## Términos y definiciones del certificado

Un

**Ruta de archivo absoluta:** la ruta de acceso completa del archivo, que comienza desde la raíz

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

**Rastreo activo de paquetes:** un tipo de ataque en el que los paquetes de datos se manipulan en tránsito

**Protocolo de resolución de direcciones (ARP):** Un protocolo de red utilizado para determinar la dirección MAC del siguiente enrutador o dispositivo en la ruta

**Amenaza persistente avanzada (APT):** una instancia en la que un actor de amenazas mantiene el acceso no autorizado a un sistema durante un período de tiempo prolongado

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

**Adware:** Un tipo de software legítimo que a veces se utiliza para mostrar anuncios digitales en aplicaciones

**Algoritmo:** Conjunto de reglas utilizadas para resolver un problema

**Análisis:** La investigación y validación de alertas

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

**Análisis basado en anomalías:** un método de detección que identifica el comportamiento anormal

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

**Aplicación:** Un programa que realiza una tarea específica

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

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

**Argumento (Python):** Los datos introducidos en una función cuando se llama

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

**Evaluar:** El quinto paso del RMF del NIST que significa determinar si los controles establecidos se implementan correctamente

**Activo:** Un elemento percibido como de valor para una organización

**Clasificación de activos:** La práctica de etiquetar los activos en función de la sensibilidad y la importancia para una organización

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

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

**Cifrado asimétrico:** el uso de un par de claves públicas y privadas para el cifrado y descifrado de datos

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

**Árbol de ataques:** un diagrama que asigna las amenazas a los activos

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

**Autenticación:** El proceso de verificar quién es alguien

**Autorización:** El concepto de otorgar acceso a recursos específicos en un sistema

**Autorizar:** 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

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

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

B

**Baiting:** Una táctica de ingeniería social que tienta a las personas para que comprometan su seguridad.

**Ancho de banda:** La capacidad máxima de transmisión de datos a través de una red, medida por bits por segundo

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

**Bash:** El shell predeterminado en la mayoría de las distribuciones de Linux

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

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

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

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

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

**Gestor de arranque:** Un programa de software que arranca el sistema operativo

**Botnet:** Una colección de computadoras infectadas por malware que están bajo el control de un solo actor de amenazas, conocido como el "pastor de bots"

**Notación entre corchetes:** Los índices colocados entre corchetes

**Cadena de custodia rota:** Inconsistencias en la recolección y registro de pruebas en la cadena de custodia

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

**Bug bounty:** Programas que animan a los hackers autónomos a encontrar y reportar vulnerabilidades

**Función integrada:** Una función que existe dentro de Python y a la que se puede llamar directamente

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

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

**Business Email Compromise (BEC):** Un tipo de ataque de phishing en el que un actor de amenazas se hace pasar por una fuente conocida para obtener una ventaja financiera

C

**Categorizar:** El segundo paso del NIST RMF que se utiliza para desarrollar procesos y tareas de gestión de riesgos

**CentOS:** Una distribución de código abierto que está estrechamente relacionada con Red Hat

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

**Cadena de custodia:** El proceso de documentar la posesión y el control de pruebas durante el ciclo de vida de un incidente

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

**Cifrado:** Algoritmo que encripta la información

**Firewalls basados en la nube:** firewalls de software alojados por el proveedor de servicios en la nube

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

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

**Seguridad** en la nube: el proceso de garantizar que los activos almacenados en la nube estén configurados correctamente y que el acceso a esos activos esté limitado a los usuarios autorizados

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

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

**Interfaz de línea de comandos (CLI):** una interfaz de usuario basada en texto que utiliza comandos para interactuar con el equipo

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

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

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

**Common Vulnerability Scoring System (CVSS):** Un sistema de medición que puntúa la gravedad de una vulnerabilidad

**Cumplimiento:** El proceso de adherirse a las normas internas y a las regulaciones externas.

**Equipos de respuesta a incidentes de seguridad informática (CSIRT):** Un grupo especializado de profesionales de seguridad capacitados en gestión y respuesta a incidentes

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

**Instrucción condicional:** instrucción que evalúa el código para determinar si cumple un conjunto especificado de condiciones

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

**Datos confidenciales:** Datos que a menudo tienen límites en el número de personas que tienen acceso a ellos.

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

**Archivo de configuración:** Un archivo utilizado para configurar los ajustes de una aplicación

**Contención:** El acto de limitar y prevenir el daño adicional causado por un incidente

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

**Cross-site scripting (XSS):** un ataque de inyección que inserta código en un sitio web o una aplicación web vulnerables.

