Términos y definiciones de la certificación

A

**Acceso no autorizado:** tipo de incidente que se produce cuando una persona obtiene acceso digital o físico a un sistema o aplicación sin permiso.

**Acceso protegido WiFi (WPA):** protocolo de seguridad inalámbrico para que los dispositivos se conecten a Internet.

**Actividad posterior al incidente:** proceso de revisión de un incidente para identificar áreas de mejora durante la gestión del incidente.

**Activo:** elemento percibido como valioso para una organización.

**Actor de amenazas:** cualquier persona o grupo que represente un riesgo para la seguridad.

**Actualización de parches:** actualización de software y sistemas operativos que soluciona las vulnerabilidades de seguridad de un programa o producto.

**Adware:** tipo de software legítimo que a veces se utiliza para mostrar publicidad digital en las aplicaciones.

**Algoritmo:** conjunto de reglas utilizadas para resolver un problema.

**Amenaza externa:** cualquier cosa fuera de la organización que tenga el potencial de dañar sus activos.

**Amenaza interna:** empleado actual o antiguo, proveedor externo o socio de confianza que suponga un riesgo para la seguridad.

**Amenaza persistente avanzada (APT):** un caso en el que un actor de amenazas mantiene el acceso no autorizado a un sistema durante un periodo prolongado de tiempo.

**Amenaza:** cualquier circunstancia o evento que pueda afectar los activos de manera negativa.

**Análisis basado en anomalías:** un método de detección que identifica comportamientos anómalos.

**Análisis de firmas:** método de detección utilizado para encontrar eventos de interés.

**Análisis de registros de red:** el proceso de examinar los registros de red para identificar eventos de interés.

**Análisis de registros:** el proceso de examinar los registros para identificar eventos de interés.

**Análisis forense digital:** la práctica de recopilar y analizar datos para determinar qué sucedió después de un ataque.

**Análisis sintáctico:** proceso de conversión de datos a un formato más legible.

**Análisis:** la investigación y validación de alertas.

**Analizador de protocolo de red (rastreador de paquetes):** herramienta diseñada para capturar y analizar el tráfico de datos dentro de una red.

**Ancho de banda:** cantidad de datos que un dispositivo recibe cada segundo.

**Angler phishing:** una técnica en la que los atacantes se hacen pasar por representantes de servicio al cliente en las redes sociales.

**Aplicación potencialmente no deseada (PUA):** tipo de software no deseado que se incluye con programas legítimos y que puede mostrar anuncios, ralentizar el dispositivo o instalar otro software.

**Aplicación:** un programa que realiza una tarea específica.

**Aprovisionamiento de usuarios:** proceso de creación y mantenimiento de la identidad digital de un usuario.

**Árbol de ataque:** diagrama que relaciona las amenazas con los activos.

**Archivo de configuración:** archivo utilizado para configurar los parámetros de una aplicación**.**

**Archivo editable por todo el mundo:** un archivo que puede ser alterado por cualquier persona en el mundo.

**Argumento (Linux):** información específica que necesita un comando.

**Argumento (Python):** los datos que se pasan a una función al llamarla.

**Arquitectura de seguridad:** tipo de diseño de seguridad compuesto por diversos componentes, como herramientas y procesos, que se utilizan para proteger a una organización de riesgos y amenazas externas.

**Ataque a la cadena de suministro:** un ataque dirigido a los sistemas, las aplicaciones, el hardware y el software con el fin de identificar una vulnerabilidad donde instalar malware.

**Ataque criptográfico:** ataque que afecta a las formas seguras de comunicación entre un remitente y su destinatario previsto.

**Ataque de “caza de ballenas”:** categoría de intentos de spear phishing que están dirigidos a ejecutivos de alto rango en una organización.

**Ataque de “watering hole”**: tipo de ataque en el que un actor de amenazas compromete un sitio web visitado con frecuencia por un grupo específico de usuarios.

**Ataque de contraseña:** intento de acceder a dispositivos, sistemas, redes o datos protegidos por contraseña.

**Ataque de denegación de servicio (DoS):** un ataque que apunta a una red o servidor y lo inunda con tráfico de red.

**Ataque de denegación de servicio distribuido (DDoS):** tipo de ataque de denegación o servicio que utiliza múltiples dispositivos o servidores para inundar la red objetivo con tráfico no deseado.

**Ataque de fuerza bruta:** el proceso de ensayo y error para descubrir información privada.

**Ataque de inundación Synchronize (SYN):** tipo de ataque DoS que simula una conexión TCP/IP e inunda un servidor con paquetes SYN.

**Ataque de inyección:** código malicioso insertado en una aplicación vulnerable.

**Ataque de reproducción:** ataque de red realizado cuando un actor malicioso intercepta un paquete de datos en tránsito y lo retrasa o repite en otro momento**.**

**Ataque en ruta:** ataque en el que un actor malicioso se coloca en medio de una conexión autorizada e intercepta o altera los datos en tránsito.

**Ataque físico:** incidente de seguridad que afecta no solo a los entornos digitales, sino también a los físicos en los que se implementa.

**Ataque pitufo:** ataque de red realizado cuando un atacante detecta la dirección IP de un usuario autorizado y la inunda con paquetes ICMP.

**Ataque XSS almacenado:** situación en la que se inyecta un script malicioso directamente en el servidor.

**Ataque XSS basado en DOM:** una instancia en la que existe un script malicioso en la página web que carga un navegador.

**Ataque XSS reflejado:** una instancia en la que se envía un script malicioso a un servidor y se activa durante la respuesta del servidor.

**Auditoría de seguridad**: revisión de los controles, políticas y procedimientos de seguridad de una organización con respecto a un conjunto de expectativas.

