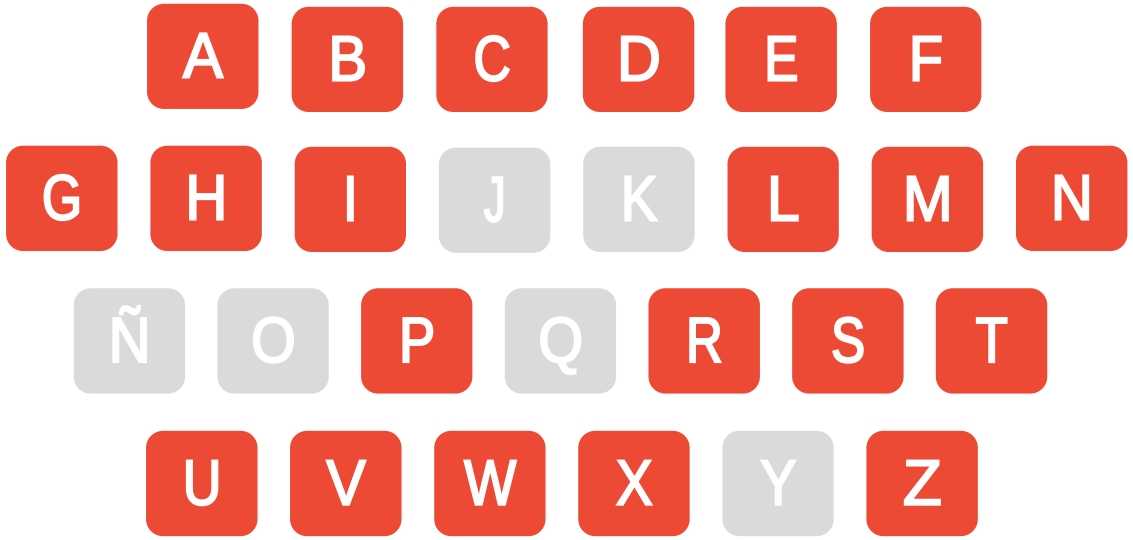
GLOSARIO

CIBERSEGURIDAD



A

- **Activo de información.** Es cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización.
- **Acuerdo de licencia.** Es una cesión de derechos entre un titular de derechos de propiedad intelectual (licenciante) y otra persona que recibe la autorización de utilizar dichos derechos (licenciatario) a cambio de un pago convenido de antemano (tasa o regalía) o de unas condiciones determinadas.
- **Administración electrónica.** Actividad consistente en la prestación de servicios a ciudadanos y empresas mediante la utilización de medios telemáticos y definida en la Ley 11/2007 de 22 de junio de acceso electrónico de los ciudadanos a los servicios públicos. Esta actividad compete a las Administraciones Públicas con el objeto de simplificar los procedimientos con la Administración, manteniendo al mismo tiempo, los niveles adecuados de seguridad jurídica y procurando la mejora de calidad de los servicios.
- **Adware.** Es cualquier programa que automáticamente va mostrando publicidad al usuario durante su instalación o durante su uso y con ello genera beneficios a sus creadores. Aunque se asocia al malware, no tiene que serlo forzosamente, ya que puede ser un medio legítimo usado por desarrolladores de software que lo implementan en sus programas, generalmente en las versiones shareware, haciéndolo desaparecer en el momento en que adquirimos la versión completa del programa. Se convierte en malware en el momento en que empieza a recopilar información sobre el ordenador donde se encuentra instalado.

- **Algoritmos de cifrado.** Operación o función matemática utilizada en combinación con una clave que se aplica a un texto en claro y permite obtener un texto cifrado (o descifrarlo) garantizando la confidencialidad e integridad de la información contenida.

- **Amenaza.** Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Una amenaza puede tener causas naturales, ser accidental o intencionada. Si esta circunstancia desfavorable acontece a la vez que existe una vulnerabilidad o debilidad de los sistemas o aprovechando su existencia, puede derivar en un incidente de seguridad.

- **Antivirus.** Es un programa informático específicamente diseñado para detectar, bloquear y eliminar código malicioso (virus, troyanos, gusanos, etc.), así como proteger los equipos de otros pro - gramas peligrosos conocidos genéricamente como malware. La forma de actuar del antivirus parte de una base de datos que contiene parte de los códigos utilizados en la creación de virus conocidos. El programa antivirus compara el código binario de cada archivo ejecutable con esta base de datos. Además de esta técnica, se valen también de procesos de monitorización de los programas para detectar si éstos se comportan como programas maliciosos.

- **Análisis de riesgos.** Es un proceso que comprende la identificación de activos de información, sus vulnerabilidades y las amenazas a los que se encuentran expuestos, así como la probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para tratar el riesgo.

- **Ataque de fuerza bruta.** Un ataque de fuerza bruta es un procedimiento para averiguar una contraseña que consiste en probar todas las combinaciones posibles hasta encontrar la combinación correcta. Los ataques por fuerza bruta, dado que utilizan el método de prueba y error, tardan mucho tiempo en encontrar la combinación correcta (hablamos en ocasiones de miles años), por esta razón, la fuerza bruta suele combinarse con un ataque de diccionario.

- **Ataque combinado.** Es uno de los ataques más agresivos ya que se vale de métodos y técnicas muy sofisticadas que combinan distintos virus informáticos, gusanos, troyanos y códigos maliciosos, entre otros. Esta amenaza se caracteriza por utilizar el servidor y vulnerabilidades de Internet para iniciar, transmitir y difundir el ataque extendiéndose rápidamente y ocasionando graves daños, en su mayor parte, sin requerir intervención humana para su propagación.

- **Ataque de repetición.** Es un tipo de ataque en el cual el atacante captura la información que viaja por la red, por ejemplo un comando de autenticación que se envía a un sistema informático, para, posteriormente, enviarla de nuevo a su destinatario, sin que este note que ha sido capturada. Si el sistema informático o aplicación es vulnerable a este tipo de ataques, el sistema ejecutará el comando, como si fuera legítimo, enviando la respuesta al atacante que puede así obtener acceso al sistema. Para protegerse de este tipo de ataques el sistema informático puede tomar medidas como usar un control de identificación de comandos, de sellado de tiempos (timestamp), etc. junto con el cifrado y la firma de los comandos con el fin de evitar que sean reutilizados.

- **Auditoría de seguridad.** Es el estudio que comprende el análisis y gestión de sistemas llevado a cabo por profesionales en tecnologías de la información (TI) con el objetivo de identificar, enumerar y describir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones, servidores o aplicaciones.

