



GLOSARIO DE TÉRMINOS DE SEGURIDAD

A

AAA	<p>Abreviatura de Autenticación, Autorización y Accounting, sistema en redes IP para a qué recursos informáticos tiene acceso el usuario y rastrear la actividad del usuario en la red.</p> <ul style="list-style-type: none">• Autenticación es el proceso de identificación de un individuo, normalmente mediante un nombre de usuario y contraseña. Se basa en la idea de que cada individuo tendrá una información única que le identifique o que le distinga de otros.• Autorización es el proceso de aceptar o denegar el acceso de un usuario a los recursos de la red una vez que el usuario ha sido autenticado con éxito. La cantidad de datos y servicios a los que el usuario podrá acceder dependen del nivel de autorización que tenga establecido.• Accounting es el proceso de rastrear la actividad del usuario mientras accede a los recursos de la red, incluso la cantidad de tiempo que permanece conectado, los servicios a los que accede así como los datos transferidos durante la sesión. Los datos registrados durante este proceso se utilizan con fines estadísticos, de planeamiento de capacidad, tarificación, auditoría,.. <p>A menudo los servicios AAA requieren un servidor dedicado. RADIUS es un ejemplo de un servicio AAA.</p>
Acceso Remoto	<p>Utilidad para que un usuario acceda desde su propio PC a otro que esté ubicado remotamente y pueda operar sobre él.</p>
Active-X	<p>Los denominados controles Active-X son componentes adicionales que se pueden incorporar a las páginas web, para dotarlas de mayores funcionalidades (animaciones, vídeo, navegación tridimensional, etc...). Están escritos en un lenguaje de programación como Visual Basic, C o C++, que no es el propio de las páginas web (HTML) y podrían estar infectados con virus.</p>
Actualización de Antivirus	<p>Incorporación en el programa Antivirus de la última versión archivo de identificación de virus. Dependiendo de la configuración del Antivirus, la actualización se hace de forma manual o automáticamente a través de Internet</p>
Ad Hoc	<p>Una WLAN bajo topología "Ad Hoc" consiste en un grupo de equipos que se comunican cada uno directamente con los otros a través de las señales de radio sin usar un punto de acceso. Las configuraciones "Ad Hoc" son comunicaciones de tipo punto-a-punto. Los equipos inalámbricos necesitan configurar el mismo canal y SSID en modo "Ad Hoc".</p>
Adjunto	<p>Archivo o fichero vinculado a un correo electrónico.</p>

	Puede ser un texto, un gráfico, un sonido o un programa
Administrador	Es la persona o programa encargado de gestionar, realizar el control, conceder permisos, etc. de todo un sistema informático o red de ordenadores.
AES - Advanced Encryption Standard	También conocido como "Rijndael", algoritmo de encriptación simétrica de 128 bit desarrollado por los belgas Joan Daemen y Vincent Rijmen. En Octubre de 2000 era seleccionado por el Instituto Nacional de Estándares y Tecnología (NIST) norteamericano como estándar de cifrado reemplazando al hasta entonces estándar DES.
Agujero	(En inglés "hole") Una vulnerabilidad en el diseño del software y/o hardware que permite engañar a las medidas de seguridad, posibilitando un acceso no autorizado a sistemas informáticos ajenos.
Algoritmo criptográfico	Conjunto finito de operaciones matemáticas, reglas o pasos, que permiten obtener un texto cifrado a partir de un texto en claro y de ciertos parámetros iniciales, como la clave criptográfica y el vector de inicialización. Se pueden clasificar en algoritmos simétricos o asimétricos (también conocidos como de clave pública).
Alias	Nombre diferente por el cual se conoce un virus. Al no existir un estándar para denominarlos, los distintos fabricantes de antivirus definen a un mismo virus informático con diferentes nombres alternativos, conocidos como Alias
Amenaza	Persona, cosa, evento o idea que supone algún peligro para un activo (en terminos de confidencialidad, integridad, disponibilidad o uso legítimo). Pueden ser deliberadas o accidentales
Análisis de impacto	Estudio y evaluación de las pérdidas y daños sufridos después de un ataque
Análisis de riesgo	Estudio de los activos, sus vulnerabilidades y las probabilidades de materialización de amenazas, con el propósito de determinar la exposición al riesgo de cada activo ante cada amenaza.
Análisis Heurístico	Se trata de una análisis adicional que solamente algunos programas anti-virus pueden realizar para detectar virus que hasta ese momento son desconocidos. Dicho análisis consiste en buscar patrones de conducta, determinadas instrucciones concretas y comunes a los diferentes códigos maliciosos, construidos con determinados lenguajes utilizados habitualmente en el diseño de virus.
Analizador de Comportamiento (Behavior Blocker)	Un programa anti-virus emplea una técnica para comprobar si un archivo incorpora los comportamientos habituales de un virus. Un behavior blocker trabaja bajo un conjunto de reglas de funcionamiento que legitima programas bajo las reglas

