proporcionar un marco que incluya tres componentes: supplicant, authenticator, y servidor de autenticación.

riesgo residual Riesgo que queda después de que se hayan implementado las salvaguardias.

aprovisionamiento de recursos El proceso en las operaciones de seguridad que garantiza que la organización implementa sólo los activos que necesita actualmente.

ARP inverso (RARP) Resuelve las direcciones MAC en direcciones IP.

revocación Proceso mediante el cual se revoca o finaliza un certificado, una cuenta de acceso, una cuenta de grupo o un rol.

RFI *Véase* interferencia de radiofrecuencia (RFI).

Algoritmo de Rijndael Algoritmo que utiliza tres tamaños de bloque de 128, 192 y 256 bits. Una clave de 128 bits con un tamaño de bloque de 128 bits se somete a 10 rondas de transformación. Una clave de 192 bits con un tamaño de bloque de 192 bits se somete a 12 rondas de transformación. Por último, una clave de 256 bits con un tamaño de bloque de 256 bits se somete a 14 rondas de transformación.

anillo Topología física en la que los dispositivos se encadenan en margarita entre sí en un círculo o anillo.

RIP *Consulte* Protocolo de información de enrutamiento (RIP).

RIPEMD-160 Algoritmo de síntesis de mensaje que genera un valor hash de 160 bits después de realizar 160 rondas de cálculos en bloques de 512 bits.

riesgo La probabilidad de que un agente de amenaza aproveche una vulnerabilidad y el impacto de la probabilidad.

aceptación del riesgo Un método de manejo del riesgo que implica comprender y aceptar el nivel de riesgo, así como el costo de los daños que pueden ocurrir.

evitación de riesgos Un método de manejo del riesgo que implica terminar la actividad que provoca un riesgo o elegir una alternativa que no sea tan arriesgada.

gestión de riesgos El proceso que se produce cuando las organizaciones identifican, miden y controlan los riesgos de la organización.

mitigación de riesgos Un método de manejo del riesgo que implica definir el nivel de riesgo aceptable que la organización puede tolerar y reducir el riesgo a ese nivel.

transferencia de riesgos Un método de manejo del riesgo que implica pasar el riesgo a un tercero.

control de acceso basado en roles (RBAC) Un modelo de control de acceso en el que cada sujeto se asigna a uno o más roles.

análisis de causa de origen Un tipo de investigación que se completa para determinar la causa raíz para que se puedan tomar medidas para evitar este incidente en el futuro.

enrutador Un dispositivo que utiliza una tabla de ruteo para determinar qué dirección enviar el tráfico destinado a una red determinada.

Protocolo de información de enrutamiento (RIP) Un protocolo de vector de distancia basado en estándares que tiene dos versiones, RIPv1 y RIPv2. Ambos utilizan el recuento de saltos como una métrica.

fila Una fila de una tabla.

RPO *Consulte* objetivo de punto de recuperación.

RTO *Consulte el* objetivo de tiempo de recuperación.

control de acceso basado en reglas Un modelo de control de acceso en el que una directiva de seguridad se basa en reglas globales impuestas para todos los usuarios.

RUM *Ver* monitoreo de usuarios reales (RUM).

ejecutar cifrado de claves Cifrado que utiliza un componente físico, normalmente un libro, para proporcionar los caracteres polialfabéticos.

SaaS *Ver* software como servicio (SaaS).

salvaguardia *Véase* la contramedida.

salazón Agregar datos aleatoriamente a una función unidireccional que "aplica un algoritmo hash" a una contraseña o frase de contraseña para defenderse de los ataques de diccionario frente a una lista de hashes de contraseña y contra los ataques de tabla de arco iris precalculados.

SAML *Consulte* Lenguaje de marcado de aserción de seguridad (SAML).

SAN *Consulte* red de área de almacenamiento (SAN).

espacio aislado Una técnica de virtualización de software que permite que las aplicaciones y los procesos se ejecuten en un entorno virtual aislado.

Ley Sarbanes-Oxley (SOX) Una ley estadounidense que controla los métodos de contabilidad y la presentación de informes financieros para las organizaciones y estipula sanciones e incluso penas de cárcel para los funcionarios ejecutivos y afecta a cualquier organización que cotiza en bolsa en los Estados Unidos.

esquema Descripción de una base de datos relacional.

host con pantalla Un firewall que se encuentra entre el enrutador final y la red interna.

subred filtrada Dos firewalls utilizados para inspeccionar el tráfico antes de que pueda entrar en la red interna.

