educación IT
CODE YOUR FUTURE

Introducción a la Ciberseguridad

Glosario de términos

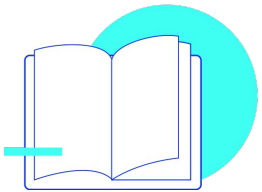
- **Activo de Información:** Se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones.
- **Algoritmos de cifrado:** Es una 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:** Es una circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos, al provocar su indisponibilidad, funcionamiento incorrecto o pérdida de valor.
- **Antivirus:** Se trata de un programa informático específicamente diseñado para detectar, bloquear y eliminar código malicioso (virus, troyanos, gusanos, etc.), y asimismo, proteger los equipos de otros programas peligrosos, conocidos genéricamente como *malware*.

- **Análisis de Riesgos:** 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, para poder determinar los controles adecuados para tratar el riesgo.
- **Ataque de Fuerza Bruta:** Procedimiento para averiguar una contraseña que consiste en probar todas las combinaciones posibles hasta encontrar la combinación correcta.
- **Ataque de Repetición:** 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.
- **Autenticación:** Procedimiento para comprobar que alguien es quien dice ser cuando accede a un ordenador o a un servicio online. Este proceso constituye una funcionalidad característica para una comunicación segura.
- **Autenticidad:** Véase *No Repudio*.

- **Autoridad de Certificación:** AC o CA, (por sus siglas en inglés, *Certification Authority*) es una entidad de confianza cuyo objetivo es garantizar la identidad de los titulares de certificados digitales, además de su correcta asociación a las claves de firma electrónica.
- **Entidad de Registro:** Entidad encargada de identificar de manera inequívoca a los usuarios para que, posteriormente, éstos puedan obtener certificados digitales.
- **Autoridad de Validación:** Entidad cuya función es informar acerca de la vigencia y validez, de los certificados electrónicos creados y registrados por una *Autoridad de Registro* y por una *Autoridad de Certificación*. Además, las autoridades de validación se encargan de almacenar la información sobre los certificados electrónicos anulados, en las *listas de revocación de certificados* (CRL).
- **Backup:** Copia de seguridad que se hace 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.

- **BIA:** Abreviatura de *Business Impact Analysis*. Es un informe que 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 para cada uno.
- **Biometría:** 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 al reconocer e identificar a sus congéneres por su aspecto físico, su voz, su forma de andar, etc.
- **Bluetooth:** Tecnología inalámbrica de radio de corto alcance, cuyo objetivo es eliminar los cables en las conexiones entre dispositivos electrónicos. Simplifica así las comunicaciones entre teléfonos móviles, ordenadores y otros dispositivos informáticos. Opera bajo la banda de radio de 2.4 GHz de frecuencia.
- **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.

- **Botnet:** Conjunto de ordenadores (denominados *bots*) que son controlados remotamente por un atacante, y pueden ser utilizados en conjunto para realizar actividades maliciosas como envío de spam, ataques de DDoS, etc.
- **Bug:** 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 verdadero.
- **Cartas nigerianas:** Comunicación inesperada mediante correo electrónico, carta o mensajería instantánea en las que el remitente promete negocios muy rentables, con el objetivo final de estafar al receptor de las mismas.
- **Centro de Respaldo:** Centro de procesamiento de datos (CPD) específicamente diseñado para poder tomar el control de otro CPD principal en caso de contingencia.