	de comportamiento que siguen los virus. Además analiza y determina las tareas y comportamientos que han sido diseñadas para un archivo y averigua si el éste contiene algún virus.
Ancho de Banda	Parámetro que define la cantidad de datos que puede ser enviada en un periodo de tiempo determinado a través de un canal de comunicación.
Anti-Virus	Aplicación cuya finalidad es la detección y eliminación de virus, troyanos, gusanos informáticos y cualquier otro código malicioso.
Ataque	Es la materialización de una amenaza: acción que puede violar los sistemas y mecanismos de seguridad de un sistema de información. Puede ser pasivos (únicamente se leen los datos transmitidos, sin modificarlos), o activos (insertar información falsa, eliminar, o corromper la existente)
Ataque de Diccionario	Método empleado para romper la seguridad de los sistemas basados en passwords (contraseñas) en la que el atacante intenta dar con la clave adecuada probando todas (o casi todas) las palabras posibles o recogidas en un diccionario. Generalmente no se introducen manualmente las posibles contraseñas sino que se emplean programas especiales que se encargan de ello.
Ataque de Fuerza Bruta	Método empleado para romper la seguridad vía contraseña probando todas las combinaciones posibles de palabras (distinto del ataque de diccionario que prueba palabras aisladas). Un ataque de fuerza bruta teóricamente no puede ser resistido por ningún sistema, siempre y cuando se disponga del tiempo suficiente y del equipo adecuado. Así, las claves lo suficientemente largas (y mejor aún si combinan caracteres alfanuméricos) ponen una limitación física, pero no lógica, al éxito de este tipo de ataque.
Atributos	Características que se asignan a los ficheros y directorios para que puedan ser sólo lectura, modificado, oculto ó de sistema.
Auditoría	Conjunto de técnicas y procedimientos sistemáticos, independientes y documentados para evaluar y controlar, total o parcialmente, un sistema informático, con el fin de proteger sus activos y recursos, verificar si sus actividades se desarrollan eficientemente y de acuerdo con la normativa informática y general existentes en cada empresa y para conseguir la eficacia exigida en el marco de la organización correspondiente.
Autenticación	Proceso en el que se da fe de la veracidad y autenticidad de un producto, de unos datos o de un servicio, así como de la fiabilidad y legitimidad de la empresa que los ofrece.
Autoridad de	En criptografía una Autoridad de certificación, (AC o

Certificación	CA por sus siglas en inglés Certification Authority) es una entidad de confianza, responsable de emitir y revocar los certificados digitales o certificados, utilizados en la firma electrónica.
Autorización	Proceso mediante el cual se permite conocer si una persona, programa o dispositivo tiene permiso para acceder a un dato, funcionalidad o servicio concreto.

B

Backdoor	Véase puerta trasera
Background	Se dice que una aplicación funciona "en background" cuando está trabajando en segundo plano, sin afectar a la actividad del usuario.
Backup	Véase copia de seguridad
Base de Datos	Grupo de datos estructurado almacenado para facilitar su consulta y posterior tratamiento.
Biométrica	Ciencia que estudia las características biológicas del ser humano (el iris, la huella dactilar, la voz, etc...) para su aplicación a la seguridad informática como medio de identificación del usuario.
Bit (dígito binario)	Es la unidad más pequeña de la información digital con la que trabajan los sistemas informáticos. Puede tener dos estados "0" o "1". La unión de 8 bits da lugar a un byte.
Blowfish	Blowfish es un algoritmo criptográfico simétrico. Sus claves son de longitud variable.
Bomba de Tiempo	Programa malicioso que se activa en una determinada fecha.
Bomba Lógica	Programa que se ejecuta cuando existen condiciones específicas para su activación. Los suelen utilizar muchos virus como mecanismo de activación.
Bombardeo de e-mail	Envío masivo de mensajes de correo electrónico muy grandes a la cuenta de correo de un usuario con el propósito de saturar la capacidad de almacenamiento y evitar que los mensajes verdaderos sean recibidos o provocar la caída del sistema al no poder manejar tal cantidad de datos.
Bug	Véase error de software

