

GLOSARIO

Acción de recuperación

Ejecución de una respuesta o tarea de acuerdo con un procedimiento escrito.

Activación

Acción de poner en operación un equipo de recuperación, sitio alternativo o servicio, procedimiento o contrato.

Acuerdo recíproco

Acuerdos de procesamiento de emergencia entre dos o más organizaciones que tienen equipo o aplicaciones similares. Por lo general, quienes los celebran prometen proporcionarse tiempo de procesamiento entre sí cuando surja una emergencia.

Almacén de datos (Data warehouse)

Término genérico para un sistema que almacena, recupera y administra grandes volúmenes de datos. El software del almacén de datos a menudo incluye técnicas complejas de comparación y fragmentación (hashing) para búsquedas rápidas, así como una filtración avanzada.

Almacenamiento externo

La locación que contiene las copias de respaldo que se van a utilizar en caso de que sea necesaria la recuperación o restablecimiento cuando ocurre un desastre.

Alojamiento Web

El negocio de proporcionar el equipo y los servicios que se requieren para alojar y mantener archivos para uno o más sitios Web, así como para proporcionar conexiones rápidas de Internet a dichos sitios. La mayor parte del alojamiento es "compartido", lo que significa que los sitios Web de múltiples compañías están en el mismo servidor a fin de compartir/reducir los costos.

Análisis de amenazas

Una evaluación del tipo, alcance y naturaleza de los incidentes o acciones que pueden resultar en consecuencias adversas; identificación de las amenazas que existen contra los activos de información y la tecnología de información. El análisis de amenazas suele definir también el nivel de amenaza y la probabilidad de que ésta se materialice.

Análisis de criticidad

Un análisis para evaluar los recursos o las funciones de negocio a fin de identificar su importancia para la organización, y el impacto que tendrían en caso de que no sea posible concluir una función o de que no esté disponible un recurso.

Análisis de impacto

Un análisis de impacto es un estudio para priorizar la criticidad de los recursos de información para una organización con base en los costos (o consecuencias) de eventos adversos. En un análisis de impacto se identifican amenazas a los activos y se determinan pérdidas de negocio potenciales para diferentes periodos. Esta valoración se utiliza para justificar el grado de protección que se requiere y los tiempos de recuperación. Este análisis es la base para establecer la estrategia de recuperación.

Análisis/valoración de impacto al negocio (BIA)

Evaluar la criticidad y la sensibilidad de los activos de información. Es un ejercicio que determina el impacto que tendría en una organización perder el soporte de algún recurso; establece el incremento de dicha pérdida al paso del tiempo; identifica los recursos mínimos que se requieren para recuperar y prioriza la recuperación de procesos y sistemas de soporte. Este proceso también incluye tratar los siguientes temas:

- Pérdida de ingresos
- Gastos inesperados
- Temas legales (cumplimiento regulatorio o contractual)
- Procesos interdependientes
- Pérdida del reconocimiento o la confianza del público

Archivos de firma de virus

El archivo de los patrones de un virus que se comparan con los archivos existentes para determinar si están infectados con algún virus o gusano.

Archivos fuera de línea

Medios de almacenamiento de archivos informáticos que no están conectados físicamente a la computadora; por lo general para este tipo de respaldo se utilizan cintas o cartuchos de cinta.

Ataque por fuerza bruta

Intentar en repetidas ocasiones todas las posibles combinaciones de contraseñas y llaves de cifrado hasta que se encuentra la correcta.

Autenticación

El acto de verificar la identidad de una entidad (p.ej. un usuario, un sistema o un nodo de red).

Autoridad de certificación (CA)

En criptografía, una CA es una entidad que emite certificados digitales para uso de otras partes. Es un ejemplo de una entidad externa de confianza. Una CA certifica, como proveedor de confianza de pares de llaves públicas/privadas, la autenticidad del dueño (compañía o persona) a la cual se le ha dado un par de llave pública/privada. El proceso involucra a una CA que toma la decisión de emitir un certificado con base en evidencia o conocimiento obtenido mediante la verificación de la identidad del receptor. Una vez verificada la identidad del receptor, la CA firma el certificado con su llave privada para su distribución al usuario, donde, a su recepción, el usuario descifra el certificado con la llave pública de la CA (p.ej. CAs comerciales, tales como Verisign, proporcionan llaves públicas en navegadores de red). La CA ideal tiene autoridad (alguien en quien el usuario confía) por el nombre o el espacio de llave que representa. Las CAs son características de muchos esquemas de infraestructura de llave/clave pública (PKI). Muchas CAs comerciales cobran por sus servicios. Algunas instituciones y gobiernos pueden tener sus propias CAs, aun cuando también existen CAs gratuitas.

Autenticación de doble factor

El uso de dos mecanismos independientes de autenticación, por ejemplo, requerir una tarjeta inteligente y una contraseña. Suele ser la combinación de algo que usted sabe, que usted es o que usted tiene.