- **Autenticación.** Procedimiento para comprobar que alguien es quién dice ser cuando accede a un ordenador o a un servicio online. Este proceso constituye una funcionalidad característica para una comunicación segura.

- **Autoridad de certificación.** La Autoridad de Certificación (AC o CA, por sus siglas en inglés, Certification Authority) es una entidad de confianza cuyo objeto es garantizar la identidad de los titulares de certificados digitales y su correcta asociación a las claves de firma electrónica.

- **Autoridad de registro.** Es la entidad encargada de identificar de manera inequívoca a los usuarios para que, posteriormente, éstos puedan obtener certificados digitales.

- **Autoridad de validación.** Entidad que informa de la vigencia y validez de los certificados electrónicos creados y registrados por una Autoridad de Registro y por una Autoridad de Certificación. Asimismo, las autoridades de validación almacenan la información sobre los certificados electrónicos anulados en las listas de revocación de certificados (CRL).

- **Aviso Legal.** Un aviso legal es un documento, en una página web, donde se recogen las cuestiones legales que son exigidas por la normativa de aplicación.

B

- **B2B.** Abreviatura de «Business to Business». Este término se refiere a las transacciones comercia- les entre empresas, utilizando medios telemáticos como EDI (Electronic Data Interchange) o el Comercio Electrónico.

- **B2C.** Abreviatura de «Business to Consumer». Este término se refiere a la estrategia que desarrollan las empresas comerciales para llegar directamente al cliente o consumidor final. Suele también indicar las transacciones realizadas directamente entre un cliente y una empresa sin que medie un intermediario.

- **Backup.** Copia de seguridad que se realiza sobre ficheros o aplicaciones contenidas en un ordenador con la finalidad de recuperar los datos en el caso de que el sistema de información sufra daños o pérdidas accidentales de los datos almacenados. Los dispositivos más empleados para llevar a cabo la técnica de backup pueden ser discos duros, discos ópticos, USB o DVD. También es común la realización de copias de seguridad mediante servicios de copia basados en la nube. Es de suma importancia mantener actualizada la copia de seguridad así como tener la máxima diligencia de su resguardo, para evitar pérdidas de información que pueden llegar a ser vitales para el funcionamiento ya sea de una empresa, institución o de un contenido de tipo personal. Además, cada cierto tiempo es conveniente comprobar que la copia de seguridad puede restaurarse con garantías.

- **BIA.** Abreviatura de «Business Impact Analysis». Se trata de un informe que nos muestra el coste ocasionado por la interrupción de los procesos críticos de negocio. Este informe nos permitirá asignar una criticidad a los procesos de negocio, definir los objetivos de recuperación y determinar un tiempo de recuperación a cada uno de ellos.

- **Biometría.** La biometría es un método de reconocimiento de personas basado en sus características fisiológicas (huellas dactilares, retinas, iris, cara, etc.) o de comportamiento (firma, forma de andar, tecleo, etc.). Se trata de un proceso similar al que habitualmente realiza el ser humano reconociendo e identificando a sus congéneres por su aspecto físico, su voz, su forma de andar, etc. Para la identificación del individuo es necesario que los rasgos o características analizadas sean de carácter universal, ser lo suficientemente distintas a las de otra persona, permanecer de forma constante e invariante en el individuo y además, poder ser medida.

- **Bluetooth.** La tecnología Bluetooth es una tecnología inalámbrica de radio de corto alcance, cuyo objetivo es eliminar los cables en las conexiones entre dispositivos electrónicos, simplificando así las comunicaciones entre teléfonos móviles, ordenadores, cámaras digitales y otros dispositivos informáticos operando bajo la banda de radio de 2.4 GHz de frecuencia. Este protocolo ofrece a los dispositivos la posibilidad de comunicarse cuando se encuentran a una distancia de hasta 10 metros, incluso a pesar de que pueda existir algún obstáculo físico o a pesar de que los usuarios de los dispositivos se encuentren en distintas habitaciones de un mismo emplazamiento.

- **Bomba Lógica.** Trozo de código insertado intencionalmente en un programa informático que permanece oculto hasta cumplirse una o más condiciones preprogramadas, momento en el que se ejecuta una acción maliciosa. La característica general de una bomba lógica y que lo diferencia de un virus es que este código insertado se ejecuta cuando una determinada condición se produce, por ejemplo, tras encender el ordenador una serie de veces, o pasados una serie de días desde el momento en que la bomba lógica se instaló en nuestro ordenador.

- **Botnet.** Una botnet es un conjunto de ordenadores (denominados bots) controlados remotamente por un atacante que pueden ser utilizados en conjunto para realizar actividades maliciosas como envío de spam, ataques de DDoS, etc. Las botnets se caracterizan por tener un servidor central (C&C, de sus siglas en inglés Command & Control) al que se conectan los bots para enviar información y recibir comandos.

- **Bug.** Es un error o fallo en un programa de dispositivo o sistema de software que desencadena un resultado indeseado.

- **Bulo.** También llamados hoax, son noticias falsas creadas para su reenvío masivo ya sea a través de redes sociales, mensajería instantánea o correo electrónico, con el fin de hacer creer al destinatario que algo es falso. Pueden ser varias las motivaciones para crear este tipo de noticias, como difundir información falsa en perjuicio de terceras personas u organismos o incitar al receptor del mensaje a causar daños en su propio ordenador.

C

- **Cartas nigerianas.** Se trata de una comunicación inesperada mediante correo electrónico carta o mensajería instantánea en las que el remitente promete negocios muy rentables. La expectativa de poder ganar mucho dinero mediante unas sencillas gestiones, es el gancho utilizado por los estafadores para involucrar a las potenciales victimas en cualquier otra situación engañosa, procurando que finalmente transfiera una fuerte cantidad de dinero para llevar a cabo la operación.