C

Caballo de Troya	Véase troyano
Cabecera	Parte inicial de un paquete que precede a los datos propiamente dichos y que contiene las direcciones del remitente y del destinatario, control de errores y otros campos. Una cabecera es también la porción de un mensaje de correo electrónico que precede al mensaje propiamente dicho y contiene, entre otras cosas, el remitente del mensaje, la fecha y la hora.
Cadena	Una serie de caracteres consecutivos de texto, dígitos numéricos, signos de puntuación o espacios en blanco. alguna de las técnicas empleadas por los anti-virus para la detección de virus es buscar determinadas

	cadenas de texto (o código) que éstos incluyen de manera frecuente.
Capturador de pulsaciones de teclado (Keylogger)	Programa que intercepta todas las pulsaciones realizadas en el teclado (e incluso a veces también el mouse), y las guarda en un archivo para obtener datos críticos como contraseñas, etc. Posteriormente puede ser enviado a un tercero sin conocimiento ni consentimiento del usuario.
Certificado digital	Un Certificado Digital es un documento digital mediante el cual un tercero confiable (una autoridad de certificación) garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública. El certificado contiene usualmente el nombre de la entidad certificada, un número de serie, fecha de expiración, una copia de la clave pública del titular del certificado (utilizada para la verificación de su firma digital), y la firma digital de la autoridad emisora del certificado de forma que el receptor pueda verificar que esta última ha establecido realmente la asociación.
CHAP - Challenge Handshake Authentication Protocol	Protocolo de autenticación para servidores PPP donde la contraseña no sólo se exige al empezar la conexión sino también durante la conexión, mucho más seguro que el PAP. Una vez efectuado el enlace, el servidor envía un mensaje de desafío al solicitante de la conexión, el cual responde con un valor hash que será comparado por el servidor con sus cálculos del valor hash esperado. Si el valor coincide, la autenticación prospera, de lo contrario, finaliza. En cualquier momento el servidor puede solicitar un mensaje de desafío. Debido a que los identificadores cambian frecuentemente y por que la autenticación puede ser solicitada en cualquier momento.
Cifrado	Resultado de aplicar un algoritmo criptográfico sobre un mensaje. El resultado es ininteligible, sólo quienes conozcan la clave podrán acceder al contenido real de los datos.
Cifrado asimétrico	Algoritmo de cifrado que necesita dos claves distintas. Cada usuario genera un par de claves usadas para el cifrado y el descifrado de mensajes, una de ellas la pone a disposición pública, clave pública y otra es la clave privada.
Cifrado simétrico	Algoritmo de cifrado que requiere que ambas partes compartan una clave secreta; se usa la misma clave para cifrar y descifrar
Clave criptográfica	Secuencia de bits utilizados por un algoritmo criptográfico para el cifrado o descifrado de los datos.
Cliente	Un ordenador o un programa que accede a los servicios ofrecidos por otro ordenador o programa llamado servidor, al que está conectado en red.
Código Malicioso	Es un término genérico utilizado para describir el

(Malware)	software malicioso tales como: virus, gusanos, troyanos, etc.
Confidencialidad	Servicio de seguridad que impide que ésta esté disponible o sea revelada a individuos, entidades o procesos no autorizados
Control de Acceso	Servicio de seguridad que previene del uso no autorizado de un recurso. El control se realiza limitando el acceso a recursos físicos o de información mediante una tabla de acceso, que describe las acciones y recursos permisibles a cada usuario. El permiso o la denegación de acceso puede realizarse en función de la dirección IP, el nombre de dominio, nombre de usuario y password, certificados del clientes, protocolos de seguridad de redes, etc...
Contraseña / Password	Clave de acceso necesaria para acceder a un determinado sistema.
Cookie	Archivo de texto que los servidores web utilizan para identificar a los usuarios que se conectan. Se almacena localmente en cada equipo, y cada vez que el usuario vuelve a visitar el sitio, se vuelve a enviar al servidor para identificarlo. Otras funciones que tienen es almacenar datos adicionales de quienes se conectan a un sitio de internet (contraseñas para inicio de conexión, datos sobre las compras realizadas, preferencias de navegación ...), para personalizar las páginas de éste o para almacenar información necesaria para la navegación.
Copia de Seguridad (Backup)	Copia o réplicas de datos que nos permiten recuperar la información original en caso de ser necesario.
Correo basura (spam)	Correo electrónico no deseado que se envía aleatoriamente a muchísimos usuarios. No es una amenaza directa, pero la cantidad de correo basura recibido y el tiempo que supone identificarlo y eliminarlo, representa un elemento molesto para los usuarios de Internet.
Cortafuegos (Firewall)	Sistema de seguridad que se compone bien de programas (software) ó de equipos (hardware) y de programas (software) en puntos clave de una red para permitir sólo tráfico autorizado. Además, estos sistemas suelen incorporar elementos de privacidad, anti-virus, autenticación, etc...
Cracker	Persona que elimina las protecciones lógicas y físicas de los sistemas para acceder a los mismos sin autorización y generalmente con malas intenciones.
Criptoanálisis	Estudio de un sistema criptográfico con la intención de detectar cualquier punto débil dentro de su algoritmo.
Criptografía	Disciplina que estudia los principios, métodos y medios de transformar los datos con objeto de ocultar la información contenida en los mismos, detectar su modificación no autorizada y prevenir su uso no