Cadena de custodia

La cadena de custodia es un principio legal relativo a la validez y la integridad de la evidencia. Requiere de responsabilidad por todo lo que se utilice como evidencia en un proceso legal, a fin de asegurar que se puede explicar desde el momento en que se obtuvo hasta cuando se presentó ante el tribunal. Esto incluye documentación sobre quién tuvo acceso a la evidencia y cuándo, así como la capacidad de identificar la evidencia como el punto exacto que se recuperó o probó. La falta de control sobre la evidencia puede conducir a que se le desacredite. La cadena de custodia depende de la capacidad para verificar que la evidencia no pudo haber sido alterada. Esto se logra al sellar la evidencia para que no se pueda cambiar, y al proporcionar registro documental de la custodia para probar que la evidencia estuvo, en todo momento, bajo estricto control y no sujeta a manipulación.

Capacidad de recuperación

La capacidad de un sistema o red para soportar eventos perjudiciales significativos sin fallar.

Capas de aplicación

En el modelo de comunicaciones de Interconexión de Sistemas Abiertos (OSI), la capa de aplicación proporciona servicios para un programa de aplicación para posibilitar una comunicación eficaz con otro programa de aplicación en una red. La capa de aplicación no es la aplicación que está realizando la comunicación, sino una capa de servicio que proporciona estos servicios.

Centro de control

Alberga las reuniones de recuperación cuando se manejan operaciones de recuperación de desastre.
Centro de Soporte

Centro de soporte (help desk)

Un recurso organizacional, conocido también como centro de servicio (help desk), que ofrece asistencia de TI a los usuarios finales

Certificado digital

Una "tarjeta de crédito" electrónica que establece las credenciales del usuario cuando se hacen negocios y otras transacciones en la red. Los certificados digitales pueden ser emitidos por una autoridad de certificación (CA). Contiene el nombre del usuario, un número de serie, las fechas de vencimiento, una copia de la llave/clave pública del poseedor del certificado (utilizada para cifrar y descifrar mensajes y firmas digitales), y la firma digital de la autoridad que emite el certificado, de tal forma que el receptor pueda verificar que el certificado es auténtico.

Clasificación de datos

La asignación de un nivel de sensibilidad a los datos (o información) que resulta en la especificación de controles para cada nivel de clasificación. Los niveles de sensibilidad de datos se asignan de acuerdo a categorías predefinidas a medida que los datos se crean, modifican, mejoran, almacenan o transmiten. El nivel de clasificación es un indicador del valor o importancia que tienen los datos para la organización.

COBIT

Conjunto internacional de objetivos de control de TI publicado por ISACA, 2007, 2005, 2000, 1998, 1996

Código de autenticación de mensajes

Una suma de verificación estándar del ANSI que se calcula mediante la Norma de cifrado de Datos (DES).

Comité directivo

Un comité directivo conformado para apoyar y administrar varios proyectos, tales como un programa de seguridad de información.

Confidencialidad

La protección de información privada o sensible contra divulgación no autorizada.

Conjunto redundante de discos económicos (RAID)

Una tecnología que brinda mejoras en el desempeño y capacidades tolerantes a fallas mediante soluciones de hardware y software, escribiendo en una serie de discos múltiples para mejorar el desempeño y guardar grandes archivos al mismo tiempo.

Conocimiento dividido

Una técnica de seguridad en la cual dos o más entidades por separado tienen partes de datos que en forma individual no transmiten ningún conocimiento de la información que resulta de combinar ambas partes. Una condición bajo la cual dos o más entidades por separado tienen componentes de llave que en forma individual no transmiten ningún conocimiento de la llave de

texto plano que se produce cuando los componentes de la llave se combinan en el módulo criptográfico.

Contramedidas

Cualquier proceso que reduce directamente una amenaza o vulnerabilidad.

Control de acceso discrecional (DAC)

Un medio para restringir el acceso a objetos basado en la identidad de los sujetos y/o grupos a los que pertenecen. Los controles son discrecionales en el sentido de que un sujeto con determinados permisos de acceso es capaz de pasarle ese permiso (tal vez en forma indirecta) a algún otro sujeto.

Control de acceso obligatorio (MAC)

Un medio para restringir el acceso a los datos con base en grados variantes de requerimientos de seguridad para la información que está contenida en los objetos y la correspondiente certificación de seguridad de los usuarios o programas que actúan en su nombre.

Control de programación del plan de recuperación de desastre

Por lo general una lectura de un plan de recuperación de desastre sin que se tome ninguna acción real. En general implica leer el plan, discutir los puntos de acción y definir cualquier brecha que pudiera identificarse.

Control dual

Un procedimiento que utiliza dos o más entidades (por lo general, personas) que operan en conjunto para proteger un recurso de un sistema, de tal forma que ninguna otra entidad que actúe sola pueda acceder a dicho recurso.

Controles

Las políticas, procedimientos, prácticas, dispositivos y estructuras organizacionales que están diseñados para brindar una confianza razonable de que se alcanzarán los objetivos de negocio y que se evitarán, o bien, detectarán y corregirán los eventos no deseados.

Controles administrativos

Las reglas, procedimientos y prácticas que están relacionados con la efectividad operativa, la eficiencia y el cumplimiento con las regulaciones y las políticas gerenciales.

