### Términos y definiciones de la certificación

A

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

**Acceso Wi-Fi protegido (WPA):** Protocolo de seguridad para proteger las redes inalámbricas cuando un dispositivo busca conectarse a Internet.

**Actividad posterior a un incidente:** Proceso de revisión de un incidente para identificar áreas de mejora en la gestión.

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

**Actualización de parches:** Modificación de un programa o sistema operativo que soluciona vulnerabilidades de seguridad.

**Adware:** Tipo de software legítimo o malicioso que se utiliza para mostrar publicidad digital en las aplicaciones.

**Agente de amenaza:** Persona o grupo de personas que representa una amenaza intencional para computadoras, aplicaciones o redes.

**Algoritmo:** Conjunto de instrucciones definidas, ordenadas y acotadas para resolver un problema, realizar un cálculo o desarrollar una tarea.

**Algoritmo de cifrado:** Algoritmo que encripta la información.

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

**Amenaza externa:** Cualquier riesgo a la seguridadproducido fuera de la organización que tenga el potencial de dañar los activos de esta.

**Amenaza interna:** Riesgo a la seguridadproducido por una persona que pertenece o perteneció a una empresao tiene una relación directa o de confianza con ella.

**Amenaza persistente avanzada (APT):** Situación en la que un agente de amenaza accede sin autorización a un sistema y permanece en él durante un periodo de tiempo prolongado.

**Análisis:** Investigación y validación de alertas.

**Análisis basado en anomalías:** Método de detección que busca identificar comportamientos atípicos a partir del análisis de un conjunto de datos.

**Análisis de firmas (o análisis basado en firmas):** Método de detección que busca identificar eventos sospechosos o maliciosos.

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

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

**Análisis forense digital:** Práctica de recopilar y analizar datos para determinar quién y cómo llevó adelante un ataque.

**Análisis sintáctico de datos:** Proceso de conversión de datos a un formato más legible; esto permite que sea más fácil de analizar, utilizar o almacenar.

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

**Angler phishing:** Tipo de ataque de suplantación de identidad en el que un agente de amenaza se hace pasar por representante del servicio al cliente de una empresa en las redes sociales.

**Aplicación:** Programa que realiza una tarea específica.

**Aplicación potencialmente no deseada (PUA):** Tipo de software que se incluye con programas legítimos y que puede mostrar anuncios, causar la ralentización del dispositivo o instalar otro software no deseado.

**Aprovisionamiento de usuarios:** Proceso de creación, actualización, modificación o eliminación de cuentas o perfiles de usuarios.

**Árbol de ataque:** Diagrama que muestra las amenazas a los activos y cómo se relacionan entre sí.

**Archivo de libre escritura (World-writable file):** Archivo que puede ser alterado por cualquier persona.

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

**Archivo pcap, captura de paquetes**: Archivo que contiene paquetes de datos interceptados desde una interfaz o red.

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

**Argumento (Python):** Dato que se introduce en una función cuando se la llama.

**Arquitectura de seguridad:** Diseño de seguridad compuesto por múltiples herramientas y procesos, que se utiliza para proteger a una organización de los riesgos y amenazas externas.

**Array:** Tipo de dato estructurado que permite almacenar un conjunto de datos homogéneo, es decir, del mismo tipo y relacionados, en una lista ordenada separada por comas.

**Ataque a la cadena de suministro:** Ataque que se dirige a sistemas y aplicaciones de empresas desarrolladoras y proveedoras de hardware y/o software para localizar una vulnerabilidad en la que se pueda implementar malware.

**Ataque criptográfico:** Ataque que afecta las formas seguras de comunicación protegidas por un sistema criptográfico.

**Ataque de “caza de ballenas” (Whaling):** Tipo de ataque de suplantación de identidad dirigido específicamente a personas de alto rango de una organización.

**Ataque de “agujero de agua” (Watering hole)**: Tipo de ataque en el que un agente de amenaza 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 con una contraseña.

**Ataque de denegación de servicio (DoS):** Ataque dirigido a una red o servidor para inundarlo con tráfico de red para inhabilitar los sistemas y servicios informáticos de forma temporal.

**Ataque de denegación de servicio distribuido (DDoS):** Tipo de ataque de denegación de servicio que utiliza múltiples dispositivos o servidores situados en diferentes ubicaciones, para inundar la red de destino con tráfico no deseado.

**Ataque de fuerza bruta:** Proceso de ensayo y error que busca descubrir información privada, como, por ejemplo, una contraseña.

**Ataque de 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.

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

**Ataque de inyección:** Ataque mediante el cual se introduce un código malicioso en una aplicación vulnerable.

**Ataque de repetición:** Ataque a la red que consiste en interceptar un paquete de datos en tránsito para retrasarlo o repetirlo en otro momento.