	permitido.
--	------------

D

Delito Informático	Delito cometido utilizando un ordenador; también se entiende por delito informático cualquier ataque contra un sistema de ordenadores
Denegación de Servicio (Denial of Service, DoS)	Se trata de un ataque diseñado específicamente para impedir el funcionamiento normal de un sistema y en consecuencia impedir el acceso legal a los sistemas para usuarios autorizados. Como consecuencia, un ordenador o un programa, dejan de responder al servicio solicitado, normalmente por saturación en la cantidad de solicitudes
DES	Data Encryption Standard (DES) es un algoritmo criptográfico simétrico haciendo bloques de datos de 64 bits y utilizando una clave de 56 bits. Durante muchos años ha sido asumido como estándar y su uso se ha propagado ampliamente por todo el mundo. Hoy en día, el DES (debido a su longitud de clave) se considera insuficiente para muchas aplicaciones, y por ello se suele usar su variante de Triple DES que utiliza el algoritmo DES tres veces. Desde hace algunos años, el algoritmo ha sido sustituido por el nuevo AES (Advanced Encryption Standard).
Desbordamiento de Búfer (Buffer Overflow)	Error de software que tiene lugar cuando se copia una cantidad más grande de datos sobre un área más pequeña, sobre-escribiendo otras zonas de datos no previstas. En algunas ocasiones eso puede suponer la posibilidad de alterar el flujo del programa pudiendo hacer que este realice operaciones no previstas. Si el programa que tiene el error en cuestión tiene privilegios especiales se convierte además en un fallo de seguridad.
Descifrar	Proceso inverso al cifrado, es decir, obtener el mensaje en claro a partir del texto cifrado.
Dialer	Programa que permite cambiar el número de acceso telefónico automáticamente, de acuerdo a la situación geográfica del usuario. Estos códigos toman el control sólo de la conexión telefónica vía módem, desviando las llamadas normales que efectúas a través de tu proveedor hacia un número del tipo 908, 906, etc..., números de tarifa especial y bastante cara por lo general.
Disponibilidad	Servicio de seguridad que garantiza que los recursos de un sistema abierto sean accesibles y utilizables a petición de una entidad autorizada.
Dropper	Usado como portador de virus, un dropper es un programa ejecutable que instala el virus en memoria, en el disco o en un archivo (aunque un dropper por sí mismo no tiene capacidades de infección ni de replicación).

E

Encriptación	Véase cifrado
Engaño (Hoax)	Falsos mensajes de alarma (bromas o engaños) sobre virus que no existen. Estos se envían por correo electrónico con la intención de extender falsos rumores por Internet. Los mensajes no suelen estar fechados, con lo que se pretende que los mensajes siempre parezcan recientes. En ocasiones, los Hoax pretenden engañar a los usuarios mediante el uso de palabras técnicas. , mensajes que simulan a los reales, alertas de nuevos virus, anuncios de nuevas soluciones, cadena de correos a reenviar,..., etc. Por otra parte, suele ser frecuente la inclusión del nombre de ciertas agencias de prensa (CBS...) en el encabezamiento de estos mensajes. Con todo esto se pretende dar un aspecto verídico a los mensajes.
Error de software (Bug)	Es el resultado de un fallo de programación introducida en el proceso de creación de programas de ordenador o computadora.
Escáner	Programa que busca virus en la memoria del PC o en los archivos.
Estafa (scam)	Fraude destinado a conseguir que una persona o grupo de personas entreguen dinero, bajo falsas promesas de beneficios económicos (viajes, vacaciones, premios de lotería, etc.).
Estándar	Especificación que se utiliza como punto de partida para el desarrollo de servicios, aplicaciones, protocolos, etc... y que regula la realización de ciertos procesos o la fabricación de componentes para garantizar la interoperabilidad.
Excepciones	Una alternativa a la búsqueda de cadenas es la búsqueda de excepciones. Cuando un virus utiliza una determinada cadena para realizar una infección pero en la siguiente emplea otra distinta, es difícil detectarlo mediante la búsqueda de cadenas. En ese caso, lo que el programa anti-virus puede chequear es el cambio en las cadenas (excepciones).
Explotar (Exploit)	Método de utilizar un bug o fallo para penetrar en un sistema.