SDN *Consulte* redes definidas por software (SDN).

buscar El acto de perseguir elementos o información.

evidencia secundaria Evidencia que ha sido reproducida de un original o sustituida por un artículo original.

memoria secundaria Medios magnéticos, ópticos o basados en flash u otros dispositivos de almacenamiento que contienen datos que el sistema operativo debe leer primero y almacenar en la memoria.

cifrado de clave secreta *Consulte* cifrado simétrico.

Sistema europeo seguro para aplicaciones en un entorno de múltiples proveedores (SESAME) Un proyecto que amplió la funcionalidad de Kerberos para corregir los puntos débiles de Kerberos. Utiliza criptografía simétrica y asimétrica para proteger los datos intercambiados y un servidor de autenticación de confianza en cada host.

Protocolo seguro de transferencia de archivos (SFTP) Una extensión del SSH que utiliza el puerto TCP 22.

HTTP seguro (S-HTTP) Un protocolo que cifra solo los datos de la página servidos y los datos enviados como los campos POST, dejando el inicio del protocolo sin cambios.

Lenguaje de marcado de aserción de seguridad (SAML) Un formato de datos estándar abierto basado en XML para intercambiar datos de autenticación y autorización entre partes, en particular, entre un proveedor de identidades y un proveedor de servicios.

dominio de seguridad Conjunto de recursos que siguen las mismas directivas de seguridad y están disponibles para un sujeto.

kernel de seguridad Los elementos de hardware, firmware y software de una base informática de confianza que implementa el concepto de monitor de referencia.

sensibilidad *Consulte* sensibilidad de datos.

separación de funciones Una medida de seguridad que implica dividir las operaciones confidenciales entre varios usuarios para que ningún usuario tenga los derechos y el acceso para llevar a cabo la operación por sí solo. Garantiza que una persona no sea capaz de poner en peligro la seguridad de la organización y evita el fraude mediante la distribución de tareas y sus derechos y privilegios asociados entre más de un usuario.

Protocolo de interfaz de línea serie (SLIP) Un protocolo de acceso remoto más antiguo que ppp había dejado obsoleto.

acuerdo de nivel de servicio (SLA) Un acuerdo entre una organización y un proveedor de servicios (ya sea interno o externo) sobre la capacidad del sistema de soporte para responder a los problemas dentro de un plazo determinado mientras proporciona un nivel de servicio acordado.

arquitectura orientada a servicios (SOA) Un enfoque que proporciona funcionalidad de comunicación basada en web sin necesidad de escribir código redundante por aplicación. Utiliza interfaces y componentes estandarizados denominados service brokers para facilitar la comunicación entre aplicaciones basadas en web.

identificador de conjunto de servicios (SSID) Un nombre o un valor asignado para identificar la red inalámbrica (WLAN) de otras redes inalámbricas (WLAN).

SESAME *Véase* Sistema Europeo Seguro para Aplicaciones en un Entorno multiproveprovista (SESAME).

ataque de secuestro de sesión Un ataque en el que un hacker intenta situarse en medio de una conversación activa entre dos ordenadores con el fin de apoderarse de la sesión de uno de los dos ordenadores, recibiendo así todos los datos enviados a ese ordenador.

Capa de sesión (capa 5) La capa de modelo de referencia OSI responsable de agregar información al paquete que hace posible una sesión de comunicación entre un servicio o aplicación en el dispositivo de origen con el mismo servicio o aplicación en el dispositivo de destino.

SFTP *Consulte* Protocolo seguro de transferencia de archivos (SFTP).

surf de hombro Un ataque de ingeniería social que se produce cuando un atacante observa cuando un usuario escribe el inicio de sesión u otros datos confidenciales.

S-HTTP *Vea* HTTP seguro (S-HTTP).

Sistema de señalización 7 (SS7) Un protocolo que configura, controla la señalización y derriba una llamada telefónica RTC.

Protocolo simple de transferencia de correo (SMTP) Un protocolo de capa de aplicación estándar utilizado entre servidores de correo electrónico. Este es también el protocolo utilizado por los clientes para enviar correo electrónico.