**Ataque de secuencia de comandos en sitios cruzados, o entre sitios (XSS):** Tipo de ataque de inyección que consiste en insertar código en un sitio web o aplicación web vulnerables.

**Ataque de suplantación de identidad:** (Consultar **Phishing)**.

**Ataque de suplantación de identidad en redes sociales (**Consultar **Phishing en redes sociales).**

**Ataque de suplantación de IP:** Ataque de red que consiste en cambiar la IP de origen de un paquete de datos para hacerse pasar por un sistema autorizado y obtener acceso a una red.

**Ataque en ruta:** Ataque en el que un agente de amenaza se coloca en medio de una conexión autorizada e intercepta o altera datos en tránsito.

**Ataque físico:** Incidente de seguridad que afecta a los entornos digitales y físicos en donde se implementa.

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

**Ataque pitufo (smurf):** Tipo de ataque de denegación de servicioen el que un atacante detecta la dirección IP de un usuario autorizado y la inunda con paquetes ICMP.

**Ataque XSS almacenado:** Tipo de ataque en el que se inyecta un script o secuencia de código malicioso directamente en el servidor.

**Ataque XSS basado en DOM:** Tipo de ataque en el que se inyecta un código malicioso directamente en la página web que carga un navegador.

**Ataque XSS reflejado:** Tipo de ataque en el que se envía un script malicioso a un servidor que se activa durante la respuesta del mismo.

**Auditoría de seguridad**: Revisión de los controles, políticas y procedimientos de seguridad de una organización.

**Autenticación:** Proceso para verificar la identidad de una persona.

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

**Autenticación de múltiples factores o multifactor (MFA):** Medida de seguridad que exige a un usuario verificar su identidad en dos o más formas, para acceder a un sistema o red.

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

**Autoridad de numeración de CVE (CNA):** Organización que voluntariamente analiza y distribuye información sobre CVE elegibles.

**Autorización:** Proceso de determinar si un usuario autenticado tiene acceso a recursos específicos en un sistema.

**Autorizar:** Sexto paso del RMF del NIST que se refiere a asumir la responsabilidad de los riesgos de seguridad y privacidad que puedan existir en una organización.

B

**Base de datos:** Colección organizada de información o datos estructurados.

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

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

**Biblioteca:** Conjunto de módulos y paquetes accesibles que se utilizan para desarrollar programas.

**Biblioteca estándar de Python:** Conjunto de módulos y paquetes que se distribuyen junto con Python.

**Bit:** La unidad más pequeña de medición de datos en una computadora.

**Botnet:** Conjunto de computadoras infectadas por software malicioso (malware), que están bajo el control de un solo agente de amenaza, conocido como el “bot-herder”.

**Buena relación:** Vínculo entre las personas que permite un entendimiento mutuo de ideas y comunicación fluida.

C

**Caballo de Troya (troyano):** Software malicioso que parece un archivo o programa legítimo.

**Cadena de custodia digital:** Procedimiento documentado que permite constatar la posesión y el control de la evidencia obtenida durante el ciclo de vida de un incidente.

**Captura de paquetes:** (Consultar **Archivo pcap**).

**Cargador:** Código malicioso que se inicia después de que un usuario inicia un programa dropper.

**Cargador de arranque:** Programa que carga el sistema operativo de una computadora.

**Categorizar:** Segundo paso del Marco de Gestión de Riesgos (RMF) del NIST, que se lleva a cabo para desarrollar procesos y tareas de gestión de riesgos.

**Caza de amenazas:** Búsqueda proactiva de amenazas en una red.

**Cebo (Baiting):** Táctica de ingeniería social que incita a las personas a comprometer su seguridad.

**Cebo USB (USB Baiting):** Ataque que consiste en incluir un software malicioso (malware) en una memoria USB para que una persona la encuentre e infecte involuntariamente una red, al utilizarla.

**CentOS:** Distribución de código abierto (Linux) estrechamente relacionada con Red Hat.

**Centro de Operaciones de Seguridad (SOC, por sus siglas en inglés):** Unidad organizativa centralizada dedicada a monitorear redes, sistemas y dispositivos en busca de amenazas o ataques a la seguridad.

**Certificado digital:** Documento electrónico que verifica la identidad del titular de una clave pública.

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

**Ciberseguridad (o seguridad cibernética):** 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):** Marco para la respuesta a incidentes que consta de cuatro fases: preparación; detección y análisis; contención, erradicación y recuperación; y actividad posterior a un incidente.