**Crowdsourcing:** La práctica de recopilar información utilizando la participación y la colaboración del público.

**Ataque criptográfico:** Un ataque que afecta a formas seguras de comunicación entre un remitente y el destinatario previsto

**Clave criptográfica:** Mecanismo que descifra el texto cifrado

**Criptografía:** El proceso de transformar la información en una forma que los lectores no deseados no pueden entender.

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

**Autoridad de numeración de CVE (CNA):** una organización que se ofrece como voluntaria para analizar y distribuir información sobre CVE elegibles.

**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 criminal

D

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

**Datos en reposo:** datos a los que no se accede actualmente

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

**Responsable del tratamiento:** Persona que determina el procedimiento y la finalidad del tratamiento de los datos

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

**Exfiltración de datos:** Transmisión no autorizada de datos desde un sistema

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

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

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

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

**Punto de datos:** Un dato específico

**Procesador de datos:** una persona que es responsable del procesamiento de datos en nombre del controlador de datos

**Oficial de protección de datos (DPO):** Una persona que es responsable de supervisar el cumplimiento de los procedimientos de protección de datos de una organización.

**Tipo de datos:** una categoría para un tipo determinado de elemento de datos

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

**Depurador:** Una herramienta de software que ayuda a localizar el origen de un error y evaluar sus causas

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

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

**Ataque de denegación de servicio (DoS):** Un ataque que se dirige a una red o servidor y lo inunda con tráfico de red

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

**Detección:** la detección rápida de eventos de seguridad

**Datos de diccionario:** datos que constan de uno o varios pares clave-valor

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

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

**Directorio:** Un archivo que organiza dónde se almacenan otros archivos

**Plan de recuperación ante desastres:** un plan que permite al equipo de seguridad de una organización describir los pasos necesarios para minimizar el impacto de un incidente de seguridad

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

**Distribuciones:** Las diferentes versiones de Linux

**Documentación:** Cualquier forma de contenido grabado que se utilice para un propósito específico

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

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

**Dropper:** Un programa o un archivo utilizado para instalar un rootkit en un equipo de destino

E

**Elevator pitch:** Un breve resumen de tu experiencia, habilidades y antecedentes

**Encapsulación:** Un proceso realizado por un servicio VPN que protege sus datos al envolver datos confidenciales en otros paquetes de datos

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

**Punto final:** cualquier dispositivo conectado a una red

**Detección y respuesta de endpoints (EDR):** una aplicación que supervisa un endpoint en busca de actividad maliciosa

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

**Directiva de escalamiento:** un conjunto de acciones que describen a quién se debe notificar cuando se produce una alerta de incidente y cómo se debe controlar ese incidente

**Evento:** Un suceso observable en una red, sistema o dispositivo

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

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

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

**Exposición:** Un error que puede ser explotado por una amenaza

**Amenaza externa:** Cualquier cosa fuera de la organización que tenga el potencial de dañar los activos de la organización

F

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

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

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

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

**Filesystem Hierarchy Standard (FHS):** El componente del sistema operativo Linux que organiza los datos

**Filtrado:** selección de datos que coincidan con una determinada condición

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

**Firewall:** Un dispositivo de seguridad de red que monitorea el tráfico hacia o desde una red

**Datos flotantes:** Datos que consisten en un número con un punto decimal

**Clave externa:** una columna de una tabla que es una clave principal de otra tabla

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

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

G

**Variable global:** Una variable que está disponible a través de todo el programa

**Interfaz gráfica de usuario (GUI):** Una interfaz de usuario que utiliza iconos en la pantalla para administrar diferentes tareas en la computadora

