**Términos y definiciones del Curso 1**

A

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

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

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

**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.

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

**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.

**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 “agujero de agua” (watering hole)**: Tipo de ataque en el que un/a agente de amenaza compromete a un sitio web visitado con frecuencia por un grupo específico de usuarios/as.

**Ataque de contraseña:** Intento de acceder a dispositivos, sistemas, redes o datos protegidos con una contraseña.

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

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

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

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

B

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

C

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

**Ciberseguridad:** Práctica de garantizar la confidencialidad, integridad y disponibilidad de la información mediante la protección de las redes, dispositivos y datos contra el acceso no autorizado o la explotación delictiva.

**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.

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

**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.

D

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

**Disponibilidad:** Principio según el cual los datos son accesibles para las personas autorizadas a utilizarlos.

E

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

G

**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.

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

H

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

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

**Hacker:** Cualquier persona o grupo de personas que utiliza computadoras para acceder a datos sin autorización.

**Hacktivista:** Persona que utiliza el hacking para lograr objetivos políticos.

I

**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.

**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.

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

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

L

**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.

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

**Log:** Ver registro

M

**Malware:** Ver **Software malicioso.**

**Marco de Ciberseguridad (CSF) 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.

O

**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.

P

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

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

**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.

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

R

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

S

**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 redes:** 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 accesos no autorizados.

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

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

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

T

**Tríada de confidencialidad, integridad y disponibilidad (CID):** Guía que ayuda a las organizaciones a evaluar los riesgos y establecer sistemas y políticas de seguridad.

V

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

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

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