**Cifrado (encriptación):** Proceso de convertir datos de un formato legible a uno codificado

**Cifrado asimétrico:** Sistema criptográfico que utiliza dos claves, una pública y otra privada, para cifrar y descifrar datos.

**Cifrado simétrico:** Sistema criptográfico que utiliza una única clave para cifrar y descifrar datos.

**Clasificación de activos:** Práctica de etiquetar los activos en función de cuán sensibles e importantes son para una organización.

**Clave criptográfica:** Secuencia de datos que descifra el texto cifrado o viceversa.

**Clave externa (o foránea):** Columna de una tabla que es clave primaria de otra tabla.

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

**Colisión de hash:** Situación en la que diferentes entradas comparten el mismo valor hash.

**Comando:** Instrucción que le indica a la computadora que haga algo.

**Comando y control (C2):** Servidor o computadora que utilizan los agentes de amenaza para mantener comunicaciones con los sistemas comprometidos. De esta manera, controlan los dispositivos infectados, extraen datos, entre otras acciones.

**Comentario:** Anotación que hacen los programadores para explicar el propósito del código, describir qué hace y por qué, de manera de hacerlo más entendible.

**Comodín:** Carácter especial que puede sustituir a cualquier otro.

**Compromiso de correo electrónico empresarial (BEC):** Tipo de ataque de suplantación de identidad, en el que un agente de amenaza se hace pasar por una persona conocida por la víctima e intenta que realice una acción, como enviar dinero u otorgar datos confidenciales de la compañía.

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

**Concatenación de cadenas:** Proceso de unir cadenas entre sí.

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

**Condición de bucle:** Parte de un bucle que determina cuándo termina.

**Confidencialidad:** Propiedad según la cual únicamente las personas autorizadas pueden acceder a activos o datos específicos.

**Conmutador de redes:** (Consultar **Switch**).

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

**Contención:** Acto de limitar que un incidente se extienda para prevenir los daños adicionales que pudiera causar.

**Continuidad del negocio:** Capacidad de una organización para seguir funcionando durante una interrupción no planificada del servicio.

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

**Controles de seguridad:** Pautas diseñadas para abordar y eliminar riesgos de seguridad específicos, como la alteración o la eliminación de información de perfiles, entre otros.

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

**Cortafuegos (Firewall):** Sistema de seguridad de red que monitorea el tráfico desde o hacia una red con el objetivo de filtrar el que es malicioso.

**Cortafuegos basado en la nube:** Tipo de cortafuegos alojado en la nube.

**Cortafuegos Stateful (gestión con estado):** Tipo de cortafuegos que realiza un seguimiento de la información que pasa a través de él y filtra proactivamente las amenazas.

**Criptografía:** (Consultar **Cifrado**).

**Crowdsourcing:** Práctica de colaboración colectiva que consiste en recopilar información con base en aportes del público, con el fin de resolver un problema o llevar adelante una tarea.

**Criptojacking:** Tipo de software malicioso que instala un programa para minar criptomonedas ilegalmente.

**Cuaderno (notebook)** Interfaz en línea para escribir, almacenar y ejecutar código.

**Cumplimiento normativo (Compliance):** Proceso de adherirse y cumplir con las normas y reglamentos internos y externos con el fin de proteger la información y los sistemas de una empresa.

**Custodio de datos:** Cualquier persona o entidad responsable del manejo, transporte y almacenamiento seguro de la información.

D

**Datos:** Información traducida, procesada o almacenada por una computadora.

**Datos biométricos:** Características físicas únicas que se pueden utilizar para verificar la identidad de una persona.

**Datos booleanos:** Tipo de datos que solo puede tener uno de dos valores, True (verdadero) o False (falso).

**Datos de cadena (o cadena):** En Python, conjunto de datos formado por una secuencia ordenada de caracteres.

**Datos confidenciales:** Datos a los que tiene acceso un número limitado de personas, y que su divulgación puede generar graves consecuencias para las personas u organizaciones.

**Datos de conjunto (o conjunto):** En Python, tipo de datos que consiste en una o más parejas clave-valor.

**Datos de diccionario (o diccionario):** En Python, tipo de datos que consiste en una o más parejas clave-valor.

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

**Datos de lista (o lista):** En Python,estructura de datos que consta de una colección de datos en forma secuencial.

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

**Datos de tupla (o tupla):** En Python, tipo de dato que consiste 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 se desplazan de un punto a otro.

**Datos en uso:** Datos a los que están accediendo uno o más usuarios.

**Datos enteros:** Tipo de datos formado por un número sin punto decimal.

**Datos float (de punto flotante):** Datos formados por un número con un punto decimal.

**Datos numéricos:** Tipo de datos cuyos valores son números.

**Datos privados**: Información que no se debe divulgar al público.

**Datos públicos**: Información que ya está a disposición del público y plantea un riesgo mínimo para la organización si es vista o compartida por otras personas.