F

Falso Negativo	Evento que se da como inexistente cuando realmente si existe, por ejemplo, decir que un sistema está limpio de virus cuando realmente está infectado.
Falso Positivo	Evento que se da como existente cuando realmente no existe, por ejemplo, decir que un sistema está infectado de virus cuando realmente está limpio.
FAQ	(Frequently Asked Questions) Preguntas frecuentemente formuladas. Las FAQs son documentos en red que enuncian y responden a las preguntas más frecuentes de un tema en concreto.

Filtros Anti-Spam	Son herramientas para filtrar el spam o correo basura no solicitado en los programas de correo.
Firma Digital o Firma Electrónica	El conjunto de datos, en forma electrónica, anexos a otros datos del mismo tipo o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge y que impide la apropiación o daño de su contenido por parte de terceros. Se obtiene cifrando la huella digital de un mensaje con la clave privada del remitente. Garantiza la identidad del firmante y que el texto no se modificó.
Firewall	(Véase cortafuego)
FTP - Protocolo de Transferencia de Archivos (File Transfer Protocol)	Protocolo de transferencia de archivos. Permite a los usuarios de Internet la captura de documentos, archivos, programas y otros datos contenidos en carpetas existentes en cualquier lugar de Internet. Se puede acceder a los archivos públicos situados en el sistema remoto al que se accede sin tener que proporcionar nombre de usuario y contraseña, o a otros privados tras introducir el login y password correspondiente.
Función unidireccional	Función matemática fácil de calcular, pero cuya inversa es inviable
Función unidireccional con trampa	Función unidireccional, pero la inversa puede obtenerse si se conoce una información privilegiada. Son la base de los algoritmos criptográficos asimétricas, siendo la clave privada la información privilegiada
Función resumen o función de hash	Función matemática que transforma un mensaje con longitud variable de bits a un conjunto de longitud fija conocido como "hash" que representa de manera unívoca al documento

G

Galleta	(Véase Cookie)
Gestión de Claves	Proceso para generar, transportar, almacenar y destruir claves de encriptación de modo seguro.
Gusano (Worm)	Programa similar a un virus que se diferencia de éste en su forma de realizar las infecciones. Mientras que los virus intentan infectar a otros programas copiándose dentro de ellos, los gusanos realizan copias de ellos mismos, infectan a otros ordenadores y se propagan automáticamente en una red independientemente de la acción humana.
Gusano de Internet	Tipo específico de gusano que aprovecha las propiedades de Internet para reproducirse a través de la red. Como cualquier gusano, su fin es replicarse a nuevos sistemas para infectarlos y seguir replicándose a otros equipos informáticos, pero lo que lo califica como un gusano de Internet es que aprovecha medios como el correo electrónico, chat, FTP, y otros protocolos específicos o ampliamente utilizados en