**Autenticación básica:** tecnología utilizada para establecer la solicitud de un usuario para acceder a un servidor.

**Autenticación de múltiples factores (MFA):** medida de seguridad que requiere que un usuario verifique su identidad de dos o más formas para acceder a un sistema o red.

**Autenticación:** proceso para verificar quién es una persona.

**Automatización:** el uso de la tecnología para reducir el esfuerzo humano y manual para realizar tareas comunes y repetitivas.

**Autoridad numeradora CVE (CNA):** organización que se ofrece voluntariamente para analizar y distribuir información sobre CVE elegibles.

**Autorización:** el concepto de conceder acceso a recursos específicos en un sistema.

**Autorización:** el sexto paso del NIST RMF que se refiere a ser responsable de los riesgos de seguridad y privacidad que puedan existir en una organización.

B

**Base de datos relacional:** base de datos estructurada que contiene tablas relacionadas entre sí.

**Base de datos:** colección organizada de información o datos.

**Bash:** el intérprete de comandos por defecto en la mayoría de las distribuciones de Linux.

**Biblioteca estándar de Python:** amplia colección de código Python que suele venir empaquetada con Python.

**Biblioteca:** colección de módulos que proporcionan código al que los usuarios pueden acceder en sus programas.

**Biometría:** las características físicas únicas que se pueden utilizar para verificar la identidad de una persona.

**Botnet:** colección de computadoras infectadas por malware que están bajo el control de un solo actor de amenazas, conocido como el “bot-herder”.

C

**Cadena de custodia:** proceso de documentar la posesión y el control de la evidencia durante el ciclo de vida del incidente.

**Cadena de datos:** datos que se componen de una secuencia ordenada de caracteres.

**Captura de paquetes (P-cap):** archivo que contiene paquetes de datos interceptados desde una interfaz o red.

**Cargador de arranque:** programa de software que arranca el sistema operativo.

**Categorización:** el segundo paso del NIST RMF que se utiliza para desarrollar procesos y tareas de gestión de riesgos.

**Caza de amenazas:** la búsqueda proactiva de amenazas en una red.

**Cebo:** táctica de ingeniería social que tienta a las personas a comprometer su seguridad**.**

**CentOS:** distribución de código abierto estrechamente relacionada con Red Hat.

**Centro de operaciones de seguridad (SOC):** unidad organizativa dedicada a monitorear redes, sistemas y dispositivos en busca de amenazas o ataques a la seguridad.

**Certificado digital:** archivo que verifica la identidad de un titular de una clave pública.

**Chronicle:** una herramienta nativa de la nube diseñada para conservar, analizar y buscar datos.

**Ciberseguridad (o seguridad):** la práctica de garantizar la confidencialidad, integridad y disponibilidad de la información mediante la protección de redes, dispositivos, personas y datos contra el acceso no autorizado o la explotación delictiva.

**Ciclo de vida de respuesta a incidentes del Instituto Nacional de Estándares y Tecnología (NIST):** un marco para la respuesta a incidentes que consta de cuatro fases: preparación; detección y análisis; contención, erradicación y recuperación, y actividad posterior al incidente.

**Cifrado asimétrico:** el uso de un par de claves pública y privada para cifrar y descifrar datos.

**Cifrado simétrico:** uso de una sola clave secreta para intercambiar información.

**Cifrado:** algoritmo que encripta la información.

**Cifrado:** el proceso de convertir datos de un formato legible a un formato codificado.

**Clasificación de activos:** práctica de etiquetar los activos en función de su sensibilidad e importancia para una organización.

**Clave criptográfica:** mecanismo que descifra el texto cifrado.

**Clave externa:** columna de una tabla que es clave primaria en otra tabla.

**Clave primaria:** una columna en la que cada fila tiene una entrada única.

**Colisión de hash**: cuando diferentes entradas producen el mismo valor hash**.**

**Comando y control (C2):** las técnicas utilizadas por los actores maliciosos para mantener las comunicaciones con los sistemas comprometidos.

**Comando:** una instrucción que le dice a la computadora que haga algo.

**Comentario:** una nota que los programadores hacen sobre la intención detrás de su código.

**Comodín:** carácter que se utiliza para representar uno o más caracteres.

**Compromiso de correo electrónico empresarial (BEC):** tipo de ataque de phishing en el que un actor de amenazas se hace pasar por una fuente conocida para obtener una ventaja financiera**.**

**Computación en la nube:** la práctica de usar servidores remotos, aplicaciones y servicios de red alojados en Internet en lugar de en dispositivos físicos locales.

**Concatenación de cadenas:** el proceso de unir dos cadenas.

**Concatenación de listas:** el concepto de combinar dos listas en una colocando los elementos de la segunda lista directamente después de los elementos de la primera lista.

**Condición de bucle:** la parte de un bucle que determina cuándo termina el bucle.

**Confidencialidad:** la idea de que solo los usuarios autorizados pueden acceder a activos o datos específicos.

**Configuración de línea base (imagen de línea base):** conjunto documentado de especificaciones dentro de un sistema que se utiliza como base para futuras compilaciones, versiones y actualizaciones.

**Conjuntos de datos:** datos que consisten en una colección desordenada de valores únicos.

**Conmutador:** dispositivo que establece conexiones entre dispositivos específicos de una red enviando y recibiendo datos entre ellos.

**Consulta:** solicitud de datos de una tabla de una base de datos o de una combinación de tablas.

**Contención:** el acto de limitar y prevenir daños adicionales causados por un incidente.

**Continuidad del negocio:** la capacidad de una organización para mantener su productividad diaria mediante el establecimiento de planes de recuperación ante desastres de riesgo.

**Controles de acceso:** controles de seguridad que gestionan el acceso, la autorización y la responsabilidad de la información.