- **Centro de respaldo.** Un centro de respaldo es un centro de procesamiento de datos (CPD) específicamente diseñado para tomar el control de otro CPD principal en caso de contingencia.
- **Certificado de autenticidad.** El Certificado de autenticidad (COA) es una etiqueta especial de seguridad que acompaña a un software con licencia legal para impedir falsificaciones. El COA suele ir pegado en el embalaje del software, y permite asegurar que el software y los demás elementos que contenga, como los medios y los manuales, son auténticos. En ocasiones el software viene preinstalado al comprar un equipo. En esos casos el COA suele encontrarse en el exterior del equipo. Si se trata de un dispositivo pequeño (con una longitud o anchura de 15 cm o menos), el COA puede encontrarse bajo la batería.
- **Certificado digital.** Un certificado digital es un fichero informático generado por una entidad denominada Autoridad Certificadora (CA) que asocia unos datos de identidad a una persona física, organismo o empresa confirmando de esta manera su identidad digital en Internet. El certificado digital es válido para autenticar la existencia y validez de un usuario o sitio web por lo que es necesaria la colaboración de un tercero que sea de confianza para cualquiera de las partes que participe en la comunicación. El nombre asociado a esta entidad de confianza es Autoridad Certificadora pudiendo ser un organismo público o empresa reconocida en Internet. El certificado digital tiene como función principal autenticar al poseedor pero puede servir también para cifrar las comunicaciones y firmar digitalmente. En algunas administraciones públicas y empresas privadas es requerido para poder realizar ciertos trámites que involucren intercambio de información sensible entre las partes.
- **Cesión de datos.** La cesión de datos es la comunicación de datos de carácter personal a una tercera persona sin el consentimiento del interesado. La comunicación de este tipo de datos está regulada en el artículo 11 de la LOPD, mientras que la comunicación de datos entre Administraciones públicas se regula en el artículo 21 de dicha ley.

- **Clave pública.** Los sistemas de criptografía asimétrica, se basan en la generación, mediante una «infraestructura de clave pública», de un par de claves, denominadas clave pública y clave privada, que tienen la peculiaridad de que los mensajes cifrados con una de ellas sólo pueden ser descifrados utilizando la otra. Así, se conoce como clave pública a una de estas claves, que puede ponerse en conocimiento de todo el mundo y que utilizará un remitente para cifrar el mensaje o documento que quiere enviar, garantizando de esta forma que tan solo pueda descifrarlo el destinatario con su clave privada.

- **Clave privada.** Los sistemas de criptografía asimétrica, se basan en la generación de un par de claves, denominadas clave pública y clave privada, que tienen la peculiaridad de que los mensajes cifrados con una de ellas sólo pueden ser descifrados utilizando la otra. En este tipo de sistemas, la clave privada sólo debe ser conocida por el usuario para el cifrado y descifrado de mensajes.

- **Cloud computing.** El término cloud computing o computación en la nube se refiere a un paradigma que permite ofrecer servicios de computación a través de una red, que usualmente es Internet. Esta tendencia permite a los usuarios almacenar información, ficheros y datos en servidores de terceros, de forma que puedan ser accesibles desde cualquier terminal con acceso a la nube o a la red, resultando de esta manera innecesaria la instalación de software adicional (al que facilita el acceso a la red) en el equipo local del usuario.

- **Confidencialidad.** Confidencialidad es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información. La confidencialidad de la información constituye la piedra angular de la seguridad de la información. Junto con la integridad y la disponibilidad suponen las tres dimensiones de la seguridad de la información.

- **Control parental.** Conjunto de herramientas o medidas que se pueden tomar para evitar que los menores de edad hagan un uso indebido del ordenador, accedan a contenidos inapropiados o se expongan a riesgos a través de Internet. Estas herramientas tienen la capacidad de bloquear, restringir o filtrar el acceso a determinados contenidos o programas, accesibles a través de un ordenador o de la red, y de dotar de un control sobre el equipo y las actividades que se realizan con él, a la persona que sea el administrador del mismo, que normalmente deberá ser el padre o tutor del menor.

- **Cookie.** Una cookie es un pequeño fichero que almacena información enviada por un sitio web y que se almacena en el equipo del usuario, de manera que el sitio web puede consultar la actividad previa del usuario.

- **Cortafuegos.** Sistema de seguridad compuesto o bien de programas (software) o de dispositivos hardware situados en los puntos limítrofes de una red que tienen el objetivo de permitir y limitar, el flujo de tráfico entre los diferentes ámbitos que protege sobre la base de un conjunto de normas y otros criterios. La funcionalidad básica de un cortafuego es asegurar que todas las comunicaciones entre la red e Internet se realicen conforme a las políticas de seguridad de la organización o corporación. Estos sistemas suelen poseer características de privacidad y autentificación.

- **Criptografía.** La criptografía es la técnica que consiste en cifrar un mensaje, conocido como texto en claro, convirtiéndolo en un mensaje cifrado o criptograma, que resulta ilegible para todo aquel que no conozca el sistema mediante el cual ha sido cifrado. Existen dos tipos principales de criptografía: por un lado, la conocida como criptografía simétrica, más tradicional, y la criptografía asimétrica o de clave pública.

- **CRL.** Cuando una autoridad de certificación emite un certificado digital, lo hace con un periodo máximo de validez (por ejemplo cuatro años). El objetivo de este periodo de caducidad es obligar a la renovación del certificado para adaptarlo a los cambios tecnológicos. Así se disminuye el riesgo de que el certificado quede comprometido por un avance tecnológico. La fecha de caducidad viene indicada en el propio certificado digital.

- **Códigos de conducta.** En el ámbito de las TIC, los códigos de conducta son aquellas recomendaciones o reglas que tienen por finalidad determinar las normas deontológicas aplicables en el ámbito de la tecnología y la informática con el objeto de proteger los derechos fundamentales de los usuarios. En definitiva, un código de conducta es un conjunto de normas y obligaciones que asumen las personas y entidades que se adscriben al mismo y mediante las cuales se pretende fomentar la confianza y la seguridad jurídica, así como una mejor tramitación de cualquier problema o incidencia.

D

- **Denegación de servicio.** Se entiende como denegación de servicio, en términos de seguridad informática, a un conjunto de técnicas que tienen por objetivo dejar un servidor inoperativo. Mediante este tipo de ataques se busca sobrecargar un servidor y de esta forma impedir que los usuarios legítimos puedan utilizar los servicios por prestados por él. El ataque consiste en saturar con peticiones de servicio al servidor, hasta que éste no puede atenderlas, provocando su colapso.

- **Desbordamiento de búfer.** Es un tipo de vulnerabilidad muy utilizada con la que se persigue conseguir acceso remoto al sistema atacado. Un desbordamiento de búfer intenta aprovechar defectos en la programación que provocan un error o el cuelgue del sistema. Un desbordamiento de búfer provoca algo similar a lo que ocurre cuando llenamos un vaso más allá de su capacidad: éste se desborda y el contenido se derrama. Cuando el programador no incluye las medidas necesarias para comprobar el tamaño del búfer en relación con el volumen de datos que tiene que alojar, se produce también el derramamiento de estos datos que se sobrescriben en otros puntos de la memoria, lo cual puede hacer que el programa falle. El atacante calcula qué cantidad de datos necesita enviar y dónde se reescribirán los datos, para a continuación enviar comandos que se ejecutarán en el sistema. Este tipo de vulnerabilidad, dado que se produce por un defecto en el código del programa, sólo puede ser solventada mediante las actualizaciones o parches del programa en cuestión. Por esta razón es imprescindible mantener actualizados todos los programas instala- dos en nuestros equipos y servidores.