Controles de acceso

Las reglas, procedimientos, prácticas y dispositivos cuyo objetivo es prevenir la entrada o el derecho de uso no autorizado, ya sea físico o electrónico.

Controles de aplicación

Actividades manuales o programadas que tienen el propósito de garantizar la integridad y la precisión de los registros, así como la validez de las entradas realizadas.

Copiado de disco

La práctica de duplicar datos en volúmenes separados en dos discos duros para hacer que el almacenamiento sea más tolerante a las fallas. El copiado protege los datos en caso de una falla en el disco, ya que los datos se actualizan constantemente en ambos discos.

COSO

Se refiere al reporte "Control Interno—Un marco integrado" patrocinado por el Committee of Sponsoring Organizations of the Treadway Commission en 1992. Brinda orientación y un marco integral de control interno para todas las organizaciones.

Criticidad

Una medida del impacto que puede tener en una organización la falla de un sistema para funcionar según lo requerido.

Cuota por notificación de desastre

La cuota que cobra el proveedor del sitio de recuperación cuando el cliente le notifica que ha ocurrido un desastre y que se requiere del sitio de recuperación. Esta cuota se cobra para desalentar notificaciones falsas de desastres.

Debida diligencia

La realización de aquellas acciones que suelen considerarse prudentes, responsables y necesarias para llevar a cabo una investigación, revisión y/o análisis objetivo y exhaustivo.

Debido cuidado

El nivel de cuidado que se espera de una persona razonable de competencia similar en condiciones similares.

Declaración de desastre

La comunicación a las partes internas y externas pertinentes de que se ha puesto en operación el plan de recuperación de desastre.

Defensa en profundidad

La práctica de dividir en capas las defensas para proporcionar una mayor protección. La defensa en profundidad incrementa la seguridad al aumentar el esfuerzo que se necesita en un ataque. Esta estrategia coloca múltiples barreras entre un atacante y los recursos de información y computación de una organización.

Derechos de acceso

Permisos o privilegios otorgados a usuarios, programas o estaciones de trabajo para crear, cambiar, borrar o ver datos y archivos dentro de un sistema, tal como definen las reglas establecidas por los dueños de los datos y la política de seguridad de información.

Descentralización

El proceso de distribuir el procesamiento informático a diferentes locaciones en una organización.

Desimantación

La aplicación de niveles variables de corriente alterna con el propósito de desmagnetizar medios magnéticos de registro. El proceso implica aumentar en forma gradual el campo de corriente alterna de cero a un valor máximo y otra vez de vuelta a cero, lo que deja un residuo muy bajo de inducción magnética en el medio. Desimantar flojamente significa borrar.

Detección de intrusos

El proceso de monitorear los eventos que ocurren en un sistema o red informático para detectar señales de accesos no autorizados o ataques.

Directrices

Una acción sugerida o recomendación relacionada con un área de una política de seguridad de información que pretende complementar un procedimiento. A diferencia de las normas, la implementación de directrices puede ser a discreción del lector.

Disponibilidad

Garantizar que los sistemas de información y los datos estén listos para su uso cuando se les necesita; a menudo se expresa como el porcentaje de tiempo que se puede utilizar un sistema para trabajo productivo.

DMZ

La zona búfer ubicada entre la Internet y la red privada que se diseña utilizando firewalls y otros dispositivos para evitar el acceso de partes externas a los sistemas internos. El acrónimo se basa en el término militar "zona desmilitarizada" que se emplea para describir la zona búfer aislada establecida entre Corea del Sur y Corea del Norte.

Enmascarados

Atacantes que penetran los sistemas mediante el uso de la identidad de usuarios legítimos y sus claves de acceso.

Entrega Objetiva del servicio (SDO)

Niveles de servicio que se alcanzarán durante el modo alterno de proceso hasta que se restablezca la situación normal. Se relacionan directamente con las necesidades del negocio.

Evaluación del daño

La determinación del grado de daño que es necesario realizar para calcular el tiempo de recuperación y la pérdida potencial para la organización.

Evasión del riesgo

El proceso para evitar un riesgo en forma sistemática, lo cual constituye un método para administrar el riesgo.

Examinación forense

El proceso de recopilar, evaluar, clasificar y documentar la evidencia digital para ayudar a la identificación de un delincuente y el método utilizado para comprometer un sistema.

Exposición

El grado al cual una vulnerabilidad puede resultar en consecuencias adversas; la pérdida potencial para un área como resultado de un evento adverso que ha ocurrido.

Filtrado de paquetes

Forma de controlar el acceso a una red mediante el análisis de atributos de los paquetes de entrada y salida, dejándolos pasar, o bien, rechazándolos con base en una lista de reglas predefinidas.

Firewall

Un sistema o una combinación de sistemas que impone una barrera entre dos o más redes que por lo regular forman una barrera entre un ambiente seguro y uno abierto, como la Internet.

Firma de código digital

El proceso de firmar en forma digital un código informático para garantizar su integridad.

Gobierno corporativo

El sistema mediante el cual se dirigen y controlan las organizaciones. Los consejos de administración son los responsables del gobierno de sus organizaciones.