H

**Hacker:** Cualquier persona o grupo que utilice ordenadores para obtener acceso no autorizado a los datos

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

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

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

**Colisión de hash:** una instancia en la que diferentes entradas producen el mismo valor de hash

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

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

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

**Honeypot:** Un sistema o recurso creado como señuelo vulnerable a los ataques con el propósito de atraer a posibles intrusos

**Sistema de detección de intrusiones basado en host (HIDS):** una aplicación que supervisa la actividad del host en el que está instalada

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

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

**Protocolo de transferencia de hipertexto seguro (HTTPS):** Un protocolo de red que proporciona un método seguro de comunicación entre los clientes y los servidores del sitio web

Yo

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

**Gestión de identidades y accesos (IAM):** una colección de procesos y tecnologías que ayuda a las organizaciones a gestionar las identidades digitales en su entorno

**IEEE 802.11 (Wi-Fi):** Un conjunto de estándares que definen la comunicación para LAN inalámbricas

**Inmutable:** Un objeto que no se puede cambiar después de crearlo y asignarle un valor

**Implementar:** El cuarto paso del NIST RMF que significa implementar planes de seguridad y privacidad para una organización

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

**Incidente:** Un suceso que pone en peligro real o inminentemente, 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

**Escalamiento de incidentes**: el proceso de identificar un posible incidente de seguridad, clasificarlo y entregarlo a un miembro del equipo más experimentado

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

**Respuesta a incidentes:** el intento rápido de una organización para identificar un ataque, contener el daño y corregir los efectos de una violación de seguridad.

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

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

**Sangría:** espacio añadido al principio de una línea de código

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

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

**Indicadores de compromiso (IoC):** Evidencia observable que sugiere signos de un posible incidente de seguridad

**Privacidad de la información:** la protección del acceso y la distribución no autorizados de datos

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

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

**Validación de entradas:** Programación que valida las entradas de los usuarios y otros programas

**Datos enteros:** datos que constan de un número que no incluye un punto decimal

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

**Integridad:** La idea de que los datos son correctos, auténticos y confiables

**Hardware interno:** los componentes necesarios para hacer funcionar el equipo

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

**Protocolo de mensajes de control de Internet (ICMP):** Un protocolo de Internet utilizado por los dispositivos para informarse entre sí sobre errores de transmisión de datos a través de la red

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

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

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

**Intérprete:** Un programa de computadora que traduce el código Python en instrucciones ejecutables línea por línea

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

**Sistema de prevención de intrusiones (IPS):** una aplicación que supervisa la actividad del sistema en busca de actividad intrusiva y toma medidas para detener la actividad

**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

**Declaración iterativa:** código que ejecuta repetidamente un conjunto de instrucciones

K

**KALI LINUX ™ :** Una distribución de código abierto de Linux que es ampliamente utilizada en la industria de la seguridad

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

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

L

**Sistema operativo heredado:** un sistema operativo que está desactualizado pero que aún se utiliza

**Reunión de lecciones aprendidas:** Una reunión que incluye a todas las partes involucradas después de un incidente importante

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

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

**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

**Lista de datos:** Estructura de datos que consiste en una colección de datos en forma secuencial

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

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

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

**Registro:** Un registro de eventos que ocurren dentro de los sistemas de una organización

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

**Registro:** El registro de eventos que ocurren en sistemas informáticos y redes

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

**Administración de registros:** el proceso de recopilación, almacenamiento, análisis y eliminación de datos de registro

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

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

M

**Malware:** software diseñado para dañar dispositivos o redes

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

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

**Método:** Una 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:** Una colección de centros de investigación y desarrollo sin fines de lucro

**Módem:** Un dispositivo que conecta su enrutador a Internet y lleva el acceso a Internet a la LAN

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

**Monitor**: El séptimo paso del NIST RMF que significa estar al tanto de cómo están funcionando los sistemas

**Autenticación multifactor (MFA):** una medida de seguridad que requiere que un usuario verifique su identidad de dos o más maneras para acceder a un sistema o red

N

**nano:** Un editor de archivos de línea de comandos que está disponible de forma predeterminada en muchas distribuciones de Linux

