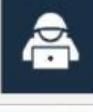


**GLOSARIO**

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

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

**GLOSARIO**

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