- **Dirección IP.** Las direcciones IP (del acrónimo inglés IP para Internet Protocol) son un número único e irrepetible con el cual se identifica a todo sistema conectado a una red. Podríamos compararlo con una matrícula en un coche. Así, una dirección IP (o simplemente IP) en su versión v4 es un conjunto de cuatro números del 0 al 255 separados por puntos. Por ejemplo: 192.168.121.40. En su versión v6, las direcciones IP son mucho más complejas, siendo hasta 4 veces más largas, más seguras y permitiendo un gran número de sistemas conectados a Internet. Un ejemplo es el siguiente: 2001:0db8:3c4d:0015:0000:0000:1a2f:1a2b. Las direcciones IP pueden ser «públicas», si son accesibles directamente desde cualquier sistema conectado a Internet o «privadas», si son internas a una red LAN y solo accesibles desde los equipos conectados a esa red privada.

- **Dirección MAC.** Una dirección MAC, también conocida como dirección física, es un valor de 48 bits único e irrepetible que identifica todo dispositivo conectado a una red. Cada dispositivo tiene su propia dirección MAC determinada que es única a nivel mundial ya que es escrita directa- mente, en forma binaria, en el hardware del interfaz de red en el momento de su fabricación. El acrónimo MAC hace referencia a Media Access Control que traducido al español significa Control de Acceso al Medio.

- **Disponibilidad.** Se trata de la capacidad de un servicio, un sistema o una información, a ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran. Junto con la integridad y la confidencialidad son las tres dimensiones de la seguridad de la información.

- **DNS.** El término DNS, del inglés Domain Name Service, se refiere tanto al servicio de Nombres de Dominio, como al servidor que ofrece dicho servicio. El servicio DNS asocia un nombre de dominio con información variada relacionada con ese dominio. Su función más importante es traducir nombres inteligibles para las personas en direcciones IP asociados con los sistemas conectados a la red con el propósito de poder localizar y direccionar estos sistemas de una forma mucho más simple.

E

- **Exploit.** Secuencia de comandos utilizados para, aprovechándose de un fallo o vulnerabilidad en un sistema, provocar un comportamiento no deseado o imprevisto.

F

- **Firma electrónica.** La firma electrónica (o digital) se define como el conjunto de datos electrónicos que acompañan o que están asociados a un documento electrónico. Una firma electrónica de un documento se consigue calculando el valor «hash» del documento y adjuntándolo al final del mismo, para a continuación cifrarlo con la clave pública de la persona a la que enviaremos el documento. De esta manera nadie pueda leerlo más que el receptor.

- **Fuga de datos.** La fuga de datos o fuga de información es la pérdida de la confidencialidad de la información privada de una persona o empresa. Información que, a priori, no debería ser conocida más que por un grupo de personas, en el ámbito de una organización, área o actividad, y que termina siendo visible o accesible para otros.

- **FTP.** Por FTP (del acrónimo inglés File Transfer Protocol) se hace referencia a un servicio de transferencia de ficheros a través de una red, así como a los servidores que permiten prestar este servicio. Mediante este servicio, desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.

G

- **Gusano.** Es un programa malicioso (o malware) que tiene como característica principal su alto grado de «dispersabilidad», es decir, lo rápidamente que se propaga. Mientras que los troyanos dependen de que un usuario acceda a una web maliciosa o ejecute un fichero infectado, los gusanos realizan copias de sí mismos, infectan a otros ordenado- res y se propagan automáticamente en una red independientemente de la acción humana. Su fin es replicarse a nuevos sistemas para infectarlos y seguir replicándose a otros equipos informáticos, aprovechándose de todo tipo de medios como el correo electrónico, IRC, FTP, correo electrónico, P2P y otros protocolos específicos o ampliamente utilizados.

H

- **HTTP.** HTTP son las siglas en inglés de Protocolo de Transferencia de Hipertexto. Se trata del protocolo más utilizado para la navegación web. Se trata de un protocolo que sigue un esquema petición-respuesta. El navegador realiza peticiones de los recursos que necesita (la web, las imágenes, los videos...) y el servidor se los envía si dispone de ellos. A cada pieza de información transmitida se la identifica mediante un identificador llamado URL (del inglés Uniform Resource Locator). La información enviada mediante HTTP se envía en texto claro, lo que quiere decir que cualquiera que intercepte el tráfico de red puede leer lo que se está enviando y recibiendo. Por esta razón se desarrolló el protocolo HTTPS, en el que la información es cifrada antes de ser enviada por la red.

- **HTTPS.** Protocolo seguro de transferencia de hipertexto, más conocido por sus siglas HTTPS, del inglés Hypertext Transfer Protocol Secure, es un protocolo de red basado en el protocolo HTTP, destinado a la transferencia segura de datos de hipertexto. Dicho en otras palabras, es la versión segura de HTTP. En HTTPS el tráfico HTTP es cifrado mediante un algoritmo de cifrado simétrico cuya clave ha sido previamente intercambiada entre el navegador y el servidor. Es utilizado por cualquier tipo de servicio que requiera el envío de datos personales o contraseñas, entidades bancarias, tiendas en línea, pago seguro, etc.

- **IDS.** Un sistema de detección de intrusos (o IDS de sus siglas en inglés Intrusion Detection System) es una aplicación usada para detectar accesos no autorizados a un ordenador o a una red. Estos accesos pueden ser ataques realizados por usuarios malintencionados con conocimientos de seguridad o usando herramientas automáticas. A diferencia de los IPS, estos sistemas sólo detectan intentos de acceso y no tratan de prevenir su ocurrencia.

- **Incidente de seguridad.** Cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa, por ejemplo: acceso o intento de acceso a los sistemas, uso, divulgación, modificación o destrucción no autorizada de información.