**Datos sensibles**: Tipo de datos que incluye información de identificación personal (PII, por sus siglas en inglés), información de identificación personal sensible (SPII, por sus siglas en inglés) o información médica protegida (PHI, por sus siglas en inglés), y que requieren ser resguardados de posibles filtraciones.

**Defensa en profundidad:** Estrategia que consiste en usar varias medidas de seguridad en capas para proteger la integridad de la información y reducir el riesgo.

**Delegado de protección de datos (DPO):** Persona responsable de supervisar el cumplimiento normativo de los procedimientos de protección de datos de una organización**.**

**Depuración:** Práctica de identificar y corregir errores de código.

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

**Detección:** Descubrimiento oportuno de eventos de seguridad.

**Detección y respuesta de puntos de conexión (EDR):** Aplicación que monitorea los puntos de conexión para detectar actividad maliciosa.

**Detectar:** Función central del NIST relacionada con la identificación de posibles incidentes de seguridad y la mejora de las capacidades de monitoreo y respuesta.

**Día cero:** Vulnerabilidad recién descubierta.

**Diario de gestión de incidentes:** 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 conectado a Internet.

**Directorio:** Archivo que organiza la ubicación de otros archivos.

**Directorio raíz (o root):** Directorio de más alto nivel en Linux.

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

**Disponibilidad:** Propiedad según la cual todas las personas autorizadas pueden acceder a activos o datos específicos.

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

**Distribuciones:** Lasdiferentes versiones de Linux.

**Documentación:** Cualquier forma de contenido que se ha registrado para un propósito específico.

**Dropper:** Tipo de troyano que instala un programa o archivo malicioso en un equipo de destino.

E

**Elevator pitch:** Breve resumen de la experiencia, las habilidades y el contexto de una persona.

**Encapsulación:** Proceso ejecutado por un servicio VPN que protege datos confidenciales al encapsularlos en otros paquetes de datos.

**Encriptación:** (Consultar **Cifrado**).

**Enrutador (Router):** Dispositivo que conecta varias redes entre sí.

**Entorno de desarrollo integrado (IDE):** Aplicación informática para escribir código que proporciona asistencia para la edición, así como herramientas de corrección de errores.

**Entrada estándar:** Información recibida por el sistema operativo por medio 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:** Eliminación completa de los elementos de un incidente en todos los sistemas afectados.

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

**Error de tipo:** 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 tiene lugar cuando la lógica utilizada en un código produce efectos no deseados.

**Escalamiento de incidentes**: Proceso de identificar un posible incidente de seguridad, clasificarlo y entregárselo a un miembro del equipo con más experiencia.

**Escáner de vulnerabilidades:** Software diseñado para realizar análisis automáticos de cualquier aplicación, sistema o red en busca de vulnerabilidades.

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

**Estándar de Seguridad de Datos para la Industria de las Tarjetas de Pago (PCI-DSS):** Guía que define controles para la protección de los datos de titulares de tarjetas de pago y otros datos sensibles de autenticación, durante su procesamiento, almacenamiento y transmisión.

**Estándares:** Referencias sobre los objetivos y controles exigibles en lo referente a la seguridad de la información.

**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 en busca de posibles debilidades.

**Evaluar:** Quinto paso del Marco de Gestión de Riesgos (RMF) del NIST, para determinar si los controles establecidos se han implementado correctamente.

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

**Excepción:** 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:** Fragmento de software o secuencia de comandos que se aprovecha de un error o vulnerabilidad.

**Exploits basados en la web:** Fragmentos de software o secuencia de comandos que se aprovecha de un error o vulnerabilidad de codificación en una aplicación web.

**Exposición:** Error que puede ser aprovechado por un agente de amenaza.

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

F

**Falso negativo:** Resultado de un análisis que no detecta una amenaza existente y, por lo tanto, no activa una alerta.

**Falso positivo:** Resultado de un análisis que detecta erróneamente una amenaza y dispara una alerta, cuando no existe un incidente real.

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

**Filtrado de puertos:** Función del cortafuegos que bloquea o habilita determinados números de puerto, con el fin de limitar la comunicación no deseada.

**Firewall:** (Consultar **Cortafuegos**).

**Firma:** Patrón relacionado con una actividad maliciosa.

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

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

**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 integrada:** Función que se encuentra incorporada a Python, por lo cual se la puede llamar directamente.