- **Certificado Digital:** Es un fichero informático generado por una entidad denominada *Autoridad Certificadora* (CA), el cual asocia unos datos de identidad a una persona física, organismo o empresa confirmando de esta manera su identidad digital en Internet.
- **Cifrado:** Véase *Algoritmo de Cifrado*.
- **Clave Pública:** Los sistemas de criptografía asimétrica se basan en la generación de un par de claves, denominadas: *clave pública* y *clave privada*. Las cuales tienen la peculiaridad de que los mensajes cifrados con una de ellas, sólo pueden ser descifrados utilizando la otra. Se conoce como *clave pública* a una de estas claves, que puede ponerse en conocimiento de todo el mundo y que usará un remitente, para cifrar el mensaje o documento que quiere enviar. Garantiza así, que solo lo pueda descifrar 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*. Las cuales tienen la peculiaridad de que los mensajes cifrados con una de ellas, sólo pueden ser descifrados usando la otra. La *clave privad*a es una de estas claves, que el usuario debe proteger estrictamente, ya que es usada para descifrar la información que se le envía cifrada con su *clave pública*.

- **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.
- **Confidencialidad:** Propiedad de la información, por la que se garantiza que la misma está accesible solo a personal autorizado a acceder a dicha información.
- **Control Parental:** Conjunto de herramientas o medidas, 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.
- **Cookie:** 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:** O *firewall*, es un 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.

- **Criptografía:** Técnica que consiste en cifrar un mensaje, conocido como *texto en claro*, al convertirlo en un mensaje cifrado o criptograma, que resulta ilegible para todo el que no conozca el sistema mediante el cual ha sido cifrado.
- **CRL:** O *listas de revocación de certificados*, es un mecanismo para verificar la validez de un certificado digital, a través de listas emitidas por las autoridades oficiales de certificación.
- **Códigos de Conducta:** En el ámbito de las TIC, los códigos de conducta son aquellas recomendaciones o reglas, cuyo fin es 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.
- **Denegación de Servicio:** Conjunto de técnicas cuyo objetivo es 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 prestados por él.

- **Desbordamiento de Búfer:** O *Buffer Overflow*. Error de software que se produce debido a que el programador no incluye las medidas necesarias para comprobar el tamaño del búfer, en relación con el volumen de datos que tiene que alojar. Eso provoca que se sobreescriban otros puntos de la memoria, lo cual puede hacer que el programa falle. En algunos casos, esto puede ser aprovechado por un atacante para hacerse del control del sistema.
- **Dirección IP:** Número único e irrepetible con el cual se identifica a todo sistema conectado a una red. Las direcciones IP pueden ser *públicas*, en caso de ser accesibles directamente desde cualquier sistema conectado a Internet, o *privadas*, si son internas a una red LAN y solo son accesibles desde los equipos conectados a esa red privada.
- **Dirección MAC:** Acrónimo de *Media Access Control*, 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 directamente, en forma binaria, en el hardware del interfaz de red, en el momento de su fabricación.

- **Disponibilidad:** Capacidad de un servicio, un sistema o una información, a ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran.
- **DNS:** *Domain Name System*, 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; el propósito es poder localizar y direccionar estos sistemas, de una forma más simple.
- **Exploit:** Secuencia de comandos usados para, aprovechándose de un fallo o vulnerabilidad en un sistema, provocar un comportamiento no deseado o imprevisto. Mediante la ejecución de *exploit* se suele perseguir el acceso a un sistema, la elevación de privilegios, o un ataque de denegación del servicio.
- **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 visible o accesible para otros.

- **FTP:** Acrónimo de *File Transfer Protocol*, hace referencia a un servicio de transferencia de ficheros a través de una red, así como a los servidores que permiten prestar este servicio. Por medio de 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.
- **Gusano:** O *Worm*, es un programa malicioso (o *malware*) cuya característica principal es su alto grado de *dispersabilidad*, es decir, la rapidez con que se propaga. Su fin es replicarse a nuevos sistemas, para infectarlos y continuar replicándose a otros equipos informáticos, al aprovecharse de todo tipo de medios, como el correo electrónico, IRC, FTP, correo electrónico, P2P y otros protocolos que son específicos o ampliamente utilizados.
- **HTTP:** Es el acrónimo de *Hypertext Transfer Protocol*. Se trata del protocolo más utilizado para la navegación web. Sigue un esquema *petición-respuesta*. El navegador hace 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 (viene del inglés *Uniform Resource Locator*). La información enviada vía HTTP se manda en *texto claro.*

Esto significa que cualquiera que intercepte el tráfico de red, puede leer lo que se envía y se recibe. Por esta razón, se desarrolló el protocolo HTTPS, en el que la información es cifrada antes de ser enviada por la red.