- **Informática forense.** La informática forense consiste en un proceso de investigación de los sistemas de información para detectar toda evidencia que pueda ser presentada como prueba fehaciente en un procedimiento judicial. Para esta investigación se hace necesaria la aplicación de técnicas científicas y analíticas especializadas que permitan identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal. Entre las técnicas mencionadas se incluyen reconstruir el sistema informático, examinar datos residuales y explicar las características técnicas del uso aplicado a los datos y bienes informáticos. Su implementación debe llevarse a cabo considerando lo dispuesto por la normativa legal aplicable, a efectos de no vulnerar los derechos de protección de datos y de intimidad de terceros.

- **Infraestructura de clave pública.** También conocido por las siglas PKI (del inglés Public Key Infrastructure), una infraestructura de clave pública es un conjunto de elemento Hardware, Software, políticas y procedimientos de actuación encaminados a la ejecución con garantías de operaciones de cifrado y criptografía, tales la firma, el sellado temporal o el no repudio de transacciones electrónicas.

- **Ingeniería social.** Las técnicas de ingeniería social son tácticas utilizadas para obtener información datos de naturaleza sensible, en muchas ocasiones claves o códigos, de una persona. Estas técnicas de persuasión suelen valerse de la buena voluntad y falta de precaución de la víctima.

- **Integridad.** La Integridad es la propiedad de la información, por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de software o hardware o por condiciones medioambientales. La integridad, la disponibilidad y la confidencialidad constituyen las dimensiones claves en la seguridad de la información, ya que de un lado, se pretende evitar los accesos no auto- rizados a los datos, y de otro, se garantiza la no alteración de los mismos.

- **Inyección SQL.** Es un tipo de ataque que se aprovecha de una vulnerabilidad en la validación de los contenidos introducidos en un formulario web y que puede permitir la obtención de forma ilegítima de los datos almacenados en la base de datos del sitio web, entre ellos las credenciales de acceso.

- **IPS.** Siglas de Intrusion Prevention System (sistema de prevención de intrusiones). Es un software que se utiliza para proteger a los sistemas de ataques y abusos. La tecnología de prevención de intrusos puede ser considerada como una extensión de los sistemas de detección de intrusos (IDS), pero en realidad es una tecnología más cercana a los cortafuegos.

L

- **LAN.** Una LAN (del inglés Local Area Network) o Red de Área Local es una red informática de pequeña amplitud geográfica, que suele limitarse a espacios como una oficina, una vivienda o un edificio. Una Red de Área Local permite interconectar distintos dispositivos todo tipo, ordenadores, impresoras, servidores, discos duros externos, etc. Las Redes de Área Local pueden ser cableadas o no cableadas, también conocidas como redes inalámbricas. Por término general las redes cableadas son más rápidas y seguras, pero impiden la movilidad de los dispositivas.

M

- **Malware.** Es un tipo de software que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información. Palabra que nace de la unión de los términos en inglés de software malintencionado: malicious software. Dentro de esta definición tiene cabida un amplio elenco de programas maliciosos: virus, gusanos, troyanos, backdoors, spyware, etc. La nota común a todos estos programas es su carácter dañino o lesivo.

- **Metadatos.** Los metadatos son el conjunto de datos relacionados con un documento y que recogen información fundamentalmente descriptiva del mismo, así como información de administración y gestión. Es una información que enriquece el documento al que está asociado. Por ejemplo, se podría considerar como una analogía al uso de índices que se emplean en una biblioteca, donde gracias a datos del tipo: autor, títulos, etcétera se nos permite localizar un libro en concreto. Otro ejemplo de uso es mejorar las consultas en los buscadores consiguiendo una mayor precisión en los resultados.

N

- **No repudio.** El no repudio en el envío de información a través de las redes es capacidad de demostrar la identidad del emisor de esa información. El objetivo que se pretende es certificar que los datos, o la información, provienen realmente de la fuente que dice ser. El problema del control de autenticidad dentro de los sistemas de información a través de la Red, en relación tanto de la identidad del sujeto como del contenido de los datos, puede ser resuelto mediante la utilización de la firma electrónica (o digital).

P

- **P2P.** P2P (del inglés Peer-to-Peer) es un modelo de comunicaciones entre sistemas o servicios en el cual todos los nodos/extremos son iguales, tienen las mismas capacidades y cualquiera de ellas puede iniciar la comunicación. Se trata de un modelo opuesto al cliente/servidor en donde el servidor se encuentra a la espera de una comunicación por parte del cliente. El modelo P2P se basa en que todos los nodos actúan como servidores y clientes a la vez. Una red P2P es por tanto una red de sistemas o servicios que utiliza un modelo P2P. Todos los sistemas/servicios conectados entre sí y que se comportan como iguales con un objetivo en común.

- **Parche de seguridad.** Un parche de seguridad es un conjunto de cambios que se aplican a un software para corregir errores de seguridad en programas o sistemas operativos. Generalmente los parches de seguridad son desarrollados por el fabricante del software tras la detección de una vulnerabilidad en el software y pueden instalarse de forma automática o manual por parte del usuario.

- **Pentest.** Una prueba de penetración es un ataque a un sistema software o hardware con el objetivo de encontrar vulnerabilidades. El ataque implica un análisis activo de cualquier vulnerabilidad potencial, configuraciones deficientes o inadecuadas, tanto de hardware como de software, o deficiencias operativas en las medidas de seguridad. Este análisis se realiza desde la posición de un atacante potencial y puede implicar la explotación activa de vulnerabilidades de seguridad. Tras la realización del ataque se presentará una evaluación de seguridad del sistema, indicando todos los problemas de seguridad detectados junto con una propuesta de mitigación o una solución técnica. La intención de una prueba de penetración es determinar la viabilidad de un ataque y el impacto en el negocio de un ataque exitoso.

- **PCI DSS.** PCI DSS (del Inglés Payment Card Industry Data Security Standard) es, como su nombre indica un Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago. Este estándar ha sido desarrollado por un comité conformado por las compañías de tarjetas más importantes, comité denominado PCI SSC (Payment Card Industry Security Standards Council) como una guía que ayude a las organizaciones que procesan, almacenan o transmiten datos de tarjetas (o titulares de tarjeta), a asegurar dichos datos, con el fin de prevenir los fraudes que involucran tarjetas de pago.

- **Pharming.** Ataque informático que aprovecha una vulnerabilidad del software de los servidores DNS y que consiste en modificar o sustituir el archivo del servidor de nombres de dominio cambiando la dirección IP legítima de una entidad (comúnmente una entidad bancaria) de manera que en el momento en el que el usuario escribe el nombre de dominio de la entidad en la barra de direcciones, el navegador redirigirá automáticamente al usuario a una dirección IP donde se aloja una web falsa que suplantará la identidad legítima, obteniéndose de forma ilícita las claves de acceso de los clientes.