**Marco de Ciberseguridad (CSF) del Instituto Nacional de Estándares y Tecnología (NIST):** Un marco voluntario que consta de estándares, directrices y mejores prácticas para gestionar el riesgo de ciberseguridad

**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

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

**Red:** Un grupo de dispositivos conectados

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

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

**Tarjeta de interfaz de red (NIC):** Hardware que conecta computadoras a una red

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

**Analizador de protocolos de red (packet sniffer):** Una herramienta diseñada para capturar y analizar el tráfico de datos dentro de una red

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

**Seguridad de red:** La práctica de mantener la infraestructura de red de una organización segura contra el acceso no autorizado

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

**Tráfico de red:** la cantidad de datos que se mueven a través de una red

**No repudio:** el concepto de que no se puede negar la autenticidad de la información

**Notebook:** una interfaz en línea para escribir, almacenar y ejecutar código

**Datos numéricos:** Datos formados por números

O

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

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

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

**Inteligencia de código abierto (OSINT):** La recopilación y el análisis de información de fuentes disponibles públicamente para generar inteligencia utilizable

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

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

**Sistema operativo (SO):** La interfaz entre el hardware de la computadora y el usuario

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

**Opciones:** Entrada que modifica el comportamiento de un comando

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

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

P

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

**Administrador de paquetes:** una herramienta que ayuda a los usuarios a instalar, administrar y eliminar paquetes o aplicaciones

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

**Rastreo de paquetes:** La práctica de capturar e inspeccionar paquetes de datos a través de una red

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

**Parrot:** Una distribución de código abierto que se usa comúnmente para la seguridad

**Análisis sintáctico:** el proceso de convertir datos en un formato más legible

**Rastreo pasivo de paquetes:** un tipo de ataque en el que un actor malintencionado se conecta a un centro de red y examina todo el tráfico de la red

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

**Actualización de parches:** una actualización de software y sistema operativo que soluciona las vulnerabilidades de seguridad de un programa o producto

**Estándares de seguridad de datos de la industria de tarjetas de pago (PCI DSS):** cualquier dato del titular de la tarjeta que una organización acepte, transmita o almacene

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

**Guía de estilo de PEP 8:** Un recurso que proporciona pautas estilísticas para los programadores que trabajan en Python

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

**Permisos:** el tipo de acceso concedido para un archivo o directorio

**Información de identificación personal (PII):** cualquier información utilizada para inferir la identidad de una persona

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

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

**Ataque físico:** Un incidente de seguridad que afecta no solo a los entornos digitales, sino también a los físicos donde se despliega el incidente

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

**Ping de la muerte:** Un tipo de ataque DoS causado cuando un hacker hace ping a un sistema enviándole un paquete ICMP de gran tamaño que tiene más de 64 KB

**Playbook:** Un manual que proporciona detalles sobre cualquier acción operativa

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

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

**Filtrado de puertos:** una función de firewall que bloquea o permite que ciertos números de puerto limiten la comunicación no deseada

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

**Aplicación potencialmente no deseada (PUA):** un tipo de software no deseado que se incluye con programas legítimos que pueden mostrar anuncios, causar ralentización del dispositivo o instalar otro software

**Datos** privados: Información que debe mantenerse oculta al público

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

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

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

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

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

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

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

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

**Proteger:** una función central del NIST que se utiliza para proteger una organización mediante la implementación de políticas, procedimientos, capacitación y herramientas que ayudan a mitigar las amenazas de ciberseguridad

**Información de salud protegida (PHI):** Información que se relaciona con la salud o condición física o mental pasada, presente o futura de una persona

**Protección y preservación de pruebas:** el proceso de trabajar adecuadamente con pruebas digitales frágiles y volátiles

**Servidor proxy:** Un servidor que cumple con las solicitudes de sus clientes reenviándolas a otros servidores

**Datos públicos**: datos que ya son accesibles al público y que suponen un riesgo mínimo para la organización si otros los ven o comparten