Gobierno de la empresa

Un conjunto de responsabilidades y prácticas, ejercidas por el consejo y la dirección ejecutiva, con la finalidad de brindar una dirección estratégica, garantizar que se logran los objetivos, determinar que los riesgos se gestionan en forma apropiada y verificar que los recursos de la empresa se utilizan con responsabilidad.

Gobierno de seguridad de la información

El conjunto de responsabilidades y prácticas, ejercidas por el consejo y la dirección ejecutiva, con la finalidad de brindar una dirección estratégica, garantizar que se logran los objetivos, determinar que los riesgos se administran en forma apropiada y verificar que los recursos de la empresa se utilizan con responsabilidad.

Gusano

Un programa auto replicable que no se adhiere a programas, sino que se propaga en forma independiente a las acciones de los usuarios. Los gusanos son, en efecto, ataques programados a redes.

Honeypot

Un servidor configurado especialmente, también conocido como servidor "señuelo" (decoy), diseñado para atraer y monitorear intrusos de tal forma que sus acciones no afecten a los sistemas en producción.

Hot site

Un sitio externo completamente operativo para el procesamiento de datos equipado con software de sistemas y hardware para su uso en caso de un desastre.

Imagen bit-stream

Las copias de respaldos bit-stream, también conocidos como respaldos espejo, implican respaldar todas las áreas de una unidad de disco duro de una computadora u otro tipo de medio de almacenamiento. Dichos respaldos replican exactamente todos los sectores de un determinado dispositivo de almacenamiento, incluyendo todos los archivos y las áreas de almacenamiento de datos ambientales.

Ingeniería social

Un ataque basado en engañar a los usuarios o administradores en el sitio objetivo para que revelen información confidencial o sensible.

Instalaciones alternas

Locaciones e infraestructuras desde las cuales se ejecutan procesos de respaldo o de emergencia, cuando las instalaciones principales no están disponibles o están destruidas. Esto incluye otros edificios, oficinas o centros de procesamiento de datos.

Integridad

La precisión, integridad y validez de la información.

Interrupciones máximas de energía eléctrica tolerables (MTO)

El tiempo máximo que la organización puede tolerar el procesamiento en modo alterno.

ISO/IEC 17799

Emitido originalmente como parte de la Norma Británica para la *Seguridad de la Información* en 1999 y luego como el *Código de Práctica para la Gerencia de la Seguridad de Información* en octubre de 2000, recibió la categoría de código internacional de práctica para la gerencia de la seguridad de información por parte de la Organización Internacional para la Estandarización (ISO). Esta norma define los controles de disponibilidad, integridad y confidencialidad de la información en un sistema integral para la gerencia de la seguridad de información. La versión más reciente es ISO/IEC 17799:2005.

ISO/IEC 27001

Una norma internacional, emitida en 2005 y revisada en 2006, sobre la gerencia de la seguridad de la información que se basa en ISO/IEC 17799 y define un conjunto de principios orientadores con respecto a la confidencialidad, integridad y disponibilidad de la información.

Lógica de ramificación

Predecir en qué forma un programa se va a ramificar cuando se presenta una aplicación. Es un código optimizado basado en una predicción de ramificación.

Llave de descifrado

Una pieza digital de información que se utiliza para recuperar texto plano de su texto cifrado correspondiente mediante descifrado.

Metodología de Pruebas de Seguridad con software libre (Open Source)

Metodología y manual abiertos y libremente disponibles para realizar pruebas a la seguridad.

Monitoreo de intrusos

El uso de investigaciones o rastros transportados para reunir información, rastrear tráfico e identificar vulnerabilidades.

Métricas de seguridad

Una forma de medición relativa a un punto de referencia que se utiliza para monitorear actividad relacionada con la seguridad y evaluar el desempeño de los programas relacionados con la seguridad.

Mitigación del riesgo

La administración de un riesgo mediante el uso de controles y contramedidas.

No repudio

La certeza de que una parte no podrá negar después haber originado los datos; es decir, se trata de dar pruebas de la integridad y el origen de los datos y puede ser verificada por un tercero. Una firma digital puede proporcionar el no repudio.

Norma de cifrado de Datos (DES)

Un algoritmo para codificar datos binarios. Se trata de un sistema criptográfico de llave/clave privada publicado por la Agencia Nacional de Normas (NBS), el antecesor del Instituto Nacional de Normas y Tecnología de los EUA (NIST). La DES se definió en 1976 como una Norma Federal para el Procesamiento de Información (FIPS) y se ha utilizado comúnmente para cifrar datos en forma de implementación de hardware y software.

Normalización de datos

Un proceso estructurado para organizar datos en tablas de tal forma que conserva las relaciones entre los datos.

Normas

Una métrica utilizada para determinar la exactitud de una cosa o proceso; un conjunto de reglas o especificaciones que, consideradas en conjunto, definen un dispositivo de software o hardware. Una norma es también una base reconocida para comparar y medir algo.

Pista de auditoría

Una serie de registros ya sea impresos o en formato electrónico que proporcionan un registro cronológico de la actividad del usuario y otros eventos que muestran los detalles de las actividades del usuario y del sistema. Las pistas de auditoría pueden utilizarse para documentar cuándo ingresan los usuarios, cuánto tiempo dedican a varias actividades, qué hacen y si se ha violado o intentado violar la seguridad.