- **Phishing.** Es la denominación que recibe la estafa cometida a través de medios telemáticos mediante la cual el estafador intenta conseguir, de usuarios legítimos, información confidencial (contraseñas, datos bancarios, etc.) de forma fraudulenta. El estafador suplanta la personalidad de una persona o empresa de confianza para que el receptor de una comunicación electrónica aparentemente oficial (vía e-mail, fax, SMS o telefónicamente) crea en su veracidad y facilite, de este modo, los datos privados que resultan de interés para el estafador. Existen diferentes modalidades de phishing. Cuando éste se realiza vía SMS el nombre técnico es smishing y cuando se realiza utilizando Voz sobre IP, se denomina vishing. Otra variedad es el spear phishing, en la que los atacantes intentan mediante un correo electrónico, que aparenta ser de un amigo o de empresa conocida, conseguir que les facilitemos números de tarjeta de crédito, cuentas bancarias o contraseñas.

- **PGP.** Pretty Good Privacy, más conocido como PGP, es un programa para proteger la información transmitida por internet mediante el uso de criptografía de clave pública, así como facilitar la autenticación de documentos mediante firma electrónica. PGP protege no solo los datos durante su tránsito por la Red, como para proteger archivos almacenados en disco. PGP goza de gran popularidad por su facilidad de uso y por su alto nivel de fiabilidad. El estándar de Internet OpenPGP, basado en PGP, es uno de los estándares de cifrado de correo electrónico más utilizados.

- **Plan de contingencia** Un Plan de Contingencia de las Tecnologías de la Información y las Comunicaciones (TIC) consiste en una estrategia planificada en fases, constituida por un conjunto de recursos de respaldo, una organización de emergencia y unos procedimientos de actuación, encaminados a conseguir una restauración ordenada, progresiva y ágil de los sistemas de información que soportan la información y los procesos de negocio considerados críticos en el Plan de Continuidad de Negocio de la compañía.

- **Plan de continuidad.** Un Plan de Continuidad de Negocio es un conjunto formado por planes de actuación, planes de emergencia, planes financieros, planes de comunicación y planes de contingencias destinados a mitigar el impacto provocado por la concreción de determinados riesgos sobre la información y los procesos de negocio de una compañía.

- **Política de seguridad.** Son las decisiones o medidas de seguridad que una empresa ha decidido tomar respecto a la seguridad de sus sistemas de información después de evaluar el valor de sus activos y los riegos a los que están expuestos. Este término también se refiere al documento de nivel ejecutivo mediante el cual una empresa establece sus directrices de seguridad de la información.

- **Protocolo.** Es un sistema de reglas que permiten que dos o más entidades se comuniquen entre ellas para transmitir información por medio de cualquier tipo de medio físico. Se trata de las reglas o el estándar que define la sintaxis, semántica y sincronización de la comunicación, así como también los posibles métodos de recuperación de errores. Los protocolos pueden ser implementados por hardware, por software, o por una combinación de ambos.

- **Proveedor de acceso.** Se denomina proveedor de acceso (a Internet) a todos los prestadores de servicios de la Sociedad de la Información que proporcionan a sus usuarios/clientes acceso a redes de tele- comunicaciones, tanto fijas como móviles. En inglés se denomina ISP, acrónimo de Internet Service Provider.

- **Proxy.** El proxy es tanto el equipo, como el software encargado de dar el servicio, que hacen de intermediario en las peticiones de los equipos de la redes LAN hacia Internet. Su cometido es centralizar el tráfico entre Internet y una red privada, de forma que se evita que cada una de las máquinas de la red privada tenga que disponer necesariamente de una conexión directa a Internet y una dirección IP pública. Al mismo tiempo un proxy puede proporcionar algunos mecanismos de seguridad (firewall) que impiden accesos no autorizados desde el exterior a la red privada.

- **Puerta trasera.** Se denomina backdoor o puerta trasera a cualquier punto débil de un programa o sistema mediante el cual una persona no autorizada puede acceder a un sistema. Las puertas traseras pueden ser errores o fallos, o pueden haber sido creadas a propósito, por los propios autores pero al ser descubiertas por terceros, pueden ser utilizadas con fines ilícitos. Por otro lado, también se consideran puertas traseras a los programas que, una vez instalados en el ordenador de la víctima, dan el control de éste de forma remota al ordenador del atacante. Por lo tanto aunque no son específicamente virus, pueden llegar a ser un tipo de malware que funcionan como herramientas de control remoto.

R

- **Ransomware.** El ciberdelincuente, toma control del equipo infectado y «secuestra» la información del usuario cifrándola, de tal forma que permanece ilegible si no se cuenta con la contraseña de descifrado. De esta manera extorsiona al usuario pidiendo un rescate económico a cambio de esta contraseña para que, supuestamente, pueda recuperar sus datos. La seguridad del sistema está basada en la dificultad de factorización de grandes números. Su funcionamiento se basa en el envío de un mensaje cifrado mediante la clave pública del destinatario, y una vez que el mensaje cifrado llega, éste se encarga de descifrarlo con su clave privada.

- **Red privada virtual.** Una red privada virtual, también conocida por sus siglas VPN (Virtual Private Network) es una tecnología de red que permite una extensión segura de una red local (LAN) sobre una red pública o no controlada como Internet. Al establecerlas, la integridad de los datos y la confidencialidad se protegen mediante la autentificación y el cifrado. Se trata realmente de una conexión virtual punto a punto entre dos redes LAN usando para la conexión una red pública como es Internet y consiguiendo que esta conexión sea segura gracias al cifrado de la comunicación.

- **RFID.** Siglas de Radio Frequency IDentification, en español Identificación por Radiofrecuencia. Como su nombre indica es un método de identificación de dispositivos por ondas de radio. El propósito fundamental de la tecnología RFID es transmitir la identidad de un objeto (similar a un número de serie único) de una forma inalámbrica. Las etiquetas RFID (RFID Tag, en inglés) son unos dispositivos pequeños, similares a una pega- tina, que pueden ser adheridas o incorporadas a un producto y que contienen una mini-antena que les permitirles recibir y responder a peticiones por radiofrecuencia desde un lector RFID. RFID se utiliza en muchos ámbitos, por ejemplo los arcos de detección en las entradas de las tiendas o los controles de acceso mediante tarjeta por proximidad.