H

Hacker	Persona que tiene un conocimiento profundo acerca del funcionamiento de redes y que puede advertir los errores y fallos de seguridad. Busca acceder por diversas vías a los sistemas informáticos, aunque no necesariamente con malas intenciones.
Hash	Un valor hash, también conocido como "message digest", es un número generado a partir de una cadena de texto. El hash es sustancialmente más pequeño que el texto en sí, y es generado por una fórmula de tal forma que sea poco probable que algún otro texto produzca el mismo valor. Los hashes juegan un papel crucial en la seguridad donde se emplean para asegurar que los mensajes transmitidos no han sido manipulados. El emisor genera un hash del mensaje, lo encripta y lo envía con el propio mensaje. El receptor luego decodifica ambos, produce otro hash del mensaje recibido y compara los dos hashes, si coinciden, existe una probabilidad muy elevada de que el mensaje recibido no haya sufrido cambios desde su origen.
Hijacker	Cualquier programa que cambia la configuración del navegador, para hacer que su página de inicio, búsqueda, etc., apunte a otro sitio distinto del indicado por el usuario.
Honeypot (tarros de miel en castellano)	Un servidor diseñado para ser atacado y que actúa como señuelo para hackers que piensan que se conectan a un verdadero sistema informático y actúan sobre él, permitiendo así a su propietario monitorizar la actividad del "pirata" con distintos fines: estudiar su comportamiento, fijar los puntos débiles de su red, etc...
Hot Spot (Punto Caliente)	Punto de Acceso generalmente localizado en lugares con gran tráfico de público (estaciones, aeropuertos, hoteles, etc...) que proporciona servicios de red inalámbrico de banda ancha a visitantes móviles.
HTML	(Hyper Text Markup Language) Es el lenguaje de marcado usado como el estándar para especificar el formato y delimitar el contenido que permite la visualización de páginas Web, desde un navegador. Se basa en etiquetas (instrucciones que le dicen al texto como deben mostrarse) y atributos (parámetro que dan valor a la etiqueta).
HTTP (Hyper Text Transfer Protocol)	Es un protocolo de comunicación que permite la visualización de páginas Web desde un navegador. En el World Wide Web, las páginas escritas en HTML utilizan el hipertexto para enlazar con otros documentos. Al pulsar en un hipertexto, se salta a otra página web, fichero de sonido, o imagen. La transferencia hipertexto es simplemente la

	transferencia de ficheros hipertexto de un ordenador a otro. El protocolo de transferencia hipertexto es el conjunto de reglas utilizadas por los ordenadores para transferir ficheros hipertexto, páginas web, por Internet.
HTTPS (Secure Hyper Text Transfer Protocol)	El Protocolo Seguro de Transferencia de Hipertexto es utilizado para establecer conexiones del tipo HTTP pero de forma segura, utilizando TLS

I

Identificación	Procedimiento de reconocimiento de la identidad de un usuario.
IDS (Sistema de detección de intrusos)	Programa usado para detectar accesos desautorizados a un computador o a una red. Estos accesos pueden ser ataques de habilidosos piratas informáticos que usan herramientas automáticas. El funcionamiento de estas herramientas se basa en el análisis pormenorizado del tráfico de red que al entrar al analizador es comparado con modelos de ataques conocidos, y/o comportamientos sospechosos, como puede ser el escaneo de puertos, paquetes malformados, etc. Normalmente esta herramienta se integra con un cortafuegos. El detector de intrusos es incapaz de detener los ataques por si solo "excepto los que están integrados en un dispositivo de pasarela con funcionalidad de cortafuegos".
IETF - The Internet Engineering Task Force	Grupo principal auto-organizado comprometido en el desarrollo de nuevas especificaciones estándares para Internet (http://www.ietf.org).
Infeción	Acción que realiza un virus al introducirse en un sistema, empleando cualquier método, para poder ejecutar sus acciones dañinas y su carga destructiva, o bien simplemente al haber conseguido acceder al mismo.
Integridad	Servicio de seguridad que garantiza que los datos no han sido alterados o destruidos de modo no autorizado. Cuando se aplica sobre ficheros, son técnicas para conseguir archivos de backup correctos de modo que se pueda recurrir a ellos en caso de tener que recuperar datos críticos después de que los datos originales se contaminen debido a una acción accidental o provocada (por ejemplo, un virus).
Internet	Red informática mundial, descentralizada, formada por la conexión directa entre ordenadores mediante un protocolo especial de comunicación. Ofrece distintos servicios, como el envío y recepción de correo electrónico (e-mail), la posibilidad de ver información en las páginas Web, de participar en foros de discusión (News), de enviar y recibir ficheros mediante FTP, de charlar en tiempo real mediante IRC
Interoperabilidad	Es la capacidad de dos o más sistemas o componentes

	de intercambiar información y utilizar la información que ha sido intercambiada.
Intrusión	Cuando un hacker, entra en una máquina, sin que el usuario legítimo se de cuenta, y ya con el control de ésta máquina, puede realizar cualquier tipo de actividades. También se pueden dar intrusiones a redes locales, por ejemplo, la de una empresa, y así obtener información sensible y confidencial.
IPsec	Conjunto de protocolos desarrollado por el IETF para soportar intercambio seguros de paquetes a nivel IP donde el emisor y receptor deben compartir una llave pública. Ampliamente extendido para la implementación de Redes Privadas Virtuales (VPNs), soporta dos modos de cifrado: Transporte y Túnel.
ISO 17999	Estándar para la gestión de la seguridad de la información.

