GLOSARIO DE TÉRMINOS

ESTÁNDAR DE COMPETENCIAS PROFESIONALES: Configurar la ciberseguridad en equipos finales

Código: ECP0959_2 NIVEL: 2

Actualización: Lanzamiento o instalación de una nueva versión de un software que incluye más y mejores funcionalidades y/o soluciona fallos de la versión precedente.

Antivirus: Tipo de software que se utiliza para evitar, buscar, detectar y eliminar virus de un ordenador.

Bluetooth: (Anglicismo). Protocolo de comunicaciones que sirve para la transmisión inalámbrica de datos (fotos, música, contactos…) y voz entre diferentes dispositivos que se hallan a corta distancia, dentro de un radio de alcance que, generalmente, es de unos diez metros.

Ciberseguridad: Conjunto de elementos, medidas y equipos destinados a defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información, seguridad de la información electrónica o seguridad informática.

Cifrado: También, encriptado. Conversión de información de un formato legible a un formato codificado. La información cifrada solo se puede comprender y procesar tras el descifrado (desencriptado).

Cifrar: Encriptar. Convertir información de un formato legible a un formato codificado. La información cifrada/encriptada solo se puede comprender y procesar tras el descifrado/desencriptado.

Cuarentena: Aislar un archivo malicioso en un área específica y segura de un dispositivo para que la infección no se propague a otros archivos en él.

EDR: (Endpoint Detection and Response). Herramienta que proporciona monitorización y análisis continuo del dispositivo terminal (endpoint) y la red. La finalidad es identificar, detectar y prevenir amenazas avanzadas (APT) con mayor facilidad. La tecnología EDR detecta ataques que nuestro antivirus ha pasado por alto. Monitoriza y evalúa todas las actividades de la red (eventos de los usuarios, archivos, procesos, registros, memoria y red). Detecta ataques informáticos en tiempo real, y permite tomar medidas inmediatas si es necesario.

End point: (Anglicismo. En español, equipos finales). Dispositivos informáticos conectados en el extremo de una red de transmisión de datos.

EPP: (Endpoint Protection Platform). Solución de seguridad integral desplegada en equipos terminales para protegerse de amenazas. Las soluciones EPP son gestionadas típicamente en la nube y usan datos en ella para asistir en soluciones avanzadas de monitorización y solución remotas. Contienen una suite de tecnologías de seguridad tales como antivirus, encriptación de datos y prevención de pérdida de datos.

Evento: Notificación automática que ha habido algún tipo de acción y que suele disparar una acción o conjunto de acciones que, a su vez, pueden dar como resultado un evento en particular o una serie de eventos.

IP: (Internet Protocol. En español, Protocolo de Internet). Conjunto de reglas que rigen el envío y recepción de datos enviados a través de Internet o de una red

local basada en ese protocolo. Por extensión, se asimila a dirección IP, esto es, dirección lógica única que identifica a un dispositivo en Internet o en una red local basada en la arquitectura TCP/IP en un momento dado según las reglas del protocolo IP.

Lista blanca: (En inglés, whitelist). Archivos, emails, direcciones IP y dominios que se consideran aceptables para enviar o almacenar. Es el término opuesto a lista negra, que son aquellos que se bloquearán.

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.

Nube: Red de servidores remotos conectados a internet para almacenar, administrar y procesar datos, servidores, bases de datos, redes y software.

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 redunda 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.

Sistema operativo: Conjunto de programas que permite manejar la memoria, disco, medios de almacenamiento de información y los dispositivos asociados, periféricos o recursos del ordenador, como son el teclado, el ratón, la impresora, la tarjeta de red, entre otros.

Syslog: (Anglicismo. En español, registro de sucesos del sistema). Estándar de mensajes de log o sucesos que casi todos los dispositivos o aplicaciones pueden enviar o almacenar, conteniendo información sobre estado, eventos y diagnósticos, entre otros.

Tampering: (Anglicismo). Acción de acceder o modificar algo que no se debería, usualmente cuando se intenta causar un daño o hacer algo ilegal.

Trazabilidad: Conjunto de procedimientos que permiten seguir la evolución de los procesos o productos en cada una de sus etapas.

Virus: Programa informático elaborado de manera anónima que tiene la capacidad de reproducirse y transmitirse independientemente de la voluntad del operador y que causa alteraciones más o menos graves en el funcionamiento de la computadora.

VPN: (Virtual Private Network. En español, Red Privada Virtual). Servicio que cifra los datos de las comunicaciones entre dos puntos, incluyendo la navegación en Internet, construyendo una red privada y segura o túnel entre la conexión de una máquina cliente y un servidor destinatario.

Vulnerabilidad: Debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible. Estos "agujeros" pueden tener distintos orígenes, por ejemplo: fallos de diseño, errores de configuración o carencias de procedimientos.