- **Router.** Es un dispositivo que distribuye tráfico de red entre dos o más diferentes redes. Un router está conectado al menos a dos redes, generalmente LAN o WAN y el tráfico que recibe procedente de una red lo redirige hacia la(s) otra(s) red(es). En términos domésticos un router es el dispositivo que proporciona el proveedor de servicios de telefonía (o ISP) y que permite conectar nuestra LAN doméstica con la red del IS. El router comprueba las direcciones de destino de los paquetes de información y decide por qué ruta serán enviados, para determinar el mejor camino emplean cabeceras y tablas de comparación.

- **RSA.** Se trata de un sistema criptográfico de clave pública desarrollado por los criptógrafos Rivest, Shamir y Adleman, de donde toma su nombre. Es el primer y más utilizado algoritmo de este tipo y permite tanto cifrar documentos como firmarlos digitalmente.

S

- **SaaS.** Son las siglas de Software as a Service, es decir la utilización de Software como un servicio. Es un modelo de distribución de software donde tanto el software como los datos que mane- ja se alojan en servidores de un tercero (generalmente el fabricante del software) y el cliente accede a los mismos vía Internet.

- **Servidor.** Puede entenderse como servidor tanto el software que realiza ciertas tareas en nombre de los usuarios, como el ordenador físico en el cual funciona ese software, una máquina cuyo propósito es proveer y gestionar datos de algún tipo de forma que estén disponibles para otras máquinas que se conecten a él. Así, se entiende por servidor tanto el equipo que almacena una determinada información como el programa de software encargado de gestionar dicha información y ofrecerla. Algunos ejemplos de servidores son los que proporcionan el alojamiento de sitios web y los que proporcionan el servicio de envío, reenvío y recepción de correos electrónicos.

- **SGSI.** Un Sistema de Gestión de la seguridad de la Información (SGSI) es un conjunto de políticas de seguridad de la información que siguen la norma ISO/IEC 27001. Un SGSI es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

- **Sistemas de reputación.** En los servicios de compraventa online se suelen adoptar sistemas de reputación. Estos sistemas permiten conocer la opinión de otros compradores y sus experiencias para valorar si el sitio merece nuestra confianza. Estos sistemas permiten que los usuarios que han utilizado un servicio de compraventa on-line publiquen sus opiniones y experiencias con éste y califiquen el servicio. A partir de esta información, nosotros podemos hacernos una idea del nivel de confianza, seguridad y garantía que podemos obtener del servicio si decidimos utilizarlo. Estos sistemas son ventajosos tanto para los propietarios de los servicios de compraventa online como para sus usuarios, por esto, no es de extrañar que las páginas especializadas en compraventa, subastas y venta por Internet demuestren su interés en utilizarlos. Otro ejemplo de sistema de reputación son las listas negras que valoran si una dirección IP son emisoras de spam o que valoran si una dirección IP aloja phishing. Estos sistemas de reputación ayudan a evitar ser víctimas de spam o phishing.

- **SLA.** Un acuerdo de nivel de servicio o ANS (en inglés Service Level Agreement o SLA), es un contrato escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio. El ANS es una herramienta que ayuda a ambas partes a llegar a un consenso en términos del nivel de calidad del servicio, en aspectos tales como tiempo de respuesta, disponibilidad horaria, documentación disponible, personal asignado al servicio, etc.

- **SMTP.** El Protocolo Simple de Transferencia de Correo (o Simple Mail Transfer Protocol del inglés) es un protocolo de red utilizado para el intercambio de mensajes de correo electrónico. Este protocolo, aunque es el más comúnmente utilizado, posee algunas limitaciones en cuanto a la recepción de mensajes en el servidor de destino (cola de mensajes recibidos). Como alternativa a esta limitación crearon los protocolos POP o IMAP, otorgando a SMTP la tarea específica de enviar correo, y recibirlos empleando los otros protocolos antes mencionados (POP O IMAP).

- **Sniffer.** Un sniffer es un programa que monitoriza la información que circula por la red con el objeto de capturar información. Las tarjetas de red pueden verificar si la información recibida está dirigida o no a su sistema. Si no es así, la rechaza. Un sniffer lo que hace es colocar a la placa de red en un modo el cual desactiva el filtro de verificación de direcciones (promiscuo) y por lo tanto acepta todos los paquetes que llegan a la tarjeta de red del ordenador donde está instalado estén dirigidos o no a ese dispositivo. El tráfico que no viaje cifrado podrá por tanto ser «escuchado» por el usuario del sniffer. El análisis de tráfico puede ser utilizado también para determinar relaciones entre varios usuarios (conocer con qué usuarios o sistemas se relaciona alguien en concreto). No es fácil detectar si nuestro tráfico de red está siendo «escuchado» mediante un sniffer, por lo que siempre es recomendable utilizar tráfico cifrado en todas las comunicaciones.

- **Spoofing.** Es una técnica de suplantación de identidad en la Red, llevada a cabo por un ciberdelincuente generalmente gracias a un proceso de investigación o con el uso de malware. Los ataques de seguridad en las redes usando técnicas de spoofing ponen en riesgo la privacidad de los usuarios, así como la integridad de sus datos.

- **Spyware.** Es un malware que recopila información de un ordenador y después la envía a una entidad remota sin el conocimiento o el consentimiento del propietario del ordenador. El término spyware también se utiliza más ampliamente para referirse a otros productos como adware, falsos antivirus o troyanos.

- **SSL.** Es un protocolo criptográfico seguro que proporciona comunicaciones seguras a través de una red (por ejemplo Internet). Generalmente comunicaciones cliente-servidor. El uso de SSL (Secure Sockets Layer) proporciona autenticación y privacidad de la información entre extremos sobre una red mediante el uso de criptografía. SSL garantiza la confidencialidad de la información utilizando una clave de cifrado simétrica y para garantizar la autenticación y seguridad de la clave simétrica, se utilizan algoritmos de cifrado asimétrico y certificados X.509. En comunicaciones SSL de forma general solo se autentica el lado del servidor mientras que el cliente se mantiene sin autenticar; la autenticación mutua requiere un despliegue de infraestructura de claves publicas (PKI) para los clientes. SSL ha evolucionado hacia TLS, siglas en ingles de «seguridad de la capa de transporte» (Transport Layer Security) protocolo ampliamente utilizado en la actualidad.

- **Suplantación de identidad.** Es la actividad maliciosa en la que un atacante se hace pasar por otra persona para cometer algún tipo de fraude, acoso (cyberbulling). Un ejemplo es, en las redes sociales, crear un perfil de otra persona e interactuar con otros usuarios haciéndose pasar por ella.