Plan de recuperación de desastre

Una serie de recursos humanos, físicos, técnicos y de procedimientos orientados a recuperar, dentro de tiempos y costos definidos, una actividad interrumpida por una emergencia o desastre.

Policía cibernético

Un investigador de actividades relacionadas con delitos informáticos.

Política de monitoreo

Reglas que describen o definen la forma en la cual se captura e interpreta la información sobre el uso de computadoras, redes, aplicaciones e información.

Política de uso aceptable

Una política que establece un acuerdo entre usuarios y la organización y define los rangos de uso para todas las partes que se aprueban antes de obtener acceso a la red o a la Internet.

Políticas

Declaraciones de alto nivel sobre la intención y la dirección de la gerencia.

Privacidad

Libertad contra intrusión o divulgación no autorizada de información sobre personas.

Procedimientos

Una descripción detallada de los pasos necesarios para realizar operaciones específicas conforme a las normas aplicables.

Proceso alterno

Procesos manuales o automáticos diseñados y establecidos para continuar con los procesos críticos de negocio desde el punto de falla hasta el regreso a la normalidad.

Programa de seguridad de la información

La combinación total de las medidas técnicas, operativas y de procedimientos, así como las estructuras administrativas implementadas para asegurar la confidencialidad, integridad y disponibilidad de la información con base en los requerimientos de negocio y el análisis de riesgos.

Programación en shell

Un script de interfaz de comandos (shell) es un script escrito para la interfaz de comandos (shell) o intérprete de línea de comando de un sistema operativo. Suele considerarse un lenguaje de programación simple de dominio específico. Entre las operaciones que llevan a cabo los scripts de interfaz de comandos (shell) se encuentran la manipulación de archivos, ejecución de programas y texto de impresión. Por lo general, los scripts de interfaz de comandos (shell) se refieren a scripts escritos para un shell de Unix, mientras que los scripts de línea de comando COMMAND.COM (DOS) y cmd.exe (Windows) suelen denominarse archivos en batch.

Muchos intérpretes de scripts de interfaz de comandos (shell) funcionan también como interfaces de línea de comandos, tales como diversas interfaces de comandos (shells) de Unix, Windows PowerShell o el COMMAND.COM de MS-DOS. Otros, tales como AppleScript, agregan una capacidad de programación (scripting) para ambientes informáticos que no cuentan con una interfaz de línea de comandos. Otros ejemplos de lenguajes de programación dirigidos en esencia a la programación de shell incluyen el lenguaje de comando digital (DCL) y el lenguaje de control de trabajos (JCL).

Protocolo de Transferencia de Archivos Anónimo (AFTP)

Un método para descargar archivos públicos utilizando el Protocolo de Transferencia de Archivos (FTP). AFTP no requiere que los usuarios se identifiquen antes de acceder a los archivos desde un servidor en particular. En general, los usuarios ingresan la palabra "anónimo" cuando el host pide un nombre de usuario. Cualquier cosa se puede ingresar para la contraseña, por ejemplo, la dirección de correo electrónico del usuario o simplemente la palabra "invitado". En muchos casos, un sitio de AFTP ni siquiera pedirá a un usuario que proporcione un nombre y una contraseña.

Proveedor del Servicio de Aplicación (ASP)

Conocido también como proveedor de servicios administrados (MSP), implementa, alberga y administra el acceso a una aplicación en paquete para múltiples partes desde una instalación administrada centralmente. Las aplicaciones se entregan a través de redes mediante una suscripción.

Proveedor de Servicio de Internet (ISP)

Un tercero que proporciona acceso a la Internet a personas y organizaciones, así como a una variedad de otros servicios relacionados con la Internet.

Protocolo de Transferencia de Hipertexto (HTTP)

Un protocolo de comunicación utilizado para conectar servidores en World Wide Web. Su función principal es establecer una conexión con un servidor Web y transmitir HTML, XML u otras páginas en los navegadores del cliente.

Pruebas de penetración

Una prueba en vivo de la eficacia de las defensas de la seguridad mediante la imitación de acciones que llevan a cabo atacantes en la vida real.

Puertos

Un punto de interfaz entre una CPU y un dispositivo periférico. Un puerto puede ser también una convención que permite que servicios remotos se conecten a un host en forma ordenada.

Punto Objetivo de Recuperación (RPO)

El tiempo específico anterior a un corte de energía al cual se debe restablecer los datos.

Red privada virtual (VPNs)

Una red privada segura que utiliza la infraestructura de telecomunicaciones pública para transmitir datos. En comparación con un sistema mucho más costoso de líneas propias o alquiladas que sólo pueden ser utilizadas por una compañía, las VPN son utilizadas por empresas tanto para extranets como para áreas amplias de Intranets. Mediante el uso de cifrado y autenticación, una VPN cifra todos los datos que pasan entre dos puntos de Internet, manteniendo la privacidad y la seguridad.

Responsabilidad

La capacidad de hacer corresponder una determinada actividad o incidente con la parte responsable.