**Controles de seguridad:** son medidas de seguridad diseñadas para reducir riesgos de seguridad específicos.

**Cookie de sesión:** token que los sitios web utilizan para validar una sesión y determinar su duración.

**Cortafuegos basados en la nube:** cortafuegos de software que aloja el proveedor de servicios en la nube.

**Cortafuegos:** dispositivo de seguridad de red que monitorea el tráfico hacia o desde una red.

**Criptografía:** el proceso de transformar información en una forma que los lectores no deseados no puedan entender.

**Crowdsourcing:** la práctica de recopilar información utilizando las aportaciones y la colaboración del público.

**Cryptojacking:** una forma de malware que instala software para minar criptomonedas ilegalmente.

**Cuaderno:** interfaz en línea para escribir, almacenar y ejecutar código.

**Cumplimiento:** proceso de adherirse a las normas internas y reglamentos externos.

**Custodio de datos:** cualquier persona o cualquier cosa que sea responsable del manejo, transporte y almacenamiento seguros de la información.

D

**Datos booleanos:** datos que solo pueden ser uno de dos valores: Verdadero o Falso.

**Datos de diccionario:** datos que consisten en uno o más pares clave-valor**.**

**Datos de fecha y hora:** datos que representan una fecha y/o una hora.

**Datos de lista:** estructura de datos que consiste en una colección de datos en forma secuencial.

**Datos de red:** los datos que se transmiten entre los dispositivos de una red.

**Datos de tupla:** datos que consisten en una colección de datos que no se pueden modificar.

**Datos en reposo:** datos a los que no se está accediendo actualmente.

**Datos en tránsito:** datos que viajan de un punto a otro.

**Datos en uso:** datos a los que acceden uno o más usuarios.

**Datos enteros:** datos formados por un número sin punto decimal.

**Datos flotantes:** datos formados por un número con un punto decimal.

**Datos numéricos:** datos formados por números.

**Datos:** información que es traducida, procesada o almacenada por una computadora.

**Defensa en profundidad:** un enfoque por capas para la gestión de vulnerabilidades que reduce el riesgo.

**Depuración:** la práctica de identificar y corregir errores en el código.

**Depurador:** herramienta de software que ayuda a localizar la fuente de un error y evaluar sus causas.

**Detección activa de paquetes:**  tipo de ataque en el que los paquetes de datos se manipulan en tránsito.

**Detección de paquetes:** la práctica de capturar e inspeccionar paquetes de datos a través de una red**.**

**Detección pasiva de paquetes:** tipo de ataque en el que un actor malicioso se conecta a un concentrador de red y observa todo el tráfico de la red.

**Detección y respuesta de puntos de conexión (EDR):** aplicación que monitorea un punto de conexión para detectar actividad maliciosa**.**

**Detección:** el rápido descubrimiento de eventos de seguridad.

**Detectar:** una función central del NIST relacionada con la identificación de posibles incidentes de seguridad y la mejora de las capacidades de monitoreo para aumentar la velocidad y la eficiencia de las detecciones**.**

**Día cero:** exploit que antes era desconocido.

**Diario del gestor de incidentes:** una forma de documentación utilizada en la respuesta a incidentes.

**Dirección de control de acceso al medio (MAC):** identificador alfanumérico único que se asigna a cada dispositivo físico de una red.

**Dirección de protocolo de Internet (IP):** cadena única de caracteres que identifica la ubicación de un dispositivo en Internet.

**Directorio raíz:** el directorio de más alto nivel en Linux.

**Directorio:** archivo que organiza donde se almacenan otros archivos.

**Disco duro:** componente de hardware utilizado para la memoria a largo plazo**.**

**Disponibilidad:** la idea de que los datos son accesibles para aquellos que están autorizados a acceder a ellos.

**Dispositivos periféricos:** componentes de hardware conectados y controlados por el sistema informático.

**Distribuciones:** las diferentes versiones de Linux.

**Documentación:** cualquier forma de contenido grabado que se utiliza para un propósito específico.

E

**Elevator pitch:** breve resumen de la experiencia, las habilidades y los antecedentes de una persona.

**Encapsulación:** un proceso realizado por un servicio VPN que protege tus datos al encapsular datos confidenciales en otros paquetes de datos.

**Endurecimiento de la seguridad:** proceso de refuerzo de un sistema para reducir sus vulnerabilidades y su superficie de ataque.

**Enrutador (o router):** dispositivo de red que conecta varias redes entre sí.

**Entorno de desarrollo integrado (IDE):** aplicación informática para escribir código que proporciona asistencia para la edición y herramientas de corrección de errores.

**Entrada estándar:** información recibida por el sistema operativo a través de la línea de comandos.

**Equipos de respuesta a incidentes de seguridad informática (CSIRT):** grupo especializado de profesionales de la seguridad formados en gestión y respuesta a incidentes.

**Erradicación:** la eliminación completa de los elementos incidentes de todos los sistemas afectados.

**Error de sintaxis:** un error que implica un uso no válido de un lenguaje de programación.

**Error de tipo:** un error que resulta de usar el tipo de datos incorrecto.

**Error estándar:** mensaje de error devuelto por el sistema operativo a través del intérprete de comandos.

**Error lógico:** error que resulta cuando la lógica utilizada en el código produce resultados no deseados.

**Escalada de incidentes**: el proceso de identificar un posible incidente de seguridad, clasificarlo y derivarlo a un miembro del equipo con más experiencia.

**Escáner de vulnerabilidades:** software que compara automáticamente las vulnerabilidades y exposiciones comunes existentes, o CVE, con las tecnologías de la red.

**Estándar de jerarquía del sistema de archivos (FHS):** el componente del sistema operativo Linux que organiza los datos.

**Estándares de seguridad de datos de la industria de tarjetas de pago (PCI DSS):** todos los datos de titulares de tarjetas que una organización acepta, transmite o almacena.

