Actividad 01. Elaboración de glosario de términos

CSRF: Cross Site Request Forgery (CSRF o XSRF) es un tipo de ataque que se suele usar para estafas por Internet. Los delincuentes se apoderan de una sesión autorizada por el usuario (session riding) para realizar actos dañinos. El proceso se lleva a cabo mediante solicitudes HTTP.

Indicadores de compromiso: Es un conjunto de datos sobre un objeto o una actividad que indica acceso no autorizado al equipo (compromiso de datos). Por ejemplo, muchos intentos fallidos de iniciar sesión en el sistema pueden constituir un indicador de compromiso. La tarea *Análisis de IOC* permite encontrar indicadores de compromiso en el equipo y tomar medidas de respuesta ante amenazas.

Resiliencia: Es la capacidad de una organización de adaptarse a las amenazas cibernéticas sin interrumpir la integridad, la finalidad ni la continuidad del negocio. Representa el nivel de preparación de una empresa para adelantarse a los ataques cibernéticos, así como para detectarlos y recuperarse de ellos.

XSS (Secuencias de comandos en sitios cruzados): Una secuencia de comandos en sitios cruzados o Cross-site scripting (XSS) es un tipo de ataque informático que permite a un actor de amenazas ejecutar código malicioso en el navegador de otro usuario. Ocurren cuando una aplicación web utiliza la entrada de un usuario sin validarla adecuadamente. Esto puede resultar en el robo de cookies, tokens de sesión y otra información confidencial.

Clave pública: Es un método para encriptar o firmar datos con dos claves diferentes y hacer que una de las claves, la pública, esté disponible para que cualquiera pueda utilizarla.

HTTP: El protocolo de transferencia de hipertexto (HTTP) es un protocolo o conjunto de reglas de comunicación para la comunicación cliente-servidor. Cuando visita un sitio web, su navegador envía una solicitud HTTP al servidor web, que responde con una respuesta HTTP. Es la tecnología subyacente que impulsa la comunicación de red.

Plugin: Son pequeños programas complementarios que amplían las funciones de aplicaciones web y programas de escritorio. Por norma general, cuando instalamos un *plugin*, el software en cuestión adquiere una nueva función. La mayoría de los usuarios conoce los *plugins* por los navegadores web, aunque ya se han asentado en cualquier tipo de programa y aplicación.

Ataque activo: Un ataque activo es un tipo de ataque cibernético en el que un intruso intenta alterar o comprometer la integridad, confidencialidad o disponibilidad de un sistema informático o red, en lugar de simplemente observar o recopilar información.

Cuentas predeterminadas: Cuenta establecida por defecto por el sistema o por programa que permite realizar el acceso por primera vez al mismo. Se recomienda que el usuario posteriormente la modifique o la elimine.

Infraestructura de clave pública: Una infraestructura de Clave Pública es un conjunto de protocolos, servicios y estándares que soportan aplicaciones basadas en criptografía de clave pública.
Algunos de los servicios ofrecidos por una ICP son los siguientes:

- Registro de claves.
- Revocación de certificados.
- Selección de claves.
- Evaluación de la confianza.
- Recuperación de claves.

SaaS: El software como servicio (SaaS) se considera tradicionalmente un modelo de software basado en la nube, el cual ofrece aplicaciones a los usuarios finales a través de un navegador de Internet. Los proveedores de SaaS alojan servicios y aplicaciones para que los clientes puedan acceder a ellos bajo demanda.

WPS: Las siglas WPS significan *Wifi Protected Setup*, y es un sistema que tiene por funcionalidad básica la de ofrecer una manera controlada de conectarse a una Wi-Fi escribiendo sólo un PIN de 8 dígitos en lugar de la contraseña inalámbrica completa.

Clave privada: Es la encargada de descifrar la información en la criptografía asimétrica, propia de los certificados digitales. La clave privada es generada por la Autoridad de Certificación a la hora de emitir un certificado y solo es conocida por el usuario que se identifica como titular del mismo.

Hacker: Aquella persona que trata de solventar, paliar o informar sobre los problemas de seguridad encontrados en programas, servicios, plataformas o herramientas.

Puerta trasera (Backdoor): Backdoor es una puerta trasera para tomar el control de un equipo, casi siempre con intenciones ilegítimas, de manera remota y sin que el titular del mismo esté al tanto.

Correo spam: Correo electrónico comercial no solicitado (UCE), consiste en anuncios no deseados y cuestionables enviados por correo electrónico de forma masiva.