Protocolo simple de administración de redes (SNMP) Protocolo de capa de aplicación que se utiliza para recuperar información de dispositivos de red y para enviar cambios de configuración a esos dispositivos.

prueba de simulación Prueba que las operaciones y el personal de soporte técnico ejecutan en un escenario de juego de roles. Esta prueba identifica los pasos y amenazas omitidos.

autenticación de un solo factor Un tipo de autenticación que incluye solo un tipo de factor de autenticación. Agregar más tipos de factores aumenta la seguridad de la autenticación.

modo único Fibra óptica que utiliza un solo haz de luz proporcionado por un láser como fuente de luz.

inicio de sesión único (SSO) Un sistema en el que un usuario escribe las credenciales de inicio de sesión una vez y, a continuación, puede acceder a todos los recursos de la red.

SIP *Consulte* Protocolo de inicio de sesión (SIP).

Listado Un algoritmo simétrico de cifrado de bloques desarrollado por la NSA de EE. UU. que utiliza una clave de 80 bits para cifrar bloques de 64 bits. Se utiliza en el chip Clipper.

SLA *Consulte* el acuerdo de nivel de servicio (SLA)

análisis de espacio flojo Análisis del espacio de holgura (marcado como vacío o reutilizable) en una unidad para ver si se puede recuperar algún dato antiguo (marcado para eliminación).

SLIP *Consulte* Serial Line Interface Protocol (SLIP).

SMDS *Consulte* Servicio de datos multimedibitos conmutado (SMDS).

sensor activado por humo Un sensor que funciona utilizando un dispositivo fotoeléctrico para detectar variaciones en la luz causadas por partículas de humo.

SMTP *Consulte* Protocolo simple de transferencia de correo (SMTP).

ataque pitufo Un ataque en el que un atacante envía una gran cantidad de tráfico de eco UDP a una dirección de difusión IP, todo ello con una dirección de origen falsa, que será, por supuesto, el sistema de destino.

SNMP *Consulte* Protocolo simple de administración de redes (SNMP).

SOA *Consulte* arquitectura orientada a servicios (SOA).

Cortafuegos SOCKS Un ejemplo de un firewall a nivel de circuito.

vapor de sodio Un sistema de iluminación que utiliza sodio en un estado excitado para producir luz.

software como servicio (SaaS) Un servicio de computación en la nube que implica que el proveedor proporcione la solución completa. Podrían proporcionarle un sistema de correo electrónico, por ejemplo, mediante el cual alojan y administran todo por usted.

redes definidas por software (SDN) Una tecnología que acelera la implementación y entrega de software, lo que reduce los costos de TI a través de la automatización del flujo de trabajo habilitada por políticas. Permite arquitecturas en la nube al ofrecer una entrega de aplicaciones automatizada y bajo demanda y movilidad a escala.

Ciclo de vida del desarrollo de software Un marco predecible de procedimientos diseñados para identificar todos los requisitos con respecto a la funcionalidad, el costo, la confiabilidad y el cronograma de entrega y garantizar que todos estos requisitos se cumplan en la solución final.

piratería de software La reproducción o distribución no autorizada de software con derechos de autor.

SONET *Vea el* establecimiento de una red óptico síncrono (SONET).

código fuente Una colección de instrucciones informáticas escritas con algún lenguaje informático legible por humanos.

Ley SOX *Ver* Ley Sarbanes-Oxley (SOX).

ataque de sniffer Un ataque en el que se utiliza un rastreador para capturar una contraseña sin cifrar o de texto no cifrado.

correo no deseado Envío de correo electrónico que no se solicita de forma masiva.

spear phishing Un ataque de phishing llevado a cabo contra un objetivo específico aprendiendo sobre los hábitos y gustos del objetivo. El proceso de imponer un ataque de phishing a una persona específica en lugar de un conjunto aleatorio de personas.

Espiral Un modelo de desarrollo que es un enfoque iterativo pero pone más énfasis en el análisis de riesgos en cada etapa.

software espía Malware que rastrea las actividades y también puede recopilar información personal que podría conducir al robo de identidad.

SSID *Consulte* el identificador del conjunto de servicios (SSID).

SSO *Consulte* inicio de sesión único (SSO).

estándar Componente de gobierno de seguridad de la información que describe cómo se implementarán las directivas dentro de una organización.

vidrio estándar Vidrio que se utiliza en zonas residenciales y se rompe fácilmente.

iluminación en espera Un tipo de sistema que ilumina sólo en ciertos momentos o en un horario.

topología en estrella La topología física más común en uso hoy en día, en la que todos los dispositivos están conectados a un dispositivo central (ya sea un concentrador o un conmutador).

modelos de máquina de estado Un modelo que examina todos los estados posibles en los que podría estar un sistema y garantiza que el sistema mantiene la relación de seguridad adecuada entre objetos y sujetos en cada estado para determinar si el sistema es seguro.

firewalls con estado Un firewall que es consciente del correcto funcionamiento del protocolo de enlace TCP, realiza un seguimiento del estado de todas las conexiones con respecto a este proceso y puede reconocer cuando los paquetes están intentando entrar en la red que no tienen sentido en el contexto del protocolo de enlace TCP.