**Estándares:** referencias que informan cómo establecer políticas.

**Ética de la seguridad:** pautas para tomar decisiones apropiadas como profesional de la seguridad.

**Evaluación de vulnerabilidades:** proceso de revisión interna de los sistemas de seguridad de una organización.

**Evaluación:** el quinto paso del NIST RMF que significa determinar si los controles establecidos se implementan correctamente.

**Evento:** una ocurrencia observable en una red, sistema o dispositivo.

**Excepción:** un error que involucra código que no se puede ejecutar aunque sea sintácticamente correcto.

**Exfiltración de datos:** transmisión no autorizada de datos desde un sistema.

**Exploit:** una forma de aprovecharse de una vulnerabilidad.

**Exploits basados en la web:** código o comportamiento malicioso que se utiliza para aprovechar las fallas de codificación en una aplicación web.

**Exposición:** un error que puede ser aprovechado por una amenaza.

**Expresión regular (regex):** secuencia de caracteres que forma un patrón.

F

**Falso negativo**: estado en el que no se detecta la presencia de una amenaza.

**Falso positivo:** alerta que detecta erróneamente la presencia de una amenaza.

**Filtrado de puertos:** función del cortafuegos que bloquea o permite que ciertos números de puerto limiten la comunicación no deseada.

**Filtrado:** selección de datos que cumplen una determinada condición.

**Firma:** patrón asociado a una actividad maliciosa**.**

**Formato de evento común (CEF):** un formato de registro que utiliza pares clave-valor para estructurar los datos e identificar los campos y sus valores correspondientes.

**Función definida por el usuario:** función que los programadores diseñan para sus necesidades específicas.

**Función hash:** algoritmo que produce un código que no se puede descifrar.

**Función incorporada:** una función que existe dentro de Python y se puede llamar directamente.

**Función:** sección de código que se puede reutilizar en un programa.

G

**Gestión de activos:** el proceso de seguimiento de los activos y los riesgos que los afectan.

**Gestión de identidad y acceso (IAM):** conjunto de procesos y tecnologías que ayuda a las organizaciones a gestionar las identidades digitales en su entorno.

**Gestión de registros:** proceso de recopilación, almacenamiento, análisis y eliminación de datos de registro.

**Gestión de vulnerabilidades:** el proceso de encontrar y corregir vulnerabilidades.

**Gestor de paquetes:** herramienta que ayuda a los usuarios a instalar, gestionar y eliminar paquetes o aplicaciones.

**Gobernanza de seguridad:** prácticas que ayudan a apoyar, definir y dirigir los esfuerzos de seguridad de una organización.

**Guía de estilo PEP 8:** un recurso que proporciona directrices de estilo para los programadores que trabajan en Python.

**Guía de estilo:** manual que informa sobre la redacción, el formato y el diseño de los documentos.

**Gusanos:** malware que puede duplicarse y propagarse por sí mismo en los sistemas.

H

**Habilidades técnicas:** habilidades que requieren conocimiento de herramientas, procedimientos y políticas específicas.

**Habilidades transferibles:** habilidades de otras áreas que pueden aplicarse a diferentes carreras.

**Hacker:** cualquier persona o grupo que utiliza computadoras para obtener acceso no autorizado a los datos.

**Hacktivista:** persona que utiliza el hacking para lograr un objetivo político.

**Hardware interno:** los componentes necesarios para que funcione la computadora.

**Hardware:** componentes físicos de una computadora.

**Honeypot:** sistema o recurso creado como señuelo vulnerable a ataques con el fin de atraer a posibles intrusos.

**Hub:** dispositivo de red que transmite información a todos los dispositivos de la red.

I

**Identificador de sesión:** un token único que identifica a un usuario y su dispositivo mientras accede a un sistema.

**Identificar:** una función central del NIST relacionada con la gestión del riesgo de ciberseguridad y su efecto sobre las personas y los activos de una organización.

**IEEE 802.11 (WiFi):** conjunto de estándares que definen la comunicación para LAN inalámbricas.

**Implementación:** cuarto paso del NIST RMF, que consiste en aplicar los planes de seguridad y privacidad de una organización.

**Incidente:** suceso que pone en peligro de forma real o inminente, sin autoridad legal, la confidencialidad, integridad o disponibilidad de la información o de un sistema de información; o que constituye una infracción o amenaza inminente de infracción de la ley, las políticas de seguridad, los procedimientos de seguridad o las políticas de uso aceptable.

**Indicadores de ataque (IoA):** serie de eventos observados que indican un incidente en tiempo real.

**Indicadores de compromiso (IoC):** evidencia observable que sugieren indicios de un posible incidente de seguridad.

**Índice:** número asignado a cada elemento de una secuencia que indica su posición.

**Infección por malware**: tipo de incidente que ocurre cuando un software malicioso diseñado para perturbar un sistema se infiltra en las computadoras o la red de una organización.

**Información de identificación personal (PII):** cualquier información que pueda usarse para deducir la identidad de una persona.

**Información de identificación personal sensible (SPII):** un tipo específico de PII que se rige por pautas de manejo más estrictas.

**Información de salud protegida (PHI):** información que se relaciona con la salud, o con la condición física o mental pasada, presente o futura de un individuo.

**Información de seguridad y gestión de eventos (SIEM)**: aplicación que recopila y analiza datos de registro para monitorear actividades críticas en una organización.

**Informe final:** documentación que proporciona una revisión exhaustiva de un incidente.

**Infraestructura de clave pública (PKI):** marco de cifrado que garantiza la seguridad del intercambio de información en línea.

**Ingeniería social física:** ataque en el que el actor de amenazas se hace pasar por un empleado, cliente o proveedor para obtener acceso no autorizado a una ubicación física.

**Ingeniería social:** técnica de manipulación que se aprovecha del error humano para obtener información privada, acceso u objetos de valor.

