



GLOSARIO DE TÉRMINOS

ESTÁNDAR DE COMPETENCIAS PROFESIONALES: ASEGURAR EQUIPOS INFORMÁTICOS

Código: ECP0486_3

NIVEL: 3



Autenticación: Proceso de verificar la identidad de alguien o algo. La autenticación suele tener lugar mediante la comprobación de una contraseña, un token de hardware o algún otro dato que demuestre la identidad.

Confidencialidad: También, principio de privacidad. Uno de los principios de la seguridad informática. Hace referencia a que la información solo debe ser conocida por las personas autorizadas para ello. Es decir, ciertos datos o programas solo pueden ser accesibles para las personas autorizadas.

Cortafuegos: (Firewall). Sistema que protege redes y terminales privadas de accesos no autorizados, especialmente durante la navegación por internet.

DNS: (Domain Name System. En español, Sistema de Nombres de Dominio). Método de denominación empleado para nombrar mediante caracteres alfanuméricos legibles para humanos a los dispositivos que se conectan a una red a través del IP (Internet Protocol o Protocolo de Internet). El DNS se encarga de vincular informaciones asociadas al nombre de dominio que se le asigna a cada equipo y traducir a direcciones de red numéricas, por ejemplo, IP.

Honeypots: (Anglicismo). Herramienta de seguridad informática dispuesto en una red o sistema informático para ser el objetivo de un posible ataque informático, y así poder detectarlo y obtener información del mismo y del atacante.

IDS: (Intrusion Detection System. En español, Sistema de Detección de Intrusos). Sistema de supervisión que detecta actividades sospechosas y genera alertas al detectarlas.

Integridad: Garantía de que la información digital no está dañada y solo pueden acceder o modificar aquellos autorizados para hacerlo.

IPS: (Intrusion Prevention System. En español, Sistema de Prevención de Intrusiones). Dispositivo o aplicación software que monitoriza una red para detectar y responder a cualquier actividad maliciosa o violaciones de la política de seguridad. Cualquier actividad o violación maliciosa es reportada o recogida de manera centralizada usando un sistema de seguridad de la información y de gestión de eventos. A diferencia de los IDS, los IPS son capaces de responder a intrusiones detectadas en el momento de su descubrimiento.

Malware: (Anglicismo. En español, programa malicioso). Cualquier tipo de software que realiza acciones dañinas en un sistema informático de forma intencionada (al contrario que el «software defectuoso») y sin el conocimiento del usuario.

NFS: (Network File System. En español, Sistema de ficheros en red). Protocolo de nivel de aplicación, según el Modelo OSI. Es utilizado para sistemas de archivos distribuidos en un entorno de red de computadoras de área local.

Protocolo SSH: (Secure Sockets Layer. En español, capa de puertos seguros). Protocolo criptográfico de la capa de transporte para comunicaciones seguras por red.



Protocolo TLS: (Transport Layer Security). Protocolo criptográfico de la capa de transporte que proporciona comunicaciones seguras por una red.

Ransomware: (Anglicismo. En español, secuestro de datos). Del inglés ransom, rescate, y ware, abreviatura de software. Tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema operativo infectado y pide un rescate a cambio de quitar esta restricción.

SAI: (Sistemas de alimentación ininterrumpida. En inglés, Uninterruptible Power Supply -UPS-). Dispositivo que, gracias a sus baterías y otros elementos almacenadores de energía, puede proporcionar energía eléctrica por un tiempo limitado a todos los dispositivos que tenga conectados.

Servicio: Programa instalado en un equipo remoto llamado servidor y cuya funcionalidad se ofrece a otros equipos conectados a él por red llamados cliente. Son típicos los servicios/servidores de impresión, de archivos, de cualquier programa/software mediante llamadas a procedimientos remotos (RPC) o de páginas web. La mayor capacidad del servidor se pone al servicio de los clientes, lo que redundará en una mayor simplicidad y menor coste de los segundos.

Servidor: Máquina física integrada en una red informática en la que, además del sistema operativo, opera uno o varios servicios "software" que se ofrecen a otros equipos denominados clientes que pueden estar conectados a nivel local o a través de una red externa. El tipo de servicio depende del tipo de "software" del servidor. La base de la comunicación es el modelo cliente-servidor y, en lo que concierne al intercambio de datos, entran en acción los protocolos de transmisión específicos del servicio.