NAT con estado (SNAT) Implementa dos o más dispositivos NAT para trabajar juntos como un grupo de traducción. Un miembro proporciona la traducción de red de la información de la dirección IP. El otro miembro utiliza esa información para crear entradas de tabla de traducción duplicadas. Mantiene una tabla sobre las sesiones de comunicación entre sistemas internos y externos.

NAT estática Asigna una dirección IP privada interna a una dirección IP pública externa específica. Se trata de una asignación uno a uno.

pruebas estáticas Analiza la seguridad del software sin ejecutar realmente el software. Esto normalmente se proporciona mediante la revisión del código fuente o la aplicación compilada.

virus de sigilo Un virus que oculta las modificaciones que está realizando en el sistema para ayudar a evitar la detección.

esteganografía El proceso de ocultar un mensaje dentro de otro objeto, como una imagen o un documento.

análisis de esteganografía Análisis de los archivos en una unidad para ver si los archivos han sido alterados o para descubrir el cifrado utilizado en los archivos.

red de área de almacenamiento (SAN) Una red que comprende dispositivos de almacenamiento de alta capacidad conectados por una red privada de alta velocidad (separada de la LAN) mediante conmutadores específicos de almacenamiento.

cifrado basado en secuencias Un cifrado que realiza el cifrado poco a poco y utiliza generadores de secuencias de claves.

prueba de recorrido estructurado Una prueba que involucra a representantes de cada departamento o área funcional revisando a fondo la precisión del BCP.

tema El usuario o proceso que solicita acceso.

sustitución El proceso de intercambiar un byte de un mensaje por otro.

cifrado de sustitución Cifrado que utiliza una clave para sustituir caracteres o bloques de caracteres por caracteres o bloques de caracteres diferentes.

superescalar Una arquitectura de equipo caracterizada por un procesador que permite la ejecución simultánea de varias instrucciones en la misma fase de canalización.

modo supervisor Modo utilizado cuando un sistema informático procesa instrucciones de entrada/salida.

suplicante El componente en un entorno RADIUS que busca la autenticación.

aumento de la tensión Un alto voltaje prolongado.

vigilancia El acto de monitorear el comportamiento, las actividades u otra información cambiante, generalmente de las personas.

Servicio de datos multimedibito conmutado (SMDS) Una tecnología de conmutación de paquetes sin conexión que se comunica a través de una red pública establecida.

conmutadores Un dispositivo inteligente que actúa en la capa 2 del modelo OSI y toma decisiones de conmutación basadas en direcciones MAC, que residen en la capa 2.

cifrado simétrico Un método de cifrado mediante el cual una sola clave privada cifra y descifra los datos. También se conoce como cifrado de clave privada o secreta.

modo simétrico Un modo en el que los procesadores o núcleos se entregan el trabajo por turnos, subproceso por hilo.

Ataque SYN ACK Un ataque en el que un hacker envía un gran número de paquetes con el indicador SYN establecido, lo que hace que el equipo receptor reserve memoria para cada paquete ACK que espera recibir a cambio. Estos paquetes nunca llegan y en algún momento los recursos de la computadora receptora se agotan, lo que hace que esto sea una forma de ataque DoS.

cifrado sincrónico Una forma de cifrado en la que el cifrado o descifrado se produce inmediatamente.

Redes ópticas síncronas (SONET) Una tecnología que utiliza enlaces basados en fibra que operan sobre líneas medidas en velocidades de transmisión de portadora óptica (OC).

transmisión síncrona Tipo de transmisión que utiliza un mecanismo de temporización para sincronizar el emisor y el receptor.

supervisión de transacciones sintéticas Un tipo de monitoreo proactivo a menudo preferido para sitios web y aplicaciones. Proporciona información sobre la disponibilidad y el rendimiento de una aplicación y advierte de cualquier problema potencial antes de que los usuarios experimenten cualquier degradación en el comportamiento de la aplicación.