**Inicio de sesión único (SSO):** tecnología que combina varios inicios de sesión diferentes en uno solo.

**Inmutable:** objeto que no se puede modificar después de que se crea y se le asigna un valor.

**Instrucción preparada:** técnica de codificación que ejecuta instrucciones SQL antes de pasarlas a una base de datos.

**Integridad:** idea de que los datos son correctos, auténticos y fiables.

**Inteligencia artificial (IA) antagónica:** técnica que manipula la inteligencia artificial (IA) y la tecnología de aprendizaje automático (ML) para realizar ataques de manera más eficiente.

**Inteligencia de fuentes abiertas (OSINT):** recopilación y análisis de información procedente de fuentes de acceso público para generar inteligencia utilizable.

**Inteligencia sobre amenazas:** información sobre amenazas basada en evidencia que proporciona contexto sobre amenazas existentes o emergentes.

**Interfaz de firmware extensible unificada (UEFI):** microchip que contiene instrucciones de carga para la computadora y reemplaza el BIOS en los sistemas más modernos.

**Interfaz de línea de comandos (CLI):** interfaz de usuario basada en texto que utiliza comandos para interactuar con la computadora.

**Interfaz de usuario:** programa que permite al usuario controlar las funciones del sistema operativo.

**Interfaz gráfica de usuario (GUI):** interfaz de usuario que utiliza íconos en la pantalla para gestionar las distintas tareas de la computadora.

**Intérprete:** programa informático que traduce el código Python en instrucciones ejecutables línea por línea.

**Inundación del protocolo de mensajes de control de Internet (inundación ICMP):** tipo de ataque DoS realizado por un atacante que envía repetidamente paquetes ICMP a un servidor de red.

**Inventario de activos:** catálogo de activos que deben protegerse.

**Inyección SQL:** ataque que ejecuta consultas inesperadas en una base de datos.

K

**KALI LINUX™:** una distribución de código abierto de Linux que se usa ampliamente en la industria de la seguridad.

**Kernel:** el componente del sistema operativo Linux que administra los procesos y la memoria.

**Kit de phishing:** conjunto de herramientas de software necesarias para lanzar una campaña de phishing.

L

**Lenguaje de procesamiento de búsqueda (SPL)**: lenguaje de consulta de Splunk.

**Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA):** ley federal de los Estados Unidos establecida para proteger la información de salud de los pacientes.

**Linux:** sistema operativo de código abierto.

**Lista de vulnerabilidades y exposiciones comunes (CVE®):** un diccionario de vulnerabilidades y exposiciones conocidas de libre acceso.

M

**Malware sin archivos:** malware que no necesita ser instalado por el usuario porque utiliza programas legítimos que ya están instalados para infectar un equipo.

**Malware:** software diseñado para perjudicar dispositivos o redes.

**Manual de actuación:** manual que proporciona detalles sobre cualquier acción operativa.

**Marco de Ciberseguridad (CSF) del Instituto Nacional de Estándares y Tecnología (NIST):** marco de adhesión voluntaria que incluye estándares, pautas y prácticas recomendadas para gestionar el riesgo para la ciberseguridad.

**Marcos de seguridad:** pautas utilizadas para crear planes que ayuden a mitigar el riesgo y las amenazas a los datos y la privacidad.

**Matriz:** tipo de datos que almacena los datos en una lista ordenada separada por comas.

**Memoria de acceso aleatorio (RAM):** componente de hardware utilizado para la memoria a corto plazo**.**

**Mentalidad de seguridad:** capacidad de evaluar el riesgo y buscar e identificar constantemente la vulneración potencial o real de un sistema, aplicación o datos.

**Método STAR:** técnica utilizada para responder a preguntas de entrevista conductuales y situacionales.

**Método:** función que pertenece a un tipo de datos específico.

**Métricas:** atributos técnicos clave, como el tiempo de respuesta, la disponibilidad y la tasa de fallos, que se utilizan para evaluar el rendimiento de una aplicación de software.

**MITRE:** conjunto de centros de investigación y desarrollo sin fines de lucro.

**Modelado de amenazas:** proceso de identificación de activos, sus vulnerabilidades y cómo cada uno de ellos está expuesto a las amenazas**.**

**Modelo de interconexión de sistemas abiertos (OSI):** concepto estandarizado que describe las siete capas que las computadoras utilizan para comunicarse y enviar datos a través de la red.

**Modelo TCP/IP:** marco utilizado para visualizar cómo se organizan y transmiten los datos a través de una red.

**Módem:** dispositivo que conecta el router a Internet y proporciona acceso a Internet a la LAN.

**Módulo**: archivo de Python que contiene funciones adicionales, variables, clases y cualquier tipo de código ejecutable.

**Monitoreo**: séptimo paso del NIST RMF que significa ser consciente de cómo funcionan los sistemas.

N

**Nano:** editor de archivos de línea de comandos disponible por defecto en muchas distribuciones de Linux.

**No repudio:** concepto según el cual no se puede negar la autenticidad de una información.

**Normativa:** reglas establecidas por un gobierno u otra autoridad para controlar la forma en que se hace algo.

**Notación entre corchetes:** los índices entre corchetes.

O

**OAuth:** un protocolo de autorización de estándar abierto que comparte el acceso designado entre aplicaciones.

**Objeto:** un tipo de datos que almacena datos en una lista separada por comas de pares clave-valor.

**Opciones:** entrada que modifica el comportamiento de un comando.

**Open Web Application Security Project (OWASP):** organización sin fines de lucro centrada en mejorar la seguridad del software.

**Operador exclusivo**: operador que no incluye el valor de comparación.

**Operador inclusivo:** operador que incluye el valor de comparación**.**

**Operador:** símbolo o palabra clave que representa una operación.

**Orden de volatilidad:** secuencia que describe el orden de los datos que deben conservarse, desde el primero hasta el último**.**

**Orquestación, automatización y respuesta de seguridad (SOAR):** conjunto de aplicaciones, herramientas y flujos de trabajo que utilizan la automatización para responder a incidentes de seguridad.