T

- **TCP/IP.** Por TCP/IP se conoce a una familia de protocolos sobre los cuales funciona Internet, permitiendo la comunicación entre todos los servido- res conectados a dicha red. TCP/IP consta entre otros muchos, del protocolo IP (Internet Protocol), que se ocupa de transferir los paquetes de datos hasta su destino correcto y el protocolo TCP (Transfer Control Protocol), que se ocupa de garantizar que la transferencia se lleve a cabo de forma correcta y con- fiable. Entre otros muchos, esta familia consta de los protocolos ICMP, UDP, DNS, HTTP y FTP.

- **Troyano.** Se trata de un tipo de malware o software malicioso que se caracteriza por carecer de capacidad de autoreplicación. Generalmente, este tipo de malware requiere del uso de la ingeniería social para su propagación. Una de las características de los troyanos es que al ejecutarse no se evidencian señales de un mal funcionamiento; sin embargo, mientras el usuario realiza tareas habituales en su ordenador, el programa puede abrir diversos canales de comunicación con un equipo malicioso remoto que permitirán al atacante controlar nuestro sistema de una forma absoluta.

U

- **URL.** Las siglas URL (Uniform Resource Locator) hacen referencia a la dirección que identifica un contenido colgado en Internet. Las URL permiten tener acceso a los recursos colgados en una red gracias a la dirección única y al servicio de DNS que permite localizar la dirección IP del contenido al que se quiere acceder.

V

- **Virtualización.** La virtualización es un medio para crear una versión virtual de un dispositivo o recurso, como un servidor, o una red, en una máquina física, generalmente con el apoyo de un software que implementa una capa de abstracción para que la maquina física y la virtual puedan comunicarse y compartir recursos.

- **Virus.** Programa diseñado para que al ejecutarse, se copie a sí mismo adjuntándose en aplicaciones existentes en el equipo. De esta manera, cuando se ejecuta una aplicación infectada, puede infectar otros archivos. A diferencia de otro tipo de malware, como los gusanos, se necesita acción humana para que un virus se propague entre máquinas y sistemas. Los efectos que pueden provocar varían dependiendo de cada tipo de virus: mostrar un mensaje, sobrescribir archivos, borrar archivos, enviar información confidencial mediante correos electrónicos a terceros, etc. Los más comunes son los que infectan a ficheros ejecutables.

- **VLAN.** Una red de área virtual o VLAN (acrónimo de Virtual Local Area Network) es una red lógica independiente dentro de una red física de forma que es posible crear diferentes una VLAN que este conectadas físicamente a diferentes segmentos de una red de área local o LAN. Los administradores de este tipo de redes las configuran mediante software en lugar de hardware, lo que las hace extremadamente flexibles. Esta flexibilidad se hace presente en el hecho de que varias de estas redes pueden coexistir en un solo conmutador o red física. Otra de las ventajas de este tipo de redes surge cuando se traslada físicamente algún ordenador a otra ubicación ya que no es necesario volver a configurar el hardware.

- **VoIP.** Señal de voz digitalizada que viaja a través de una red utilizando el protocolo IP (Internet Protocol) que es el utilizado en Internet. Esta tecnología permite mantener conversaciones de voz sin necesidad de una conexión telefónica. La tecnología VoIP utiliza un software especial que transforma la voz humana en una señal digital, que es enviada a través de Internet, donde el proceso se invierte para que la persona destinataria pueda escuchar correctamente la voz, tal y como ocurre en la telefonía tradicional. La principal ventaja de esta tecnología es la importante reducción de los costes que conlleva su uso, así como la portabilidad y la posibilidad de enviar o recibir llamadas de y desde cualquier parte del mundo con un coste mínimo.

- **Vulnerabilidad.** Fallos o deficiencias de un programa que pueden permitir que un usuario no legítimo acceda a la información o lleve a cabo operaciones no permitidas de manera remota. Los agujeros de seguridad pueden ser aprovechadas por atacantes mediante exploits, para acceder a los sistemas con fines maliciosos. Las empresas deben ser conscientes de estos riesgos y mantener una actitud preventiva, así como llevar un control de sus sistemas mediante actualizaciones periódicas.

W

- **Wifi.** Una red wifi es una red de dispositivos inalámbricos interconectados entre sí y generalmente también conectados a Internet a través de un punto de acceso inalámbrico. Se trata por tanto de una red LAN que no utiliza un cable físico para el envío de la información. Tecnología de interconexión de dispositivos electrónicos de forma inalámbrica, que funciona en base al estándar 802.11, que regula las transmisiones inalámbricas. Esta ausencia de cable físico quiere decir que se pierda la confidencialidad de la información transmitida. Por esta razón se hace necesario el cifrado de los contenidos transmitidos a través de una red wifi.

X

- **XSS.** Se trata de una vulnerabilidad existente en algunas páginas web generadas dinámicamente (en función de los datos de entrada). XSS viene del acrónimo en inglés de Secuencias de comandos en sitios cruzados (Cross-site Scripting). Dado que los sitios web dinámicos dependen de la interacción del usuario, es posible insertar en un formulario un pequeño programa malicioso, ocultándolo entre solicitudes legítimas y hacer que éste se ejecute. Los puntos de entrada comunes incluyen buscadores, foros, blogs y todo tipo de formularios alojados en una página web. Una vez realizado el ataque XSS, el atacante puede cambiar la configuración del servidor, secuestrar cuentas, escuchar comunicaciones (incluso cifradas), instalar publicidad en el sitio víctima y en general cualquier acción que desee de forma inadvertida para el administrador.

Z

- **Zero-day.** Vulnerabilidades en sistemas o programas informáticos que son únicamente conocidas por determinados atacantes y son desconocidas por los fabricantes y usuarios. Al ser desconocidas por los fabricantes, no existe un parche de seguridad para solucionarlas. Son muy peligrosas ya que el atacante puede explotarlas sin que el usuario sea consciente de que es vulnerable.

- **Zombie.** Es el nombre que se da a los ordenadores controlados de manera remota por un ciberdelincuente al haber sido infectados por un malware. El atacante remoto generalmente utiliza el ordenador zombie para realizar actividades ilícitas a través de la Red, como el envío de comunicaciones electrónicas no deseadas, o la propagación de otro malware. Son sistemas zombie los ordenadores que forman parte de una botnet, a los que el bot master utiliza para realizar acciones coordinadas como ataques de denegación de servicio.