Ciclo de vida del desarrollo del sistema Un proceso que proporciona pasos claros y lógicos que deben seguirse para garantizar que el sistema que surge al final del proceso de desarrollo proporciona la funcionalidad deseada, con un nivel aceptable de seguridad.

propietario del sistema La persona que posee un sistema y puede necesitar trabajar con los propietarios de datos y los custodios de datos para asegurarse de que los datos del sistema se administran correctamente.

resistencia del sistema La capacidad de un sistema, dispositivo o centro de datos para recuperarse rápidamente y continuar funcionando después de una falla del equipo, corte de energía u otra interrupción.

directiva de seguridad específica del sistema Una directiva de seguridad que aborda la seguridad de un equipo, red, tecnología o aplicación específicos.

amenazas del sistema Amenazas que no provienen de las fuerzas de la naturaleza sino de fallas en los sistemas que proporcionan servicios básicos como la electricidad y los servicios públicos.

TACACS+ *Vea* el sistema de control de acceso del controlador de acceso de terminal más (TACACS+).

planes tácticos (u objetivos) Planes que alcanzan los objetivos del plan estratégico y tienen una duración más corta (de 6 a 18 meses).

activos tangibles Cualquier activo que pueda tocar físicamente, incluidos equipos, instalaciones, suministros y personal.

prueba de destino Una prueba en la que tanto el equipo de pruebas como el equipo de seguridad de la organización reciben la máxima información sobre la red y el tipo de prueba que se producirá. Esta es la prueba más fácil de completar, pero no proporciona una imagen completa de la seguridad de la organización.

T-portador Una línea dedicada a la que el suscriptor tiene acceso privado y no comparte con otro cliente.

TCB *Consulte* Base de equipos de confianza (TCB).

Protocolo de enlace de tres vías TCP Proceso que implica la creación de un estado de conexión entre los dos hosts antes de que se transfieran los datos.

TCP/IP Un modelo de cuatro capas que se centra en TCP/IP.

TCSEC *Consulte* Criterios de evaluación de sistemas informáticos de confianza (TCSEC).

TDM *Vea* la multiplexación por división de tiempo (TDM).

lágrima Proceso en el que un hacker envía fragmentos mal formados de paquetes que, al volver a montar por el receptor, hacen que el receptor se bloquee o se vuelva inestable.

desastres tecnológicos Desastres que se producen cuando se produce un error en un dispositivo.

Telnet Protocolo de acceso remoto no seguro que se usa para conectarse a un dispositivo con el fin de ejecutar comandos en el dispositivo.

vidrio templado Vidrio que se calienta para darle fuerza extra.

Terminal Access Controller Access-Control System Plus (TACACS+) Un servicio de autenticación propietario de Cisco que actúa en dispositivos Cisco, proporcionando una solución de autenticación centralizada.

sitio terciario Un sitio de copia de seguridad secundario que proporciona una alternativa en caso de que el sitio caliente, el sitio caliente o el sitio frío no estén disponibles.

análisis de cobertura de prueba Utiliza casos de prueba que se escriben con respecto a las especificaciones de requisitos de la aplicación.

Thicknet Un tipo de coaxial, también llamado 10Base5, que funciona a 10 Mbps y es capaz de correr 500 metros.

Thinnet Un tipo de coaxial, también llamado 10Base2, que opera a 10 Mbps y es capaz de correr 185 pies.

subproceso Un trabajo individual realizado para un proceso específico.

amenaza Condición que se produce cuando se identifica o se aprovecha una vulnerabilidad.

agente de amenazas La entidad que lleva a cabo una amenaza.

firewall de tres patas Un firewall que utiliza tres interfaces: una conectada a la red que no es de confianza, otra a la red interna y otra a una parte de la red denominada DMZ.

tigre Una función hash que genera valores hash de 128, 160 o 192 bits después de realizar 24 rondas de cálculos en bloques de 512 bits.

Multiplexación por división de tiempo (TDM) Multiplexación en la que las transmisiones se turnan en lugar de enviar al mismo tiempo.

ataque de tiempo de comprobación/tiempo de uso Un ataque que intenta aprovechar la secuencia de eventos que tienen lugar a medida que el sistema completa tareas comunes.

TLS/SSL *Consulte* Seguridad de la capa de transporte/Capa de sockets seguros (TLS/SSL).

TOGAF El marco de arquitectura de grupo abierto; tiene sus orígenes en el Departamento de Defensa de los Estados Unidos y requiere un Método de Desarrollo Arquitectónico (ADM) que emplea un proceso iterativo que requiere que los requisitos individuales se supervisen y actualicen continuamente según sea necesario.

paso de tokens Se llama a un método de contención utilizado tanto en FDDI como en Token Ring. En este proceso, un paquete especial llamado token se pasa alrededor de la red. Una estación no puede enviar hasta que el token llegue y esté vacío.