**OWASP Top 10:** documento de concientización estándar reconocido a nivel mundial que enumera los 10 riesgos de seguridad más críticos para las aplicaciones web.

P

**Paquete de datos:** una unidad básica de información que viaja de un dispositivo a otro dentro de una red.

**Paquete:** fragmento de software que se puede combinar con otros paquetes para formar una aplicación**.**

**Par clave-valor:** un conjunto de datos que representa dos elementos vinculados: una clave y su valor correspondiente.

**Parámetro (Python):** un objeto que se incluye en la definición de una función para su uso en esa función.

**Parrot:** una distribución de código abierto que se utiliza comúnmente para la seguridad.

**Parte interesada:** individuo o grupo que tiene interés en alguna decisión o actividad de una organización**.**

**Permisos:** tipo de acceso concedido a un archivo o directorio.

**Phishing de redes sociales:** tipo de ataque en el que un actor de amenazas recopila información detallada de su objetivo en sitios de redes sociales antes de iniciar el ataque.

**Phishing:** uso de comunicaciones digitales para engañar a las personas para que revelen datos confidenciales o implementen software malicioso.

**Ping de la muerte:** un tipo de ataque DoS causado cuando un hacker hace ping a un sistema enviándole un paquete ICMP sobredimensionado de más de 64 KB.

**Plan de continuidad del negocio (BCP):** documento que describe los procedimientos para mantener las operaciones comerciales durante y después de una interrupción significativa**.**

**Plan de respuesta a incidentes:** documento que describe los procedimientos a seguir en cada paso de la respuesta a un incidente.

**Política de escalamiento:** conjunto de acciones que describen a quién se debe notificar cuando se produce una alerta de incidente y cómo se debe manejar ese incidente.

**Política:** conjunto de reglas que reducen el riesgo y protegen la información.

**Postura de seguridad:** capacidad de una organización para administrar la defensa de sus activos y datos críticos y reaccionar ante los cambios.

**Preparación:** el primer paso del NIST RMF relacionado con las actividades necesarias para gestionar los riesgos de seguridad y privacidad antes de que se produzca una infracción.

**Principio de mínimo privilegio:** el concepto de conceder solo el acceso y la autorización mínimos necesarios para completar una tarea o función.

**Privacidad de la información:** protección contra el acceso y la difusión no autorizados de datos.

**Privilegio:** cualquier autoridad para realizar cambios en un sistema informático.

**Procedimientos:** instrucciones paso a paso para realizar una tarea de seguridad específica.

**Proceso de simulación de ataques y análisis de amenazas (PASTA):** un popular marco de modelado de amenazas que se utiliza en muchas industrias.

**Programación:** proceso que se puede usar para crear un conjunto específico de instrucciones para que una computadora ejecute tareas**.**

**Propietario de los datos:** la persona que decide quién puede acceder, editar, usar o destruir su información.

**Protección de la privacidad:** acto de salvaguardar la información personal del uso no autorizado.

**Protección y preservación de la evidencia:** proceso de trabajar adecuadamente con evidencia digital frágil y volátil.

**Protección:** una función central del NIST utilizada para proteger a una organización a través de la implementación de políticas, procedimientos, capacitación y herramientas que ayudan a mitigar las amenazas a la ciberseguridad.

**Protocolo de control de transmisión (TCP):** protocolo de comunicación de Internet que permite a dos dispositivos establecer una conexión y transmitir datos.

**Protocolo de datagramas de usuario (UDP):** protocolo sin conexión que no establece una conexión entre dispositivos antes de las transmisiones.

**Protocolo de Internet (IP):** conjunto de estándares utilizados para enrutar y direccionar paquetes de datos a medida que viajan entre dispositivos en una red.

**Protocolo de mensajes de control de Internet (ICMP):** protocolo de Internet que utilizan los dispositivos para informarse mutuamente sobre los errores de transmisión de datos a través de la red**.**

**Protocolo de resolución de direcciones (ARP):** protocolo de red utilizado para determinar la dirección MAC del siguiente enrutador o dispositivo a atravesar.

**Protocolo de transferencia de hipertexto (HTTP):** protocolo de capa de aplicación que proporciona un método de comunicación entre clientes y servidores de sitios web.

**Protocolo seguro de transferencia de archivos (SFTP):** un protocolo seguro utilizado para transferir archivos de un dispositivo a otro a través de una red**.**

**Protocolo seguro de transferencia de hipertexto (HTTPS):** protocolo de red que proporciona un método seguro de comunicación entre clientes y servidores de sitios web.

**Protocolo simple de administración de red (SNMP):** protocolo de red utilizado para monitorear y administrar los dispositivos de una red**.**

**Protocolos de red:** conjunto de reglas utilizadas por dos o más dispositivos de una red para describir el orden de entrega y la estructura de los datos.

**Prueba de penetración (pen test):** ataque simulado que ayuda a identificar vulnerabilidades en sistemas, redes, sitios web, aplicaciones y procesos.

**Publicación Especial (SP) del Instituto Nacional de Estándares y Tecnología (NIST) 800-53:** marco unificado para proteger la seguridad de los sistemas de información dentro del gobierno federal de los EE. UU.

**Puerto:** ubicación basada en software que organiza el envío y la recepción de datos entre dispositivos de una red.

**Punto de conexión (endpoint):** cualquier dispositivo conectado a una red.

**Punto de datos:** elemento de información específico.

Q

**Quid pro quo:** un tipo de cebo utilizado para engañar a alguien haciéndole creer que será recompensado a cambio de compartir acceso, información o dinero.

R

**Ransomware:** ataque malicioso en el que los actores de amenazas cifran los datos de una organización y exigen un pago (rescate) para restablecer el acceso a ellos.