G

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

**Gestión de eventos e información de seguridad (SIEM, por sus siglas en inglés)**: Solución de seguridad que recopila y analiza los datos de registro para monitorear actividades críticas en una organización.

**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:** Proceso de identificar, evaluar 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:** Manual que establece lineamientos sobre la redacción, el formato y el diseño de documentos.

**Guía de estilo PEP 8:** Recurso que proporciona directrices de estilo para los programadores que trabajan en Python, con el objetivo de que sea legible y consistente

**Guía operativa** (Consultar **Manual de estrategias**).

**Gusano:** Software malicioso que se reproduce por sí mismo y se propaga a través de los sistemas y redes.

H

**Habilidades técnicas:** Competencias que requieren el conocimiento de herramientas, políticas y procedimientos específicos.

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

**Hacker:** Cualquier persona o grupo de personas que utiliza computadoras para obtener acceso no autorizado a los datos. Se diferencia entre hacker ético, que es quien tiene como objetivo mejorar la seguridad y prevenir posibles ataques, y no ético o malintencionado, que es aquel que busca comprometer la seguridad de un sistema informático o de una red, con fines delictivos.

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

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

**Hardware interno:** Componentes necesarios para que funcione una computadora.

**Honeypot:** Sistema o recurso vulnerable a los ataques creado como señuelo para atraer a posibles intrusos.

**Host**: Toda computadora o máquina conectada a una red a través de un nombre y número de IP determinados. Proporciona recursos, información y servicios a los usuarios.

**Hub:** Dispositivo de red que transmite información a todos los dispositivos de esa red.

I

**Identificador de sesión (ID de sesión):** Token único que identifica a un usuario y su dispositivo mientras accede a un sistema**.**

**Identificar:** Función esencial 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 (Wi-Fi):** Conjunto de estándares que definen la comunicación para redes locales inalámbricas.

**Implementar:** Cuarto paso del Marco de Gestión de Riesgos (RMF) del NIST, que consiste en aplicar planes de seguridad y privacidad en una organización.

**Incidente:** Acontecimiento 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 violación o amenaza inminente de violación 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 sugiere 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 tiene lugar 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, por sus siglas en inglés):** Cualquier información que pueda usarse para deducir la identidad de una persona.

**Información de identificación personal sensible (SPII, por sus siglas en inglés):** Tipo específico de información personal identificable que se rige por pautas de manejo más estrictas.

**Información médica protegida (PHI, por sus siglas en inglés):** Cualquier información relacionada con la salud, o la condición física o mental pasada, presente o futura de una persona**.**

**Informe final:** Documento que se crea al término de un incidente, para proporcionar una revisión integral y exhaustiva del mismo.

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

**Ingeniería social:** Técnica de manipulación que busca engañar a las personas con el fin de que revelen información o realicen determinadas acciones.

**Ingeniería social física:** Ataque en el que un agente de amenaza se hace pasar por una persona ligada a la empresa para obtener acceso no autorizado a una ubicación física.

**Inicio de sesión único (SSO):**. Solución que permite a los usuarios iniciar sesión en varias aplicaciones, sitios o sistemas con una única autenticación de usuario.

**Integridad:** Cualidad que identifica a los datos como correctos, auténticos y confiables.

**Inteligencia artificial (IA) antagónica (o adversativa):** Técnica que manipula la inteligencia artificial y el aprendizaje automático para realizar ataques más eficientes.

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

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

**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 a un usuario controlar las funciones de un sistema operativo.

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

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

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

**Inventario de activos:** Catálogo de elementos valiosos que se deben proteger.

**Inyección SQL:** Tipo de ataque que consiste en ejecutar consultas maliciosas, con el fin de manipular una base de datos y acceder a la información.

K

**Kali Linux ™:**  Distribución de código abierto de Linux que se usa ampliamente en el sector de la seguridad.

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

**Kit de phishing:** Conjunto de herramientas de software, preparado para lanzar una campaña de phishing con facilidad.

L

**Lenguaje de procesamiento de búsqueda:** (Consultar **Search Processing Language**).

**Ley de Transferencia y Responsabilidad de los Seguros Médicos (HIPAA):** Ley federal de los Estados Unidos establecida para proteger la información de salud de los pacientes.

**Línea base de configuración:** Conjunto documentado de especificaciones dentro de un sistema que se utiliza como base para futuras compilaciones, versiones y actualizaciones.

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

**Lista de vulnerabilidades y exposiciones comunes (CVE®):** Listado de vulnerabilidades y exposiciones conocidas divulgadas públicamente.

