## Términos y definiciones del Curso 1

A

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

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

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

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

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

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

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

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

**Ataque de “watering hole”**: tipo de ataque en el que un actor 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 por contraseña

**Ataque físico:** incidente de seguridad que no solo afecta entornos digitales sino los físicos en donde se implemente el incidente

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

B

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

C

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

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

**Confidencialidad:** únicamente los usuarios autorizados pueden acceder a activos o datos específicos

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

D

**Disponibilidad:** idea de que los datos son accesibles para quienes estén autorizados a acceder a ellos.

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

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

H

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

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

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

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

I

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

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

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

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

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

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

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

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

L

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

**Linux:** sistema operativo de código abierto

M

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

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

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

O

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

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

P

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

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

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

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

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

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

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

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

S

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

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

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

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

T

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

U

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

V

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

**Virus:** consulta “virus informático”

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