Respuesta pasiva

Una opción de respuesta a la detección de intrusos en la cual el sistema simplemente notifica y registra el problema detectado, confiando en que el usuario tomará acciones posteriores.

Riesgo residual

La cantidad de riesgo que permanece aun después de que se han implementado controles y contramedidas.

Rootkit

Un rootkit es un conjunto de herramientas de software que tienen como finalidad esconder procesos en ejecución, archivos o datos de sistema del sistema operativo. Los rootkits tienen su origen en aplicaciones benévolas pero han sido utilizados cada vez más por malware para ayudar a los intrusos a mantener el acceso a los sistemas mientras que se evita la detección. Existen rootkits para varios sistemas operativos, tales como Microsoft Windows, Linux y Solaris. Los rootkits suelen modificar las partes de un sistema operativo o instalarse como unidades de disco o módulos centrales del sistema operativo.

Ruta abierta más corta primero (OSPF – Open Shortest Path First)

Un protocolo de enrutamiento que se ha desarrollado para redes IP. Se basa en la primera ruta más corta o algoritmo de estado de enlace.

Ruta de acceso

La ruta lógica que toma un usuario final para acceder a información computarizada que incluye redes, sistemas, sistemas autorizados y de autenticación, aplicaciones y controles de aplicación.

Seguridad IP (IPSec)

Un protocolo que soporta dos modos de cifrado: transporte y túnel. El modo transporte cifra la porción de datos (carga útil) de cada paquete pero deja intacto al encabezado. El modo túnel es más seguro, ya que cifra tanto al encabezado como la carga útil. Del lado de la recepción, un dispositivo que cumple con IPSec descifra cada paquete.

Sensibilidad

El nivel del impacto que una divulgación inapropiada o peligro podría tener en una organización.

Servidor de nombre de dominio (DNS)

Un servicio de red basado en un sistema jerárquico de base de datos distribuido a lo largo de la Internet que traduce una dirección Web en una dirección IP y *viceversa*.

Servidor falso de correo electrónico no deseado (mail relay)

Un servidor de correo electrónico que retransmite mensajes de tal forma que ni el emisor ni el receptor sea un usuario local.

Servidor proxy

Un servidor que actúa a nombre de un usuario. Por lo general, los proxies aceptan una conexión de un usuario, deciden si la dirección IP del cliente o usuario tiene permiso para utilizar el proxy, tal vez realiza una autenticación adicional, y después completa una conexión a un destino remoto a nombre del usuario.

Servidor Web

Mediante el uso del modelo cliente-servidor y del Protocolo de Transferencia de Hipertexto (HTTP) de World Wide Web, el servidor web es un programa de software que presta servicios de páginas web a usuarios.

Sistema de detección de intrusos (IDS)

Un IDS inspecciona la actividad en la seguridad del host y la red para identificar patrones sospechosos que pudieran ser indicadores de un ataque al sistema o la red.

Sitio alterno

Es una instalación alterna para continuar con las operaciones de TI/SI cuando el sitio principal de procesamiento de datos no está disponible.

Sitio espejo

Un sitio alterno que contiene la misma información que el original. Los sitios espejo están configurados para respaldo y recuperación en caso de desastre, así como para equilibrar la carga de tráfico de numerosas solicitudes de descarga. Dichos espejos de descarga con frecuencia se colocan en diferentes ubicaciones a lo largo de la Internet.

Sitio móvil

El uso de un sitio móvil/temporal que sirve como un lugar para retomar el negocio. Por lo general se pueden establecer en cualquier sitio y albergar tecnología de información y personal.

Sitio redundante

Una estrategia de recuperación que implica duplicar los componentes clave de tecnología de información, incluso datos u otros procesos de negocio clave mediante los cuales se puede conseguir una recuperación rápida.

Situación de alerta

El punto en un procedimiento de emergencia en el cual el tiempo transcurrido atraviesa un valor umbral y la interrupción no se resuelve. La organización que entra en una situación de alerta inicia una serie de pasos de escalamiento.

Sniffing

El proceso mediante el cual los datos que atraviesan una red son capturados o monitoreados.

Software antivirus

Un software de aplicación implementado en múltiples puntos en una arquitectura de TI. Está diseñado para detectar y eliminar potencialmente el código de virus antes de que ocurra un daño y reparar o colocar en cuarentena los archivos que ya están infectados.

Spoofing

Falsificar la dirección de envío de una transmisión de red.

Tiempo Objetivo de recuperación (RTO)

Tiempo establecido para la recuperación de una función o recurso de negocio después de que ha ocurrido un desastre.

Transferencia de riesgo

El proceso de ceder el riesgo a otra organización, por lo general mediante la compra de una póliza de seguro o la subcontratación de un servicio.

Usuario final

Una persona que utiliza sistemas informáticos que no es responsable de su conservación o mantenimiento.

Valoración de la dependencia del negocio

El proceso de identificar los recursos que son críticos para la operación de un proceso de negocio.

Ventana de interrupción aceptable

La ventana de interrupción aceptable (AIW) es el periodo máximo que un sistema puede no estar disponible antes de que se ponga en riesgo el logro de los objetivos de negocio de la organización.