**Infraestructura de clave pública (PKI):** un marco de cifrado que protege el intercambio de información en línea

**Biblioteca estándar de Python:** Una extensa colección de código Python que a menudo viene empaquetado con Python

Q

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

**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

**Tabla Rainbow:** Un archivo de valores hash generados previamente y su texto sin formato asociado

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

**Ransomware:** Un ataque malicioso en el que los actores de amenazas cifran los datos de una organización y exigen un pago para restaurar el acceso

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

**Recuperación:** Una función central del NIST relacionada con la devolución de los sistemas afectados al funcionamiento normal

**Recuperación:** El proceso de devolver los sistemas afectados a las operaciones normales

**Red Hat® Enterprise Linux®** (también conocido simplemente como Red Hat en este curso): Una distribución de Linux basada en suscripción creada para uso empresarial

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

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

**Regulaciones:** Reglas establecidas por un gobierno u otra autoridad para controlar la forma en que se hace algo

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

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

**Ataque de reproducción:** Un ataque de red que se realiza cuando un actor malintencionado intercepta un paquete de datos en tránsito y lo retrasa o lo repite en otro momento

**Resiliencia**: la capacidad de prepararse, responder y recuperarse de las interrupciones

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

**Instrucción return:** Una instrucción de Python que se ejecuta dentro de una función y envía información de vuelta a la llamada a la función

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

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

**Mitigación de riesgos:** el proceso de contar con los procedimientos y reglas adecuados para reducir rápidamente el impacto de un riesgo como una infracción.

**Directorio raíz:** El directorio de nivel más alto en Linux

**Rootkit**: malware que proporciona acceso administrativo remoto a un equipo

**Usuario root (o superusuario):** Un usuario con privilegios elevados para modificar el sistema

**Router:** Un dispositivo de red que conecta varias redes entre sí

S

**Salado:** una protección adicional que se utiliza para reforzar las funciones de hash

**Scareware:** malware que emplea tácticas para asustar a los usuarios para que infecten su dispositivo.

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

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

**Secure shell (SSH):** Un protocolo de seguridad utilizado para crear un shell con un sistema remoto

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

**Auditoría de seguridad**: revisión de los controles, políticas y procedimientos de seguridad de una organización en función de un conjunto de expectativas

**Controles de seguridad:** Salvaguardas diseñadas para reducir riesgos de seguridad específicos

**Ética de seguridad:** Directrices para tomar decisiones adecuadas como profesional de la seguridad

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

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

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

**Gestión de eventos e información de seguridad (SIEM):** una aplicación que recopila y analiza datos de registro para supervisar las actividades críticas de una organización

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

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

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

**Postura de seguridad:** la capacidad de una organización para gestionar su defensa de activos y datos críticos y reaccionar ante el cambio

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

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

**Datos confidenciales**: un tipo de datos que incluye información de identificación personal (PII), información de identificación personal confidencial (SPII) o información de salud protegida (PHI)

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

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

**Sesión:** una secuencia de solicitudes y respuestas HTTP de red asociadas con el mismo usuario

**Cookie de sesión:** Un token que los sitios web utilizan para validar una sesión y determinar cuánto tiempo debe durar esa sesión

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

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

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

**Responsabilidad compartida:** La 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

**Shell:** El intérprete de línea de comandos

**Firma:** un patrón que está asociado con actividad maliciosa

**Análisis de firmas:** Método de detección utilizado para encontrar eventos de interés

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

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

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

**Ataque smurf:** Un ataque de red que se realiza cuando un atacante rastrea la dirección IP de un usuario autorizado y la inunda con paquetes ICMP

**Ingeniería social:** una técnica de manipulación que explota el error humano para obtener información privada, acceso u objetos de valor.

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

**Spear phishing:** Un ataque de correo electrónico malicioso dirigido a un usuario o grupo de usuarios específico, que parece originarse en una fuente confiable

**Velocidad:** La velocidad a la que un dispositivo envía y recibe datos, medida por bits por segundo

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

**Splunk Enterprise:** una herramienta autoalojada que se utiliza 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 utiliza para recopilar y vender información sin consentimiento.

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

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

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

**Error estándar:** Un mensaje de error devuelto por el sistema operativo a través del shell

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

**Salida estándar:** Información devuelta por el sistema operativo a través del shell

**Estándares:** Referencias que informan sobre cómo establecer políticas

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

**Stateful:** una clase de firewall que realiza un seguimiento de la información que pasa a través de él y filtra de forma proactiva las amenazas.