**Recompensas por errores:** programas que animan a los hackers autónomos a encontrar y notificar vulnerabilidades.

**Recuperación:** proceso por el que los sistemas afectados vuelven a funcionar con normalidad.

**Recuperar:** función central del NIST relacionada con el restablecimiento del funcionamiento normal de los sistemas afectados**.**

**Red de área extensa (WAN):** una red que abarca una gran área geográfica como una ciudad, un estado o un país.

**Red de área local (LAN):** red que abarca áreas pequeñas, como un edificio de oficinas, una escuela o un hogar.

**Red en la nube:** conjunto de servidores o computadoras que almacenan recursos y datos en centros de datos remotos a los que se puede acceder a través de Internet.

**Red Hat:** distribución de Linux por suscripción para uso empresarial.

**Red privada virtual (VPN):** servicio de seguridad de red que cambia tu dirección IP pública y enmascara tu ubicación virtual para que puedas mantener tus datos privados cuando utilizas una red pública como Internet.

**Red:** grupo de dispositivos conectados.

**Reducción del riesgo:** el proceso de disponer de los procedimientos y reglas adecuados para reducir rápidamente el impacto de un riesgo, como una infracción.

**Registro:** inventario de eventos que tienen lugar dentro de los sistemas de una organización.

**Registro:** registro de eventos que se producen en los sistemas y redes informáticos.

**Relación:** una relación amistosa en la que las personas involucradas entienden las ideas de los demás y se comunican bien entre sí.

**Resiliencia**: capacidad de prepararse, responder y recuperarse de las perturbaciones.

**Responsabilidad compartida:** la idea de que todas las personas de una organización asuman un papel activo en la reducción del riesgo y el mantenimiento de la seguridad física y virtual.

**Respuesta a incidentes:** intento rápido de una organización de identificar un ataque, contener los daños y corregir los efectos de una infracción de seguridad.

**Respuesta:** una función central del NIST relacionada con asegurarse de que se utilicen los procedimientos adecuados para contener, neutralizar y analizar incidentes de seguridad, e implementar mejoras en el proceso de seguridad.

**Reunión sobre las lecciones aprendidas:** reunión en la que participan todas las partes implicadas tras un incidente grave.

**Riesgo:** cualquier cosa que pueda afectar a la confidencialidad, integridad o disponibilidad de un activo.

**Rootkit**: malware que proporciona acceso remoto y administrativo a una computadora.

**Ruptura de la cadena de custodia:** inconsistencias en la recogida y registro de pruebas en la cadena de custodia.

**Ruta absoluta del archivo:** la ruta completa del archivo, que comienza en la raíz.

**Ruta de archivo relativa:** una ruta de archivo que comienza en el directorio actual del usuario.

**Ruta del archivo:** la ubicación de un archivo o directorio.

S

**Salida estándar:** información devuelta por el sistema operativo a través del intérprete de comandos.

**Salting:** una protección adicional que se utiliza para reforzar las funciones hash.

**Saneamiento de entradas:** programación que valida las entradas de usuarios y otros programas.

**Sangría:** espacio que se añade al principio de una línea de código.

**Scareware:** malware que emplea tácticas para asustar a los usuarios e infectar sus dispositivos.

**Secuencia de comandos en sitios cruzados (XSS):** ataque de inyección que inserta código en un sitio web o aplicación web vulnerable.

**Secuestro de sesión:** evento en el que los atacantes obtienen el identificador de sesión de un usuario legítimo.

**Secure Shell (SSH):** un protocolo de seguridad utilizado para crear un intérprete de comandos con un sistema remoto.

**Segmentación de red:** técnica de seguridad que divide la red en segmentos.

**Seguridad de la información (InfoSec):** la práctica de mantener los datos en todos los estados alejados de usuarios no autorizados.

**Seguridad de red:** la práctica de evitar accesos no autorizados a la infraestructura de red de una organización.

**Selección**: el tercer paso del NIST RMF que significa elegir, personalizar y capturar la documentación de los controles que protegen a una organización.

**Sentencia condicional:** sentencia que evalúa el código para determinar si cumple con un conjunto específico de condiciones.

**Sentencia iterativa:** código que ejecuta repetidamente un conjunto de instrucciones.

**Sentencia Return:** una sentencia Python que se ejecuta dentro de una función y envía información de vuelta a la llamada a la función.

**Separación de funciones:** el principio de que los usuarios no deben tener niveles de autorización que les permitan hacer un uso indebido de un sistema.

**Servidor proxy de reenvío:** servidor que regula y restringe el acceso de una persona a Internet.

**Servidor proxy inverso:** un servidor que regula y restringe el acceso de Internet a un servidor interno.

**Servidor proxy:** servidor que satisface las solicitudes de sus clientes reenviándolas a otros servidores.

**Sesión:** secuencia de solicitudes y respuestas de autenticación básica HTTP de red asociadas con el mismo usuario.

**Shell:** intérprete de línea de comandos.

**Sin estado:** clase de cortafuegos que funciona sobre la base de reglas predefinidas y que no realiza un seguimiento de la información de los paquetes de datos.

**Sintaxis:** las reglas que determinan lo que está correctamente estructurado en un lenguaje informático.

**Sistema básico de entrada/salida (BIOS):** microchip que contiene instrucciones de carga para la computadora y que predomina en los sistemas más antiguos.

**Sistema de detección de intrusiones (IDS):** aplicación que monitorea la actividad del sistema y alerta sobre posibles intrusiones.

**Sistema de detección de intrusos basado en host (HIDS):** aplicación que monitorea la actividad del host en el que está instalada.

**Sistema de detección de intrusos basado en la red (NIDS):** aplicación que recopila y monitorea el tráfico y los datos de la red.

**Sistema de nombres de dominio (DNS):** un protocolo de red que traduce los nombres de dominio de Internet en direcciones IP.