Ventana de interrupción

El tiempo que una compañía puede esperar desde el punto de falla hasta el restablecimiento de los servicios o aplicaciones mínimos y críticos. Después de ese tiempo, las pérdidas progresivas ocasionadas por la interrupción son excesivas para la organización.

Verificación de plan de recuperación ante desastres

Generalmente una prueba sólida del plan de recuperación que requiere que algunas actividades de recuperación se materialicen y pongan a prueba. A menudo se establece un escenario de desastre y los equipos de recuperación discuten los pasos que necesitan tomar para la recuperación. Deben probar tantos aspectos del plan como sea posible.

Violación de contraseñas

Una herramienta que prueba la resistencia de las contraseñas de los usuarios y busca aquellas que sean fáciles de adivinar al intentar en repetidas ocasiones palabras de diccionarios elaborados especialmente y a menudo generan miles (y en algunos casos incluso millones) de combinaciones de caracteres, números y símbolos.

Valoración de riesgos

Un proceso que se utiliza para identificar y evaluar los riesgos y su posible impacto en la organización en términos cuantitativos o cualitativos.

Vulnerabilidades

Una deficiencia en el diseño, la implementación, la operación o los controles internos en un proceso que podría explotarse para violar la seguridad del sistema.

Warm site

Un warm site es similar a un hot site; sin embargo, no está completamente equipado con todo el hardware necesario para la recuperación.

ACRÓNIMOS

El candidato a CISM debe estar familiarizado con la siguiente lista de acrónimos. Estos acrónimos son las únicas abreviaturas utilizadas en las preguntas del examen.

CD	Compact Disk
CD-ROM	Compact Disk Read Only Memory
DMZ	Demilitarized zone
HTML	Hypertext Markup Language
ID	Identification
IP	Internet Protocol
IPS	Intrusion prevention system
IPSec	Internet Protocol Security
IS	Information systems
ISP	Internet service provider
IT	Information technology
OS	Operating system
URL	Universal resource locator
XML	Extensible Markup Language

Además de los acrónimos antes mencionados, los candidatos podrían desear conocer los siguientes acrónimos adicionales. En caso de que alguna de estas abreviaturas se utilice en las preguntas de evaluación, sus significados se incluirían cuando aparezca el acrónimo.

AES	Advanced Encryption Standard
AESRM	Alliance for Enterprise Security Risk Management
AICPA	American Institute of Certified Public Accountants
AIW	Acceptable interruption window
ALE	Annual loss expectancy
API	Application programming interface
ARP	Address Resolution Protocol
AS/NZS	Australian Standard/New Zealand Standard
ASCII	American Standard Code for Information Interchange
ASIC	Application-specific integrated circuit
ASP	Application service provider
ATM	Asynchronous Transfer Mode
BCI	Business Continuity Institute
BCM	Business continuity management
BCP	Business continuity planning
BGP	Border Gateway Protocol
BI	Business intelligence
BIA	Business impact analysis
BIIMS	Biometric information management and security
BIOS	Basic input/output system
BIS	Bank for International Settlements
BITS	Banking Information Technology Standards
BLP	Bell-LaPadula
BLP	Bypass label process
BMS	Building management systems
BS	British Standard
CA	Certificate authority
CASPR	Commonly accepted security practices and recommendations
CBT	Computer-based training
CCO	Chief compliance officer

CEO	Chief executive officer
CERT	Computer emergency response team
CFO	Chief financial officer
CICA	Canadian Institute of Chartered Accountants
CIM	Computer-integrated manufacturing
CIO	Chief information officer
CIRT	Computer incident response team
CIS	Center for Internet Security
CISO	Chief information security officer
CLC	Chief legal counsel
CMM	Capability Maturity Model
CMU	Carnegie Mellon University
COO	Chief operating officer
COOP	Continuity of operations plan
CORBA	Common Object Request Broker Architecture
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CPO	Chief privacy officer
CPS	Certification practice statement
CPU	Central processing unit
CRL	Certificate revocation list
CRM	Customer relationship management
CSA	Control self-assessment
CSF	Critical success factor
CSIRT	Computer security incident response team
CSO	Chief security officer
CSRC	Computer Security Resources Center (USA)
CVE	Common vulnerabilities and exposures
CW	Clark-Wilson
DAC	Discretionary access controls
DBMS	Database management system
DCE	Distributed control environment
DCE	Data communications equipment
DCE	Distributed computing environment
DCL	Digital command language
DDoS	Distributed denial of service
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DLT	Digital linear tape
DNS	Domain name server
DNSSEC	Domain Name Service Secure
DoS	Denial of service
DOSD	Data-oriented system development
DR	Disaster recovery
DRII	Disaster Recovery Institute International
DRP	Disaster recovery planning
EDI	Electronic data interchange
EER	Equal error rate
EFT	Electronic funds transfer
EGRP	External Gateway Routing Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
EU	European Union
FAR	False-acceptance rate
FCPA	Foreign Corrupt Practices Act
FERC	Federal Energy Regulatory Commission (USA)
FFIEC	Federal Financial Institution Examination Council (USA)
FIPS	Federal Information Processing Standards (USA)
FISMA	Federal Information Security Management Act (USA)

