FUNDAMENTOS DE SEGURIDAD INFORMÁTICA Nivel 1

GLOSARIO

Capacítate para el empleo | FUNDACIÓN Carlos Slim

Durante el desarrollo del curso será necesario que manejes la siguiente **terminología** para una mejor comprensión de éste.

Término	Definición
Amenaza avanzada persistente (APT)	**Adversario que procesa niveles de habilidad sofisticados** y recursos que le permiten múltiples ataques.
Antivirus	Aplicación cuyo propósito es **identificar, desactivar y eliminar códigos maliciosos**.
Big Data	**Datos en grandes cantidades, velocidad y variedad** cuyo procesamiento ayuda en la automatización y toma de decisiones.
Ciberataque	**Intenciones de daño, detención e ingreso sin permiso** a los sistemas computacionales y sus comunicaciones por medios cibernéticos.
Ciberinteligencia	Reunión y procesamiento de datos con la finalidad de **discriminar, seguir y contrarrestar las actividades de los atacantes**.
Códigos maliciosos	**Aplicaciones cuyo objetivo es infiltrarse en los sistemas** para generar problemas en los equipos de los usuarios.
Denegación de servicio (DoS)	**Negativa de la solicitud de usar un servicio de cómputo** por un usuario legítimo.
Dispositivo de usuario final	**Equipos inteligentes**, de telefonía o cómputo **que se conectan a la red de la empresa**.
Firewall	**Sistema de seguridad de red que controla su tráfico según las reglas de seguridad**, conocido también como cortafuegos.
Gestión de movilidad empresarial (EMM)	**Procedimiento de aseguramiento y habilitación del uso de celulares** y tabletas por los empleados.
Huella digital	Rastro de los **datos digitales del usuario**.

FUNDAMENTOS DE SEGURIDAD INFORMÁTICA Nivel 1

GLOSARIO

Capacítate para el empleo | FUNDACIÓN Carlos Slim

Término	Definición
 **Identidad digital**	Información que permite **reconocer a una persona en internet**.
 **Ingeniería social**	**Técnicas usadas para manipular a los usuarios** para la difusión de datos útiles por el atacante.
 **Inteligencia de amenazas**	**Reportes que describen técnicas, procedimientos, actores, tipos de sistemas** considerados como objetivos.
OSI **Modelo de interconexión de sistemas abiertos (OSI)**	**Estandarización de la comunicación de los sistemas computacionales** de distintas tecnologías y estructuras internas.
ISO **Organización internacional para la estandarización (ISO)**	**Entidad** de diferentes miembros nacionales **encargada de establecer modelos unificados**.
 **Parche**	**Actualización de protección** que mejora la funcionalidad del *software*.
ISP **Política de seguridad de la información (ISP)**	**Conjunto de reglas promulgadas por la empresa u organización** para asegurar su acato según las prescripciones de protección.
 **Protección de marca**	**Resguardo de la propiedad intelectual** de la empresa.
ISMS **Sistema de administración de la seguridad de información (ISMS)**	**Conjunto de reglas y procedimientos de gestión sistemática de los activos informáticos** para reducir sus riesgos y asegurar la continuidad del negocio.
 ***Skimming***	**Robo de información sensible** usada para su aprovechamiento.
 **Suplantación de identidad o *Phishing***	Mensajes de correo electrónico cuyo propósito es **conseguir datos confidenciales de los usuarios**.