**Sin estado:** una clase de firewall que funciona en base a reglas predefinidas y que no realiza un seguimiento de la información de los paquetes de datos

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

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

**Datos de cadena:** datos que constan de una secuencia ordenada de caracteres

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

**Subreds:** La subdivisión de una red en grupos lógicos llamados subredes

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

**Sudo:** Un comando que otorga temporalmente permisos elevados a usuarios específicos

**Ataque a la cadena de suministro:** un ataque que se dirige a sistemas, aplicaciones, hardware y/o software para localizar una vulnerabilidad en la que se pueda desplegar malware

**Suricata**: Un sistema de detección de intrusiones de código abierto, un sistema de prevención de intrusiones y una herramienta de análisis de red

**Switch:** Un dispositivo que realiza conexiones entre dispositivos específicos en una red enviando y recibiendo datos entre ellos

**Cifrado simétrico:** el uso de una única clave secreta para intercambiar información

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

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

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

T

**Tailgating:** Una táctica de ingeniería social en la que personas no autorizadas siguen a una persona autorizada a un área restringida

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

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

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

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

**Amenaza:** Cualquier circunstancia o evento que pueda afectar negativamente a los activos

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

**Threat hunting:** la búsqueda proactiva de amenazas en una red

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

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

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

**Protocolo de control de transmisión (TCP):** Un protocolo de comunicación por Internet que permite que dos dispositivos formen una conexión y transmitan datos

**Triaje**: La priorización de incidentes según su nivel de importancia o urgencia

**Caballo de Troya:** malware que parece un archivo o programa legítimo

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

**Verdadero positivo** Una alerta que detecta correctamente la presencia de un ataque

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

**Error de tipo:** un error que se produce por usar el tipo de datos incorrecto

U

**Ubuntu:** Una distribución de código abierto y fácil de usar que se usa ampliamente en seguridad y otras industrias

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

**Zona no controlada:** cualquier red fuera del control de su organización

**Unified Extensible Firmware Interface (UEFI):** Un microchip que contiene instrucciones de carga para la computadora y reemplaza el BIOS en sistemas más modernos

**USB baiting:** un ataque en el que un actor de amenazas deja estratégicamente una memoria USB de malware para que un empleado la encuentre e instale para infectar una red sin saberlo

**Usuario:** La persona que interactúa con una computadora

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

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

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

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

V

**Variable:** Un contenedor que almacena datos

**Red privada virtual (VPN):** un servicio de seguridad de red que cambia su dirección IP pública y oculta su ubicación virtual para que pueda mantener la privacidad de sus datos cuando utilice una red pública como Internet

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

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

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

**Panel de control visual:** una forma de mostrar varios tipos de datos rápidamente en un solo lugar

**Vulnerabilidad:** Una debilidad que puede ser explotada por una amenaza

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

**Gestión de vulnerabilidades:** el proceso de encontrar y parchear vulnerabilidades

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

W

**Ataque de abrevadero**: un tipo de ataque cuando un actor de amenazas compromete un sitio web visitado con frecuencia por un grupo específico de usuarios

**Vulnerabilidades de seguridad basadas en la web:** código o comportamiento malintencionado que se utiliza para aprovecharse de los errores de codificación de una aplicación web.

**Whaling:** Una categoría de intentos de spear phishing dirigidos a ejecutivos de alto rango de una organización

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

**Wi-Fi Protected Access (WPA):** Un protocolo de seguridad inalámbrico para que los dispositivos se conecten a Internet

**Comodín:** Un carácter especial que se puede sustituir por cualquier otro carácter

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

**Archivo de escritura universal:** Un archivo que puede ser alterado por cualquier persona en el mundo

**Gusano:** malware que puede duplicarse y propagarse a través de los sistemas por sí solo

Y

**YARA-L:** Un lenguaje informático utilizado para crear reglas para buscar a través de datos de registro ingeridos

Z

**Zero-day:** Un exploit que hasta ahora era desconocido