K

Keylogger	Programa que intercepta todas las pulsaciones realizadas en el teclado (e incluso a veces también el mouse), y las guarda en un archivo para obtener datos sensibles como contraseñas, etc. Posteriormente puede ser enviado a un tercero sin conocimiento ni consentimiento del usuario.
------------------	---

L

LAN - Red de Área Local	Red informática que cubre que área relativamente pequeña (generalmente un edificio o grupo de edificios).
LDAP - Protocolo de Acceso Ligero a Directorio	Protocolo para el acceso a directorios jerárquicos de información y que soporta TCP/IP.
Lista de distribución	Es una manera de tener una discusión de grupo por medio del correo electrónico y distribuir anuncios a un gran número de personas. Cada vez que un miembro de la lista envía una réplica a la conversación, ésta es distribuida por correo electrónico a todos los demás miembros.
Log	Fichero de texto en el que queda recogida toda la actividad que tiene lugar en un determinado ordenador, permitiendo para ciertos programas que su propietario o administrador detecte actividades ilícitas e identifique, por medio de su dirección IP, al usuario correspondiente.
Login	Nombre que es requerido al acceder a un sistema informático y que identifica al usuario. También sirve para que el usuario se identifique ante su proveedor de acceso Internet o al revisar el correo.

M

MAC - Dirección de Control de	Dirección hardware única que identifica únicamente cada nodo de una red
--------------------------------------	---

Acceso al Medio	
Mbps (Megabits por segundo)	Unidad de medida de la capacidad de transmisión por una línea de telecomunicación. Cada megabit está formado por 1.048.576 bits.
MD5	Función de hash con salida de 128-bits
Malware	Ver Código malicioso
Monitor de red	Véase sniffer

N

Navegador	Un navegador (también llamado navegador web o de internet) es el programa que permite visualizar los contenidos de las páginas Web en Internet. También se conoce con el nombre de browser. Algunos ejemplos de navegadores Web son: Internet Explorer, Netscape Navigator, Opera, etc.
No repudio	Servicio de seguridad que previene que un emisor niegue haber remitido un mensaje, cuando realmente lo ha emitido, y que un receptor niegue su recepción, cuando realmente lo ha recibido. En el primer caso se denomina no repudio en origen y el segundo no repudio en destino.
Nodo	Un nodo es el punto de unión entre varias redes. Es importante para la rapidez de las conexiones que el ordenador gestor sea potente y capaz de soportar un alto nivel de tráfico. Cada nodo de una red tiene un nombre distinto. En Internet, un nodo es un equipo con un sólo nombre de dominio y dirección
Nombre de dominio	Identificador único o dirección de un sitio, un servidor o una máquina, conectada a Internet, consta de dos o más partes separadas por puntos, la parte izquierda es más específica y la derecha es más general, normalmente todas las máquinas de una misma red tienen en común la parte derecha de su nombre de dominio.
Normas	Acuerdos documentados que contienen especificaciones técnicas o criterios precisos para ser usados consistentemente como reglas, guías, o definiciones de características, asegurando de esta forma que los materiales, productos, procesos y servicios son apropiados para lograr el fin para el que se concibieron
Nuke	Ver Pérdida de conexión
Número de identificación personal (PIN)	Contraseña de acceso para el uso de una diversidad de servicios: cajeros automáticos, conexión de teléfono móvil, etc..

P

PAP - Protocolo de Autenticación de Claves	El método más básico de autenticación, en el cual el nombre de usuario y la contraseña (clave) se transmiten a través de una red y se compara con una tabla de parejas nombre-clave, la no coincidencia provocará la desconexión. Típicamente, las
---	--