- **HTTPS:** Acrónimo de *Hypertext Transfer Protocol Secure*, es un protocolo de red basado en el protocolo HTTP, destinado a la transferencia segura de datos de hipertexto. Es decir, es la versión segura de HTTP.

- **IDS:** *Sistema de detección de intrusos* (del inglés *Intrusion Detection System*) se trata de una aplicación usada para detectar accesos no autorizados a un ordenador o a una red. Estos accesos pueden ser ataques hechos 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:** Se refiere a cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa. Como por ejemplo, los siguientes: acceso o intento de acceso a los sistemas, uso, divulgación, modificación o destrucción no autorizada de información.
- **Informática Forense:** Proceso de investigación de los sistemas de información, con el fin de poder detectar toda evidencia que pueda ser presentada como prueba fehaciente, en un procedimiento judicial. Para esta investigación, se necesita la aplicación de técnicas científicas y analíticas especializadas que permitan identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.
- **Infraestructura de clave pública:** También conocido por las siglas PKI (del inglés *Public Key Infrastructure*). Se trata de un conjunto de hardware, software, políticas y procedimientos de actuación, encaminados a la ejecución con garantías de operaciones de cifrado y criptografía; tales como la firma, el sellado temporal o el no repudio de transacciones electrónicas.

- **Ingeniería Social:** Tácticas utilizadas para obtener información o 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:** Propiedad de la información por la que se garantiza la exactitud de los datos transportados o almacenados. Al asegurar 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.
- **Inyección SQL:** O *SQL Injection*, es un tipo de ataque que se aprovecha de una vulnerabilidad, en la validación de los contenidos introducidos en un formulario web. Y 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 se puede considerar como una extensión de los sistemas de detección de intrusos (IDS), pero en realidad es una tecnología más cercana a los cortafuegos.

- **LAN:** *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 de todo tipo, ordenadores, impresoras, servidores, discos duros externos, etc. Pueden ser cableadas o no cableadas, también conocidas como redes inalámbricas.
- **Malware:** Es un tipo de software, cuyo fin es dañar o infiltrarse, sin el consentimiento de su propietario, en un sistema de información. La palabra, nace de la unión de los términos en inglés que define *software malicioso*: *malicious software*. En 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:** Conjunto de datos relacionados con un documento y que recogen información fundamentalmente descriptiva del mismo, así como información de administración y gestión. Los metadatos es una información que enriquece el documento al que está asociado.

- **No repudio:** En el envío de información mediante las redes es la 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.
- **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.
- **Parche de Seguridad:** También llamado actualización de seguridad, es un conjunto de cambios que se aplican a un software para corregir errores de seguridad en programas o sistemas operativos.
- **Pentest:** *Penetration test*, o *prueba de penetración*, es un ataque a un sistema software o hardware, con el fin 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.

- **PCI DSS:** *Payment Card Industry Data Security Standard* es un *Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago*. Ha sido desarrollado por un comité formado por varias compañías de tarjetas (débito y crédito), que se denomina PCI SSC (*Payment Card Industry Security Standards Council*).
- **Pharming:** Ataque informático que aprovecha una vulnerabilidad del software de los servidores DNS. Consiste en modificar o sustituir el archivo del servidor de DNS, al cambiar la dirección IP legítima de una entidad; de manera que, en el momento en el que un usuario intenta acceder al sitio web de dicha entidad, es redirigido automáticamente a un equipo controlado por el atacante.
- **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 o *phisher,* 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 de manera telefónica) crea en su veracidad y le 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 hace al usar 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 una empresa conocida, conseguir que se les facilite: información financiera, números de tarjeta de crédito, cuentas bancarias o contraseñas.

