GLOSARIO DE TÉRMINOS

CUALIFICACIÓN PROFESIONAL: Operaciones de seguridad en sistemas informáticos

Código: IFC300_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.

Backup: (Anglicismo. En español, respaldo, copia de respaldo o copia de reserva). Copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.

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.

Certificado digital: Certificación electrónica expedida por una entidad de confianza o autoridad certificadora que vincula a su suscriptor (persona, programa o máquina) con unos datos de verificación de firma y se usa para confirmar su identidad.

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.

Clave pública: Una de las dos claves que genera un procedimiento de criptografía asimétrica. La clave privada y la pública están matemáticamente relacionadas. La clave pública se genera siempre a partir de la clave privada. La clave pública puede ser difundida por su propietario para ser usada por terceros. Estos terceros pueden usar la clave pública del propietario para cifrar mensajes que solo el propietario de la clave pública podrá leer usando su clave privada.

Conectividad: Capacidad de un dispositivo de conectarse y comunicarse con otro, con el fin de intercambiar información o establecer una conexión directa a base de información digital.

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.

Controlador: (En inglés, Driver). Rutina o programa que enlaza un dispositivo periférico al sistema operativo.

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

CPU: (Central Processing Unit. En español, Unidad Central de Procesamiento). Suele asimilarse coloquialmente al microprocesador o, simplemente, procesador. Es el dispositivo encargado de recibir e interpretar datos y ejecutar las secuencias de instrucciones a realizar por cada programa, valiéndose de operaciones aritméticas y matemáticas, de movimiento de datos y de cambios o saltos en la secuencia de ejecución. La CPU interpreta la información que proviene del sistema de almacenamiento del dispositivo, que puede ser tanto un programa, un dato o un conjunto de datos con los que operar.

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.

Datos SMART: (En español, datos inteligentes). También SMART data. Datos que realmente poseen un valor estratégico para la organización.

Disponibilidad: Capacidad de un servicio, de unos datos o de un sistema, a ser accesible y utilizable por los usuarios o procesos autorizados cuando estos lo requieran. Es uno de los principios fundamentales de la ciberseguridad junto a la confidencialidad y la integridad.

DLP: (Data Loss Prevention. En español, prevención de fuga de datos). Herramienta que tiene como finalidad prevenir las fugas de información cuyo origen está dentro de la propia organización, de una manera activa y sin perder productividad. Estas herramientas suelen incorporar inteligencia artificial que les permite aprender sobre el tipo de documentos confidenciales que se utilizan y qué acciones llevan a cabo los usuarios sobre los mismos, para volverse cada vez más efectivas en la prevención de fugas de información.

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.

Dominio: Nombre único y exclusivo que se le da a un sitio web en Internet para que cualquiera pueda visitarlo.

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.

Framework: (Anglicismo). Marco o esquema de trabajo generalmente utilizado por programadores para realizar el desarrollo de "software". Utilizar un "framework" permite agilizar los procesos de desarrollo ya que evita tener que escribir código de forma repetitiva, asegura unas buenas prácticas y la consistencia del código.

Hardware: (Anglicismo). Conjunto de los componentes que conforman la parte material (física) de una computadora.

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.

Interfaz: Conexión física y funcional que se establece entre dos aparatos, programas, dispositivos o sistemas que funcionan independientemente uno del otro o entre persona y máquina (interfaz de usuario).

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.

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.

Latiguillo: Pieza hueca en forma de tubo flexible, generalmente reforzado, que sirve para unir o empalmar dos objetos.

LED: (Light-Emitting Diode. En español, diodo emisor de luz). Dispositivo que produce luz al pasa la electricidad en un sentido y no en el inverso. Es decir, tiene que existir una corriente circular de un término positivo (ánodo) a uno negativo (cátodo). Es aquí cuando se produce el llamado “fotón” al desprenderse los electrones y se produce luz. El proceso de electroluminiscencia es mucho más eficiente que el proceso de incandescencia de una bombilla con filamento ya que la energía se destina directamente a generar luz y no a generar calor. Se usa frecuentemente como indicador de actividad en dispositivos.

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.

Mantenimiento preventivo: Acción de revisar de forma sistemática y con criterios determinados los equipos o aparatos de cualquier tipo (mecánicos, eléctricos, informáticos, etc.), para evitar averías ocasionadas por uso, desgaste o tiempo de vida útil.

Monitorización: Acción realizada por elementos físicos y "software" que registran la situación en que están cada uno de los aspectos que se desean controlar.

Nodo: Punto de conexión que puede recibir, crear, almacenar o enviar datos a lo largo de rutas de red distribuidas. Cada nodo de la red, ya sea un punto final para la transmisión de datos o un punto de redistribución, tiene una capacidad programada o diseñada para reconocer, procesar y reenviar transmisiones a otros nodos de la red.

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

Parche: Nueva versión de un software o de parte de él que incluye más y mejores funcionalidades y/o soluciona fallos de la versión precedente.

Parsear: En inglés parsing. También parseo. Proceso de analizar una secuencia de símbolos a fin de determinar su estructura gramatical definida. También llamado análisis de sintaxis.

Protocolo: Conjunto de normas y procedimientos establecidos para el desarrollo de una actuación.

RAM: (Random Access Memory. En español, memoria de acceso aleatorio). Componente físico de un sistema informático donde se guardan temporalmente los datos, las aplicaciones y/o el sistema operativo (o partes del mismo) actualmente en ejecución (procesos) de manera que puedan ser leídos de manera rápida por el procesador de la máquina.

Registro log: Archivo de texto en el que constan cronológicamente los acontecimientos que han ido afectando a un sistema informático (programa, aplicación, servidor, etc.), así como el conjunto de cambios que estos han generado.

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.

SIEM: (Security Information and Event Management. En español, gestión de información y eventos de seguridad). Solución de seguridad que ayuda a las organizaciones a reconocer posibles amenazas y vulnerabilidades de seguridad antes de que tengan la oportunidad de interrumpir operaciones empresariales.

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.

Software de base: También "Software" base o "software" de sistema. Programa o conjunto de programas que se encargan de gestionar las funciones que dan soporte al resto de aplicaciones que soporta un dispositivo o sistema informático, que puede ser un servidor, ordenador de sobremesa, teléfono móvil o "tablet", entre otros. Usualmente son "software base" o "software de base" todo el "firmware", controladores y programas del sistema que constituyen el sistema operativo y ciertas utilidades asociadas.

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.