FSA	Financial Security Authority (USA)	NDA	Nondisclosure agreement
GAISP	Generally Accepted Information Security Principles	NetBIOS	Network basic input/output systems
GAS	Generalized audit software	NFPA	National Fire Protection Association
GASSP	Generally Accepted Security System Principles	NFS	Network file system
GLBA	Gramm-Leach-Bliley Act (USA)	NIC	Network interface card
GMI	Governance Metrics International	NIDS	Network intrusion detection system
HD-DVD	High definition/high density-digital video disc	NIST	National Institute of Standards and Technology (USA)
HIDS	Host-based intrusion detection system	NPV	Net present value
HIPAA	Health Insurance Portability and Accountability Act (USA)	OCC	Office of the Comptroller of the Currency (USA)
HIPO	Hierarchy Input-Process-Output	OCSF	Online Certificate Status Protocol
HR	Human resources	OCTAVE	Operationally Critical Threat, Asset and Vulnerability Evaluation
HTTP	Hypertext Transfer Protocol	OECD	Organization for Economic Co-operation and Development
HTTPS	Secure Hypertext Transfer Protocol	OEM	Original equipment manufacturer
HVAC	Heating, ventilating and air conditioning	OEP	Occupant emergency plan
I&A	Identification and Authentication	OSI	Open systems interconnection
I/O	Input/output	OSPF	Open Shortest Path First
ICMP	Internet control message protocol	PAN	Personal area network
ICT	Information and communication technologies	PC	Personal computer/microcomputer
IDC	International Development Corp.	PCI	Payment Card Industry
IDEFIX	Integration Definition for Information Modeling	PDCA	Plan-do-check-act
IDS	Intrusion detection system	PKI	Public key infrastructure
IEC	International Electrotechnical Commission	PMBOK	Project Management Body of Knowledge
IETF	Internet engineering task force	POS	Point-of-sale
IFAC	International Federation of Accountants	PPP	People, process and policy
IIA	Institute of Internal Auditors	PPPoE	Point-to-point Protocol over Ethernet
IMT	Incident management team	PPT	People, process and technology
IPF	Information processing facility	PSTN	Public switched telephone network
IPL	Initial program load	PVC	Permanent virtual circuit
IPMA	International Project Management Association	QA	Quality assurance
IPRs	Intellectual property rights	RAID	Redundant Array of Inexpensive Disks
IPS	Intrusion-prevention system	RARP	Reverse Address Resolution Protocol
IRP	Incident response plan	RCERT	Regional Computer Emergency Response Team (USA)
IRS	Internal Revenue Service (USA)	ROI	Return on investment
IRT	Incident response team	ROSI	Return on security investment
ISF	Information Security Forum	RPO	Recovery point objective
ISO	International Organization for Standardization	RRT	Risk Reward Theorem/Tradeoff
ISO	Information security officer	RSA	Rivest, Shamir and Adleman (RSA stands for the initials of the developers last names)
ISS	Institutional Shareholders Services	RTO	Recovery time objective
ISSA	Information System Security Association	S/HTTP	Secure Hypertext Transfer Protocol
ISSEA	International System Security Engineering Association	S-MIME	Secure Multipurpose Internet Mail Extensions
ITGI	IT Governance Institute	SABSA	Sherwood Applied Business Security Architecture
JCL	Job control language	SAC	Systems auditability and control
KGI	Key goal indicator	SCADA	Supervisory Control and Data Acquisition
KLOC	Kilo lines of code	SDLC	System development life cycle
KPI	Key performance indicator	SDO	Service delivery objective
L2TP	Layer 2 Tunneling Protocol	SEC	Securities and Exchange Commission (USA)
LAN	Local area network	SEI	Software Engineering Institute
LCP	Link Control Protocol	SIEM	Security Information and Event Management
M&A	Mergers and Acquisition	SIM	Security information management
MAC	Mandatory access control	SLA	Service level agreement
MAO	Maximum allowable outage	SMART	Specific, measurable, achievable, relevant, time-bound
MIME	Multi-Purpose Internet Mail Extensions	SMF	System management facility
MIS	Management information system	SOP	Standard operating procedure
MitM	Man-in-the-middle	SPI	Security Parameter Index
MTD	Maximum tolerable downtime		
MTO	Maximum tolerable outage		
NAT	Network address translation		
NCP	Network Control Protocol		

SPICE	Software process improvement and capability determination	TCO	Total cost of ownership
SPOC	Single point of contact	TCP	Transmission Control Protocol
SPOOL	Simultaneous peripheral operations online	TCP/IP	Transmission Control Protocol/Internet Protocol
SQL	Structured Query Language	TCP/UDP	Transmission Control Protocol/User Datagram Protocol
SSG	Security steering group	TLS	Transport layer security
SSH	Secure Shell	UDP	User Datagram Protocol
SSL	Secure Sockets Layer	UPS	Uninterruptible power supply
SSO	Single sign-on	USB	Universal Serial Bus
		VAR	Value at risk
		VoIP	Voice-over IP
		VPN	Virtual private network
		WAN	Wide area network
		XBRL	Extensible Business Reporting Language