Token Ring Un protocolo propietario de capa 2 que gozó de un pequeño éxito y ya no es ampliamente utilizado.

detección de topología Implica determinar los dispositivos de la red, sus relaciones de conectividad entre sí y el esquema de direccionamiento IP interno en uso.

ley de agravio *Ver* ley civil/agravio.

riesgo total El riesgo que podría correr una organización si decide no implementar ninguna salvaguarda.

TPM *Consulte* Módulo de plataforma segura (TPM).

secreto comercial Un tipo de propiedad intelectual que garantiza que la información técnica o comercial de propiedad permanezca confidencial. Los secretos comerciales incluyen recetas, fórmulas, listados de ingredientes, etc., que deben protegerse contra la divulgación.

marca registrada Tipo de propiedad intelectual que garantiza que el símbolo, el sonido o la expresión que identifica un producto o una organización están protegidos contra el uso de otra organización.

copia de seguridad del registro de transacciones Una copia de seguridad que captura todas las transacciones que se han producido desde la última copia de seguridad.

Capa de transporte (capa 4) La capa de modelo de referencia OSI que recibe toda la información de las capas 7, 6 y 5 y agrega información que identifica el protocolo de transporte en uso y el número de puerto específico que identifica el protocolo de capa 7 requerido.

Seguridad de la capa de transporte/Capa de sockets seguros (TLS/SSL) Protocolo para crear conexiones seguras a servidores. Funciona en la capa de aplicación del modelo OSI y se utiliza principalmente para proteger el tráfico HTTP o servidores web.

transposición El proceso de barajar o reordenar el texto no cifrado para ocultar el mensaje original. También se conoce como permutación.

cifrado de transposición Cifrado que codifica las letras del mensaje original en un orden diferente.

trampilla *Ver* puerta trasera.

trampilla (cifrado) Mecanismo secreto que permite la implementación de la función inversa en una función unidireccional.

Triple DES (3DES) Una versión de DES que aumenta la seguridad mediante el uso de tres claves de 56 bits.

Caballo de Troya Un programa o aplicación maliciosa que parece o se pretende hacer una cosa, pero hace otra cuando se ejecuta.

Base de equipos de confianza (TCB) Los componentes (hardware, firmware o software) en los que se confía para aplicar la directiva de seguridad de un sistema que, si se ve comprometido, pone en peligro las propiedades de seguridad de todo el sistema.

Criterios de evaluación de sistemas informáticos de confianza (TCSEC) Un modelo de evaluación de la seguridad del sistema desarrollado por el Centro Nacional de Seguridad Informática (NCSC) para que el Departamento de Defensa de los Estados Unidos evalúe los productos.

ruta de acceso de confianza Un canal de comunicación entre el usuario o el programa a través del cual está trabajando y la base de equipos de confianza.

Módulo de plataforma segura (TPM) Un chip de seguridad instalado en una placa base de equipo que es responsable de administrar claves simétricas y asimétricas, hashes y certificados digitales.

recuperación de confianza La respuesta de un sistema a un error (como un bloqueo o inmovilización) que deja el sistema en un estado seguro.

modelo de identidad federada de terceros de confianza Un modelo de identidad federada en el que cada organización se suscribe a los estándares de un tercero.

cerradura del vaso Una cerradura con más partes móviles que una cerradura con carcasa, en la que una llave eleva una pieza de metal a la altura correcta.

par trenzado El tipo más común de cableado de red hoy en día. Se llama así porque dentro del cable hay cuatro pares de cables más pequeños que se trenzan o se tuercen.

control de dos personas También conocida como una regla de dos hombres, esto ocurre cuando ciertos accesos y acciones requieren la presencia de dos personas autorizadas en todo momento.

Dos peces Una versión de Blowfish que utiliza bloques de datos de 128 bits con claves de 128, 192 y 256 bits y realiza 16 rondas de transformación.

unidifusión Una transmisión de un solo sistema a otro sistema único. Se considera uno a uno.

fuente de alimentación ininterrumpida (UPS) Un dispositivo que va entre la toma de corriente y un dispositivo electrónico y utiliza una batería para proporcionar energía si se pierde la fuente de la pared.

Directrices federales de sentencias de los Estados Unidos de 1991 Un acto estadounidense que afecta a individuos y organizaciones condenadas por delitos graves y delitos menores graves (Clase A).