- **Plan de Contingencia:** Un *Plan de Contingencia de las Tecnologías de la Información y las Comunicaciones* (TIC) consiste en una estrategia planificada en fases y formada 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 de Negocio:** O *Business Continuity Plan* (BCP), 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 riesgos a los que están expuestos. Este término también se refiere al documento de nivel ejecutivo por 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.
- **Proveedor de Acceso:** O *Internet Service Provider* (ISP) son todos los prestadores de servicios de la Sociedad de la Información, que proporcionan a sus usuarios/clientes

acceso a redes de telecomunicaciones, las mismas pueden ser tanto fijas como móviles.

- **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* o *cortafuegos*) que impiden accesos no autorizados desde el exterior hacia la red privada.

- **Puerta trasera:** O *backdoor*, es cualquier punto débil de un programa o sistema, por 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 usadas 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.

- **Ransomware:** Tipo de malware en el que se toma control del equipo infectado y «secuestra» la información del usuario cifrándola, de tal forma que permanece ilegible, si no se posee la contraseña de descifrado. Así, extorsiona al usuario al pedir un rescate económico a cambio de esta contraseña para que, supuestamente, pueda recuperar sus datos.
- **Red Privada Virtual:** *Virtual Private Network* (VPN) 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 autenticación 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.
- **Router:** o *Enrutador*, encaminador, 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.

- **RSA:** Es un sistema criptográfico de clave pública, desarrollado por los criptógrafos *Rivest*, *Shamir* y *Adleman*, de donde toma su nombre. Se trata del primer y más utilizado algoritmo de este tipo y permite tanto cifrar documentos, como firmarlos de manera digital.
- **SaaS:** Siglas de *Software as a Service*, o sea, la utilización de Software como un servicio. Es un modelo de distribución de software, donde tanto el software como los datos que maneja, se alojan en servidores de un tercero y el cliente accede a los mismos vía Internet.
- **Servidor:** Se trata de, tanto el software que realiza ciertas tareas en nombre de los usuarios, como del 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 conectan 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 siguientes: los que brindan el alojamiento de sitios web, así como también los que proporcionan el servicio de envío, reenvío y recepción de correos electrónicos.

- **SGSI:** Un *Sistema de Gestión de la Seguridad de la Información* 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.

- **SLA:** Un acuerdo de nivel de servicio o ANS (*Service Level Agreement*), se trata de 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; y lo hace 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*) es un protocolo de red usado para el intercambio de mensajes de correo electrónico. Este protocolo, aunque es el más comúnmente utilizado, tiene algunas limitaciones en relación 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:** 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 y estén dirigidos o no a ese dispositivo.

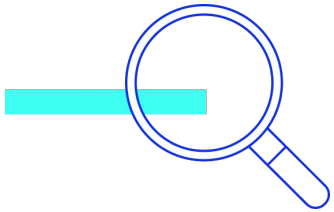
- **Spoofing:** Técnica de suplantación de identidad en la red. Los ataques de seguridad en las redes mediante técnicas de *spoofing* ponen en riesgo la privacidad de los usuarios, así como la integridad de sus datos. Según la tecnología utilizada, se pueden diferenciar varios tipos de spoofing, como ***IP spoofing***, ***ARP spoofing***, ***DNS spoofing***, ***Web spoofing*** o ***Mail spoofing***.
- **Spyware:** *Malware* que recopila información de un ordenador y luego la envía a una entidad remota, sin el conocimiento del usuario. El término *spyware* también se utiliza más ampliamente para referirse a otros productos como *adware*, falsos antivirus o troyanos.
- **SSL:** Protocolo criptográfico que proporciona comunicaciones seguras a través de una red (por ejemplo Internet). Generalmente comunicaciones cliente-servidor. El uso de SSL (*Secure Sockets Layer*) brinda autenticación y privacidad de la información entre extremos sobre una red mediante el uso de criptografía. SSL ha evolucionado hacia ***TLS***, siglas en inglés de *seguridad de la capa de transporte* (*Transport Layer Security*) protocolo utilizado de manera amplia, en la actualidad.