**Sistema de prevención de intrusiones (IPS):** aplicación que monitorea la actividad del sistema en busca de actividades intrusivas y toma medidas para detenerlas.

**Sistema de puntuación de vulnerabilidad común (CVSS):** sistema de medición que puntúa la gravedad de una vulnerabilidad.

**Sistema Operativo (SO)**: la interfaz entre el hardware de la computadora y el usuario.

**Sistema operativo heredado:** sistema operativo obsoleto pero que se sigue utilizando.

**Smishing**: uso de mensajes de texto para engañar a los usuarios con el fin de obtener información confidencial o hacerse pasar por una fuente conocida.

**Software antivirus:** programa de software utilizado para prevenir, detectar, y eliminar malware y virus.

**Spear phishing:** ataque por correo electrónico malicioso dirigido a un usuario o grupo de usuarios específico que parece provenir de una fuente confiable.

**Splunk Cloud:** herramienta alojada en la nube que se utiliza para recopilar, buscar y monitorear datos de registro.

**Splunk Enterprise:** herramienta autoalojada utilizada para retener, analizar y buscar los datos de registro de una organización para proporcionar información de seguridad y alertas en tiempo real.

**Spyware:** malware que se usa para recabar y vender información sin el consentimiento de los propietarios de esta.

**SQL (lenguaje de consulta estructurado):** lenguaje de programación utilizado para crear, interactuar y solicitar información de una base de datos.

**Stateful:** clase de cortafuegos que realiza un seguimiento de la información que pasa a través de este y filtra proactivamente las amenazas.

**Subcadena:** secuencia continua de caracteres dentro de una cadena.

**Subnetting:** subdivisión de una red en grupos lógicos llamados subredes.

**Superficie de ataque:** todas las vulnerabilidades potenciales que un actor de amenazas podría explotar.

**Suplantación de IP:** un ataque de red realizado cuando un atacante cambia la IP de origen de un paquete de datos para hacerse pasar por un sistema autorizado y obtener acceso a una red.

**Suricata**: sistema de detección de intrusos de código abierto, sistema de prevención de intrusos y herramienta de análisis de redes.

T

**Tabla hash:** estructura de datos que se utiliza para almacenar y hacer referencia a los valores hash.

**Tabla Rainbow:** archivo de valores hash pregenerados y su texto plano asociado.

**Tailgating:** táctica de ingeniería social en la que personas no autorizadas siguen a una persona autorizada hasta una zona restringida.

**Tarjeta de interfaz de red (NIC):** hardware que conecta las computadoras a una red.

**tcpdump:** analizador de protocolos de red de línea de comandos.

**Telemetría:** recopilación y transmisión de datos para su análisis.

**Tipo de datos:** una categoría para un tipo particular de elemento de datos.

**Token de interfaz de programación de aplicaciones (API):** un pequeño bloque de código cifrado que contiene información sobre un usuario.

**Tráfico de red:** cantidad de datos que circulan por una red.

**Tríada de confidencialidad, integridad y disponibilidad (CIA):**  modelo que ayuda a informar sobre cómo tienen en cuenta el riesgo las organizaciones al configurar sistemas y políticas de seguridad.

**Triaje**: priorización de incidentes en función de su nivel de importancia o urgencia.

**Troyano:** malware que parece un archivo o programa legítimo.

U

**Ubuntu:** distribución de código abierto y fácil de usar que se emplea ampliamente en el sector de la seguridad y en otras industrias.

**Unidad central de procesamiento (CPU):** el procesador principal de una computadora, que se utiliza para realizar tareas informáticas generales en esta.

**USB baiting:** ataque en el que un actor de amenazas deja estratégicamente una unidad USB que contiene malware para que un empleado la encuentre y la instale, con el fin de causar la infección involuntaria de una red.

**Uso indebido:** tipo de incidente que se produce cuando un empleado de una organización infringe las políticas de uso aceptable de la organización.

**Usuario raíz (o superusuario):** usuario con privilegios elevados para modificar el sistema.

**Usuario:** la persona que interactúa con una computadora.

V

**Variable de bucle:** variable que se utiliza para controlar las iteraciones de un bucle.

**Variable global:** variable disponible en todo el programa.

**Variable local:** variable asignada dentro de una función.

**Variable:** contenedor que almacena datos.

**Vectores de ataque:** las vías que utilizan los atacantes para penetrar en las defensas de seguridad.

**Velocidad:** rapidez a la que se reciben o descargan paquetes de datos.

**Verdadero negativo:** estado en el que no se detecta actividad maliciosa.

**Verdadero positivo**: una alerta que detecta correctamente la presencia de un ataque.

**Virus informático:** código malicioso escrito para interferir con las operaciones informáticas, y causar daños a los datos y al software.

**Virus:** consulta “virus informático”.

**VirusTotal:** un servicio que permite a cualquier persona analizar archivos, dominios, URL y direcciones IP sospechosos en busca de contenido malicioso.

**Vishing:** explotación de la comunicación por voz electrónica para obtener información sensible o hacerse pasar por una fuente conocida.

**Vulnerabilidad:** debilidad que puede ser aprovechada por una amenaza.

**Vulneración de la seguridad:** acceso no autorizado a sistemas, aplicaciones, redes o dispositivos.

W

**Wireshark:** analizador de protocolos de red de código abierto.

Y

**YARA-L:** lenguaje informático utilizado para crear reglas de búsqueda en los datos de registro transferidos.

Z

**Zona controlada:** una subred que protege la red interna de la zona no controlada.

**Zona de seguridad:** segmento de la red de una empresa que protege la red interna de la Internet.

**Zona de seguridad:** segmento de la red de una empresa que protege la red interna de la Internet.

**Zona no controlada:** parte de la red que queda fuera de la organización.