M

**Malware:** (Consultar **Software malicioso**)**.**

**Malware sin archivos:** (Consultar **Software malicioso sin archivos**).

**Manual de estrategias:** Guía que proporciona detalles sobre cualquier acción operativa.

**Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST por sus siglas en inglés):** Marco de adhesión voluntaria creado en los Estados Unidos, que incluye estándares, pautas y prácticas recomendadas para gestionar los riesgos de 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 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:** Función que pertenece a un tipo de datos específico.

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

**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 creado en los Estados Unidos, con el fin de buscar soluciones a posibles amenazas a la ciberseguridad.

**Modelado de amenazas:** Proceso de identificación de activos, sus vulnerabilidades y su exposición a las amenazas, con el objetivo de planificar y optimizar las operaciones de seguridad de la red.

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

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

**Módem:** Dispositivo que conecta el enrutador (router) a Internet y proporciona acceso a Internet a la red de área local (LAN).

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

**Monitorear**: Séptimo paso del Marco de Gestión de Riesgos (RMF) del NIST, que consiste en evaluar cómo están funcionando 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.

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

**Notación entre corchetes:** Índices escritos entre corchetes.

O

**OAuth “Open Authorization” (Autorización abierta):** Protocolo de autorización de estándar abierto que comparte el acceso designado entre aplicaciones.

**Objeto:** Tipo de datos, en JavaScript, que almacena datos en una lista separada por comas de parejas clave-valor.

**Objeto inmutable:** Objeto que no se puede modificar después de que se crea y se le asigna un 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 de software.

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

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

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

**Orden:** Instrucción que le indica a la computadora que haga algo.

**Orden de volatilidad:** Secuencia que establece el orden en que deben conservarse los datos, del primero al último, en relación al tiempo en que estarán disponibles.

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

**OWASP Top 10:** Documento de concientización estándar reconocido en todo el mundo que enumera los diez riesgos de seguridad más críticos para las aplicaciones web, según la Fundación OWASP.

P

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

**Paquete de datos:** Unidad básica de información que se desplaza de un dispositivo a otro dentro de una red.

**Panel de control visual:** Forma de mostrar con rapidez diversos tipos de datos en un solo lugar.

**Parámetro (Python):** Objeto que se incluye en la definición de una función para ser utilizado en esa función.

**Parche de actualización:** (Consultar **Actualización de parches**).

**Pareja clave-valor:** Conjunto de datos que representa dos elementos vinculados, una clave y su valor correspondiente.

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

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

**Permisos:** Tipo de acceso concedido para un archivo o directorio.

**Phishing (suplantación de identidad):** Uso de comunicaciones digitales en las que se suplanta la identidad de una persona o empresa con el objetivo de engañar a otras personas para que revelen datos confidenciales o implementen un software malicioso.

**Phishing en redes sociales (suplantación de identidad en redes sociales):** Tipo de ataque en el que el agente de amenaza contacta a la víctima en alguna red social, con el fin de robar información personal o tomar el control de la cuenta.

**Phishing localizado (Spear phishing):** Ataque por correo electrónico malicioso dirigido a una persona o grupo de personas específico que parece provenir de una fuente confiable.

**Ping:** Herramienta de la línea de comandos de prácticamente cualquier sistema operativo (por ejemplo, Windows y Linux) que posea conectividad a red. Se utiliza para probar la posibilidad de acceder a un dispositivo a través de la red. El comando Ping envía una solicitud a un dispositivo específico mediante el uso del protocolo ICMP.

**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 recuperación ante desastres:** Enfoque estructurado y documentado que describe los pasos a seguir para minimizar el impacto de un incidente de seguridad.

**Plan de respuesta a incidentes:** Documento que describe paso a paso los procedimientos a seguir en caso de que ocurra un incidente.

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

**Política de escalamiento:** Conjunto de acciones que describen a quién se debe notificar cuando se produce una alerta por un incidente y cómo se debe manejar dicho incidente.

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

**Preparar:** Primer paso del Marco de Gestión de Riesgos (RMF) del NIST, relacionado con las actividades necesarias para gestionar los riesgos de seguridad y privacidad antes de que se produzca una vulneración.

**Principio de mínimo privilegio:** Concepto de conceder únicamente 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:** Condición que determina las acciones que un usuario puede realizar en un sistema informático.

**Procedimiento:** Instrucciones paso a paso para realizar una tarea de seguridad específica.

**Proceso de simulación de ataques y análisis de amenazas (PASTA):** Metodología de modelado de amenazas de uso común en numerosas industrias.

**Programación:** Proceso que permite crear un conjunto específico de instrucciones para que una computadora ejecute tareas.

**Propietario de datos:** Persona que tiene la potestad de decidir quién puede acceder a su información, editarla, usarla o destruirla.