- **Suplantación de Identidad:** Actividad maliciosa en la que un atacante se hace pasar por otra persona con el fin de cometer algún tipo de fraude, acoso (*cyberbullying*). Un ejemplo es, en las redes sociales, la creación de un perfil de otra persona y la interacción con otros usuarios, haciéndose pasar por ella.

- **TCP/IP:** Familia de protocolos sobre los cuales funciona Internet, permitiendo la comunicación entre todos los servidores 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 confiable. Entre otros muchos, esta familia consta de los protocolos ICMP, UDP, DNS, HTTP y FTP.

- **Troyano:** Tipo de *malware* que se caracteriza por carecer de capacidad de autorreplicación. Generalmente requiere del uso de la ingeniería social para su propagación. Una de las características principales es que al ejecutarse no se evidencian señales de un mal funcionamiento; sin embargo, mientras el usuario hace tareas habituales en su ordenador, el programa puede abrir diversos canales de comunicación con un equipo malicioso remoto, que permitirán al atacante poder controlar nuestro sistema.

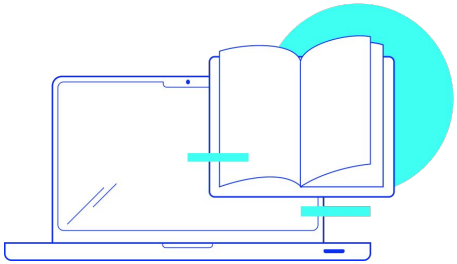
- **URL:** *Uniform Resource Locator* hace referencia a la dirección que identifica un contenido colgado en Internet. Las URL permiten tener acceso a los recursos colgados en una red gracias a la dirección única y al servicio de DNS que permite localizar la dirección IP del contenido al que se quiere acceder.
- **Virtualización:** Es un medio para crear una versión virtual de un dispositivo o recurso, (como por ejemplo, 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 máquina física y la virtual puedan comunicarse y compartir recursos.
- **Virus:** Tipo de *malware* diseñado para que al ejecutarse, se copie a sí mismo y se adjunte 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.



- **VLAN:** Una red de área virtual o VLAN (*Virtual Local Area Network*) es una red lógica independiente dentro de una red física de forma que es posible crear diferentes VLAN dentro de una misma LAN física.
- **VoIP:** Se trata de una señal de voz digitalizada que viaja a través de una red y utiliza el protocolo IP (*Internet Protocol*) que es el utilizado en Internet. Esta tecnología permite mantener conversaciones de voz sin necesidad de una conexión telefónica.
- **VPN:** Véase *Red Privada Virtual*.
- **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. 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.

- **Wifi:** Es una red de dispositivos inalámbricos interconectados entre sí y que generalmente también están 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.
- **XSS:** *Cross Site Scripting* (Secuencias de comandos en sitios cruzados) es una vulnerabilidad existente en algunas páginas web que están generadas dinámicamente (en función de los datos de entrada). Se asocia al ataque con ese mismo nombre, el cual se aprovecha de la ausencia o insuficiencia de validación de datos de entrada, para lograr ejecutar código malicioso en el navegador de los usuarios, generalmente mediante el lenguaje *JavaScript*.
- **Zero-day:** También escritas como *0-day*, son aquellas vulnerabilidades en sistemas o programas informáticos, que son conocidas solamente por determinados atacantes y resultan desconocidas por los fabricantes y usuarios. Al ser desconocidas por los fabricantes, no existe un parche de seguridad para solucionarlas. Por esta razón 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 usa el ordenador zombie para hacer actividades ilícitas a través de la red, como el envío de comunicaciones electrónicas no deseadas, o la propagación de otro malware. Son sistemas zombie (o *bots*) 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.



Ahora sí,
¡Comencemos!