Uniendo y fortaleciendo a Estados Unidos proporcionando las herramientas apropiadas necesarias para interceptar y obstruir el terrorismo (USA PATRIOT) Act de 2001 Una ley estadounidense que afecta a las agencias de inteligencia y aplicación de la ley en los Estados Unidos. Su propósito es mejorar las herramientas de investigación que las fuerzas del orden pueden utilizar, incluidas las comunicaciones por correo electrónico, los registros telefónicos, las comunicaciones por Internet, los registros médicos y los registros financieros.

UPS *Consulte* fuente de alimentación ininterrumpida (UPS).

Ocultación de URL Un ataque que aprovecha la capacidad de incrustar URL en páginas web y correo electrónico.

USA PATRIOT Act *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001.

VDSL *consulte* DSL de velocidad de bits muy alta (VDSL).

verificación El proceso mediante el cual una aplicación comprueba que un certificado es válido.

DSL de velocidad de bits muy alta (VDSL) Una forma de DSL capaz de soportar HDTV y VoIP.

idiomas de muy alto nivel Una cuarta generación de lenguajes que se centra en algoritmos abstractos que ocultan parte de la complejidad al programador. Esto libera al programador para centrarse en los problemas del mundo real que está tratando de resolver en lugar de los detalles que pasan detrás de las escenas.

ver La representación del sistema desde la perspectiva de una parte interesada o un conjunto de partes interesadas. La seguridad se aplica mediante el uso de vistas, que es el conjunto de datos disponibles para un usuario determinado.

firewall virtual Software que se ha escrito específicamente para proporcionar un firewall de seguridad en el entorno virtual.

LAN virtual (VLAN) Una subdivisión lógica de un switch que segrega los puertos entre sí como si estuvieran en diferentes LAN. Las VLAN también pueden abarcar varios conmutadores, lo que significa que los dispositivos conectados a conmutadores en diferentes partes de una red se pueden colocar en la misma VLAN independientemente de la ubicación física.

red privada virtual (VPN) Una red que utiliza una red de operador que no es de confianza pero proporciona protección de la información a través de protocolos de autenticación seguros y mecanismos de cifrado.

Protocolo de redundancia de enrutador virtual (VRRP) Un protocolo que se utiliza para proporcionar los gatewayes múltiples a los clientes para la tolerancia a errores en el caso de un router que va abajo.

red de área de almacenamiento virtual (VSAN) Un método de almacenamiento definido por software que permite la agrupación de capacidades de almacenamiento y el aprovisionamiento instantáneo y automático de almacenamiento de máquinas virtuales.

virus Un programa autorreplicante que infecta el software. Utiliza una aplicación host para reproducir y entregar su carga y normalmente se adjunta a un archivo.

vishing Un tipo de phishing que utiliza un sistema telefónico o tecnologías VoIP. El usuario recibe inicialmente una llamada, un mensaje de texto o un correo electrónico que le dice que llame a un número específico y proporcione información personal como nombre, fecha de nacimiento, número de Seguro Social e información de tarjeta de crédito.

VLAN *Consulte* la LAN virtual (VLAN).

Voz sobre IP (VoIP) Una tecnología que implica encapsular la voz en paquetes y enviarlos a través de redes de conmutación de paquetes.

VoIP *Consulte* Voz sobre IP (VoIP).

memoria volátil Memoria que se vacía cuando el dispositivo se apaga.

VPN *Consulte* red privada virtual (VPN).

Raspador de pantalla VPN Una aplicación que permite a un atacante capturar lo que está en la pantalla del usuario.

VRRP *Vea el* Virtual Router Redundancy Protocol (VRRP).

VSAN *Consulte* red de área de almacenamiento virtual (VSAN).

En forma de V Un modelo de desarrollo que difiere del método Waterfall principalmente en que la comprobación y la validación se realizan en cada paso.

vulnerabilidad Una ausencia o una debilidad de una contramedida que está en su lugar.

evaluación de vulnerabilidad Un método de evaluación mediante el cual se prueba la red de una organización para detectar ausencias de contramedidas u otras debilidades de seguridad.