**Protección de la privacidad:** Acto de proteger la información personal de usos no autorizados**.**

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

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

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

**Protocolo de control de transmisión (TCP) 3-way handshake:** Proceso de tres pasos utilizado para establecer una conexión autenticada entre dos dispositivos en una red.

**Protocolo de datagramas de usuario (UDP):** Protocolo de transmisión que no establece una conexión entre dispositivos.

**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 utilizado para determinar la dirección MAC del siguiente router o dispositivo a atravesar.

**Protocolo de transferencia de hipertexto (HTTP):** Protocolo de red que se utiliza para la comunicación entre clientes y servidores de sitios web.

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

**Protocolo seguro de transferencia de archivos (SFTP):** 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 Estados Unidos.

**Puerto:** Interfaz a través de la cual se pueden enviar y recibir los diferentes tipos de datos.

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

**Punto de dato:** Elemento de información específico.

Q

**Quid pro quo:** Tipo de cebo utilizado para engañar a una persona y hacerle creer que será recompensada si comparte un acceso, información o dinero.

R

**Ransomware:** (Consultar **Secuestro de datos**)**.**

**Rastreo activo de paquetes:** Tipo de ataque en el que los paquetes de datos se manipulan durante su tránsito.

**Rastreo de paquetes (packet sniffing):** Práctica de capturar e inspeccionar paquetes de datos a través de una red.

**Rastreo pasivo de paquetes:** Tipo de ataque en el que un agente de amenaza se conecta a un hub de red y observa todo el tráfico.

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

**Recuperación:** Proceso tras el cual 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:** Grupo de dispositivos conectados.

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

**Red de área local (LAN):** Red que abarca un área geográfica de gran tamaño, como una ciudad, un estado o un país.

**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):** Tecnología de seguridad de red que cambia la dirección IP pública y enmascara su ubicación para establecer una conexión segura en Internet.

**Reducción del riesgo:** Proceso de disponer de procedimientos y reglas adecuadas para reducir rápidamente el impacto de cualquier amenaza, por ejemplo, una brecha.

**Reforzamiento de la seguridad:** Proceso de reforzar un sistema para reducir sus vulnerabilidades y su superficie de ataque.

**Registro (Log):** Inventario de eventos que tienen lugar dentro de los sistemas de una organización.

**Resiliencia**: Capacidad de prepararse, responder y recuperarse de las interrupciones.

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

**Responsable del tratamiento de datos:** Persona que determina el procedimiento y el objetivo del procesamiento de datos.

**Responsabilidad compartida:** Idea de que todos los individuos dentro de una organización asumen 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.

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

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

**Rootkit**: Software malicioso que proporciona acceso administrativo remoto a una computadora.

**Ruptura de la cadena de custodia:** Inconsistencias en la recolección y registro de pruebas en la cadena de custodia.

**Ruta de archivo:** Ubicación de un archivo o directorio.

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

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

S

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

**Salting (salado):** Protección adicional que se utiliza para reforzar las funciones hash que consiste en añadir un factor aleatorio a cada hash con el fin de que no se pueda predecir.

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

**Sangrar:** Dejarespacio al principio de una línea de código, para mejorar la legibilidad.

**Sangría (o indentación):** Espacio que se agrega al principio de una línea de código, para mejorar la legibilidad.

**Scareware:** Software malicioso que emplea tácticas para asustar a las personas con el fin de que infecten su dispositivo.

**Search Processing Language (lenguaje de procesamiento de búsquedas, SPL)**: Lenguaje de consulta de Splunk.

**Secuestro de datos (Ransomware):** Ataque malicioso que consiste en cifrar los datos de una organización para exigir el pago de un rescate para restablecer el acceso a ellos.

**Secuestro de sesión:** Ataque malicioso que consiste en obtener el identificador de sesión de un usuario legítimo.

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

**Segregación de funciones:** Principio según el cuál no se debe otorgar a una misma persona accesos a dos o más responsabilidades dentro del sistema que le permitirían hacer un uso indebido del mismo.

**Seguridad:** Actividad 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 criminal.

**Seguridad de la información (InfoSec):** Práctica de controlar y salvaguardar los datos de una organización.

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

**Seleccionar**: Tercer paso del Marco de Gestión de Riesgos (RMF) del NIST, que consiste en elegir, personalizar y capturar la documentación de los controles que protegen a una organización.

**Sentencia "return":** Instrucción Python que se ejecuta dentro de una función y devuelve información a la llamada a la función.

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

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

**Sentencia preparada:** Técnica de codificación que ejecuta sentencias SQL antes de pasarlas a una base de datos.

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

**Servidor proxy directo (o de reenvío):** Servidor que regula y restringe el acceso a Internet para permitir la conexión sin comprometer la seguridad de la red interna.

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

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

**Shell:** Intérprete de línea de comandos.

**Sintaxis:** Reglas que determinan qué 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, por sus siglas en inglés):** Aplicación que monitorea la actividad del sistema y alerta sobre posibles intrusiones.

**Sistema de detección de intrusiones basado en host (HIDS, por sus siglas en inglés):** Aplicación que monitorea la actividad del host en el que está instalada.

**Sistema de detección de intrusiones basado en la red (NIDS, por sus siglas en inglés):** Aplicación que recopila y monitorea el tráfico y los datos de una red.

**Sistema de nombres de dominio (DNS, por sus siglas en inglés):** Protocolo de red que traduce los nombres de dominio de Internet como direcciones IP.

**Sistema de prevención de intrusiones (IPS, por sus siglas en inglés):** 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 asigna un puntaje a la gravedad de una vulnerabilidad.

**Sistema operativo (SO)**: Interfaz entre el hardware de una computadora y un usuario.

**Sistema operativo heredado:** Sistema operativo obsoleto que aún se sigue utilizando.

**Smishing**: Tipo de ataque de suplantación de identidad (phishing) que utiliza mensajes de texto para engañar a los/las usuarios/as con el fin de obtener información confidencial.

**Software antivirus:** Programa utilizado para prevenir, detectar, y eliminar software malicioso y virus.

**Software malicioso (Malware):** Programa diseñado para dañar dispositivos o redes.

**Software malicioso sin archivos (Malware sin archivos):** Tipo de software malicioso que utiliza programas legítimos que ya están instalados en una computadora para infectarla.

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

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

**Spyware:** Software malicioso que se usa para recabar y vender información sin el consentimiento de su propietario.

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

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

**Subnetting (creación de subredes):** Subdivisión de una red en grupos lógicos llamados subredes.

**Sudo:** Comando que otorga temporalmente permisos elevados a usuarios específicos.

**Superficie de ataque:** Suma de vulnerabilidades, vías o métodos susceptibles de recibir un ataque.

**Suricata**: Sistema de monitoreo de redes de código abierto para la detección y prevención de amenazas.

**Switch (conmutador):** Dispositivo que establece conexiones entre dispositivos específicos en una red, enviando y recibiendo datos entre ellos.

T

**Tabla Arcoiris (Tabla Rainbow):** Archivo de valores hash generados previamente y su texto sin cifrar asociado.

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

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

**Tarjeta de interfaz de red (NIC, por sus siglas en inglés):** Dispositivo que se instala en el interior de una computadora para que esta pueda conectarse a Internet.

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

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

**Tipo de datos:** Categoría para un tipo particular de elemento (o ítem) de datos.

**Token de interfaz de programación de aplicaciones (API):** 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 (CID):** Guía que ayuda a las organizaciones a evaluar los riesgos y establecer sistemas y políticas de seguridad.

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

**Troyano:** (Consultar **Caballo de Troya**).

U

**Ubuntu:** Distribución de código abierto y fácil de usar, que se usa ampliamente en el sector de la seguridad, entre otros.

**Unidad central de procesamiento (CPU):** Procesador principal de una computadora que se utiliza para realizar tareas informáticas generales.

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

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

**Usuario:** Persona que interactúa con una computadora. En ocasiones, también puede ser un dispositivo o software conectado a la red empresarial.

V

**Variable:** Contenedor que almacena datos.

**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.

**Vector de ataque:** Vía que utilizan las y los atacantes para penetrar en las defensas de seguridad.

**Velocidad de conexión:** Rapidez con la que un dispositivo envía y recibe datos, que se mide en bits por segundo.

**Verdadero negativo:** Resultado de un análisis o una detección en el que un sistema de seguridad identifica correctamente la inexistencia de incidentes.

**Verdadero positivo**: Resultado de un análisis o una detección en el que un sistema de seguridad identifica correctamente un incidente real.

**Verdadero positivo**:Resultado de un análisis o proceso de detección en el que un sistema de seguridad identifica correctamente un incidente real

**Violación de la seguridad:** Acceso no autorizado a sistemas, aplicaciones, redes o dispositivos.

**Virus:** (Consultar **Virus informático**).

**Virus informático:** Código malicioso escrito para interferir en el funcionamiento de las computadoras y dañar los datos y el software.

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

**Vishing:** Tipo de estafa por suplantación de identidad en la que se busca obtener información sensible a través de una llamada telefónica.

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

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 ingeridos.

Z

**Zona controlada:** Subred que protege la red interna de la externa.

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

**Zona no controlada:** Parte de la red que está fuera de la organización.