WAN *Consulte* red de área extensa (WAN).

tiza de guerra Una práctica que se utiliza típicamente para acompañar la conducción de guerra. Después de que el conductor de guerra haya localizado una WLAN, indica en tiza en la acera el SSID y los tipos de seguridad utilizados en la red.

conducción de guerra Conduciendo y localizando WLAN con una computadora portátil y una antena de alta potencia.

cerradura warded Una cerradura con un perno de resorte que tiene una muesca en ella. La cerradura tiene salas, o proyecciones de metal, dentro de la cerradura con la que coincide la llave para permitir la apertura de la cerradura.

sitio cálido Una instalación arrendada que contiene cableado eléctrico y de comunicaciones, servicios públicos completos y equipos de red.

WASC *Vea* Web Application Security Consortium (WASC).

Cascada Un modelo de desarrollo que divide el proceso en distintas fases. Aunque es un enfoque algo rígido, ve el proceso como una serie secuencial de pasos que se siguen sin volver a pasos anteriores. Este enfoque se denomina desarrollo incremental.

detector de movimiento de onda Dispositivo que genera un patrón de onda en el área y detecta cualquier movimiento que perturbe el patrón de onda aceptado. Cuando se altera el patrón, suena una alarma.

Consorcio de seguridad de aplicaciones web (WASC) Una organización que proporciona procedimientos recomendados para aplicaciones basadas en web junto con una variedad de recursos, herramientas e información que las organizaciones pueden utilizar en el desarrollo de aplicaciones web.

WEP *Vea* La aislamiento equivalente alambrada (WEP).

extintor de tubería húmeda Un extintor que utiliza agua contenida en tuberías para extinguir el fuego. En algunas áreas, el agua podría congelarse y reventar las tuberías causando daños. Este sistema no se recomienda para las habitaciones donde el equipo sería dañado por el agua.

caza de ballenas Una práctica que implica dirigirse a una sola persona que es alguien de importancia o importancia, como un CEO, CFO, CSO, COO o CTO.

pruebas de caja blanca El equipo de pruebas entra en el proceso de pruebas con un profundo conocimiento de la aplicación o el sistema. Con este conocimiento, el equipo crea casos de prueba para ejercitar cada ruta de acceso, campo de entrada y rutina de procesamiento. Este término se utiliza para referirse a las pruebas de seguridad de red, así como a las pruebas de aplicación.

listas blancas Configurar direcciones de correo electrónico aceptables, direcciones de Internet, sitios web, aplicaciones o algunos otros identificadores como buenos remitentes o según lo permitido.

red de área extensa (WAN) Una red utilizada para conectar LAN entre sí (incluidas las MAN).

Acceso protegido Wi-Fi (WPA) Una medida de seguridad creada para abordar la preocupación generalizada por la insuficiencia de WEP.

Privacidad equivalente por cable (WEP) La primera medida de seguridad utilizada con 802.11. Se especificó como el algoritmo en la especificación original. Puede ser utilizado para autenticar un dispositivo y para cifrar la información entre el AP y el dispositivo. Sin embargo, WEP se considera inseguro hoy en día, y se recomienda el uso de WPA2.

red de área local inalámbrica (WLAN) Permite que los dispositivos se conecten de forma inalámbrica entre sí a través de un punto de acceso inalámbrico (WAP). Los WAP múltiples pueden trabajar juntos para ampliar el rango de la red inalámbrica (WLAN).

factor de trabajo (cifrado) La cantidad de tiempo y recursos necesarios para interrumpir el cifrado.

gusano Un tipo de malware que se puede propagar sin ayuda del usuario.

WPA *Consulte* Acceso protegido Wi-Fi (WPA).

WPA2 Una mejora sobre el WPA que utiliza el CCMP, basado en el Advanced Encryption Standard (AES) bastante que el TKIP.

X.25 Un protocolo algo parecido a Frame Relay en que el tráfico se mueve a través de una red de conmutación de paquetes. Utiliza mecanismos de confiabilidad que ya no son necesarios en las líneas telefónicas actuales y que crean sobrecarga.

XML *Vea* Lenguaje de marcado extensible (XML).

Marco Zachman Un marco de arquitectura empresarial que utiliza un sistema de clasificación bidimensional basado en seis preguntas de comunicación (Qué, Dónde, Cuándo, Por qué, Quién y Cómo) que se cruzan con diferentes perspectivas (Ejecutivo, Administración de empresas, Arquitecto, Ingeniero, Técnico y Empresa).

prueba de conocimiento cero Una prueba en la que se proporciona al equipo de pruebas sin conocimientos sobre la red de la organización. El equipo de pruebas puede utilizar cualquier medio disponible para obtener información sobre la red de la organización. Esto también se conoce como prueba de caja cerrada o negra.