	<p>contraseñas almacenadas en la tabla se encuentran encriptadas. El principal defecto de PAP es que tanto el nombre de usuario como la clave se transmiten sin codificar, a diferencia de sistema CHAP.</p>
Parche de seguridad	<p>Conjunto de ficheros adicionales al software original de una herramienta o programa informático, que sirven para solucionar sus posibles carencias, vulnerabilidades, o defectos de funcionamiento. También conocidos como actualizaciones. En sistemas operativos Windows, son normalmente programas ejecutables que reemplazan las anteriores versiones para complementarlas y solucionar problemas sobre agujeros de seguridad. Existen conjuntos de parches, más estables, que incluyen varias actualizaciones a diversas fallas, que suelen ser llamados Service Packs, y son liberados cada cierto tiempo por las empresas responsables de las aplicaciones y sistemas operativos más utilizados.</p>
Pérdida de conexión (Nuke)	<p>Caída de la conexión de red, provocada de forma intencionada por alguna persona ó programa (nuker) provocando el bloqueo de un ordenador o impidiendo que éste pueda acceder a la red donde está conectado.</p>
Phishing	<p>Técnica en auge que consiste en atraer mediante engaños a un usuario hacia un sitio web fraudulento donde se le insta a introducir datos privados, generalmente números de tarjetas de crédito, nombres y passwords de las cuentas, números de seguridad social, etc... Uno de los métodos más comunes para hacer llegar a la "víctima" a la página falsa es a través de un e-mail que aparenta provenir de un emisor de confianza (banco, entidad financiera u otro) en el que se introduce un enlace a una web en la que el "phiser" ha reemplazado en la barra de dirección del navegador la verdadera URL para que parezca una legal.</p> <p>Una de las consecuencias más peligrosas de este fraude es que la barra "falsa" queda en memoria aún después de salir de la misma pudiendo hacer un seguimiento de todos los sitios que visitamos posteriormente y también el atacante puede observar todo lo que se envía y recibe a través del navegador hasta que éste sea cerrado.</p> <p>Una manera para el usuario de descubrir el engaño es que no se muestra la imagen del candado en la parte inferior del navegador que indica que la navegación es segura.</p>
PIN - Número de Identificación Personal	<p>Véase número de identificación personal</p>
Pirata informático	<p>Véase hacker</p>

PKI - Infraestructura de Clave Pública	Sistema de certificados digitales, Autoridades Certificadores y otras entidades de registro que verifican y autentican la validez de cada una de las partes implicadas en una transacción vía Internet.
Polimorfismo	Característica que presentan algunos virus consistente en que su código no siga un patrón fijo de caracteres de modo que es muy difícil detectarlo.
Privacidad	Derecho de los individuos a controlar e influir en la recogida y almacenamiento de datos relativos a ellos mismos, así como por quien y a quien pueden ser dados a conocer estos datos.
Protocolo	Normas a seguir en una cierta comunicación: formato de los datos que debe enviar el emisor, cómo debe ser cada una de las respuestas del receptor, etc.
Puerta Trasera	No se trata de un virus, sino de una herramienta de administración remota. Si es instalada por un hacker tiene la capacidad de dar a un atacante privilegios como administrador. Puede incluso buscar passwords y datos confidenciales y enviarlos vía mail a un área remota.
Punto de Acceso (PA)	Dispositivo inalámbrico central de una WLAN que mediante sistema de radio frecuencia (RF) se encarga de recibir información de diferentes estaciones móviles bien para su centralización, bien para su enrutamiento.
P2P (Peer to peer)	Programas -o conexiones de red- empleados para prestar servicios a través de Internet (intercambio de ficheros, generalmente). Algunos ejemplos de estos programas son KaZaA, Emule, eDonkey, etc. Es un modelo de comunicaciones en el cual cada parte tiene las mismas capacidades y cualquiera de ellas puede iniciar la comunicación. Otro modelo totalmente opuesto es el cliente/servidor en donde el servidor se encuentra a la espera de una comunicación por parte del cliente. Este modelo se basa en que ambos nodos actúen como servidores y clientes a la vez.

Q

QoS	(Quality Of Service) Calidad de servicio. En Internet y otras redes, designa la posibilidad de medir, mejorar y, en alguna medida, garantizar por adelantado los índices de transmisión y error. Es importante para la transmisión fluida de información multimedia.
------------	--

R

RADIUS - Remote Authentication Dial-In User Service	Sistema de autenticación y accounting empleado por la mayoría de proveedores de servicios de Internet (ISPs) si bien no se trata de un estándar oficial. Cuando el usuario realiza una conexión a su ISP debe introducir su nombre de usuario y contraseña,
--	---

	información que pasa a un servidor RADIUS que chequeará que la información es correcta y autorizará el acceso al sistema del ISP si es así.
RAS - Servidor de Acceso Remoto	Servidor dedicado a la gestión de usuarios que no están en una red pero necesitan acceder remotamente a ésta. Permite a los usuarios, una vez autenticados, obtener acceso a los archivos y servicios de impresora de una LAN desde una localización remota.
Repudio	Denegación, por una de las entidades implicadas en una comunicación, de haber participado en la totalidad o en parte de una comunicación.
Revocación	Anulación definitiva de un certificado digital, o bien, a petición del suscriptor, o bien, por propia iniciativa de la autoridad de certificación en caso de duda de la seguridad de las claves.
Riesgo	Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización.
Riesgo aceptable	Exposición a un riesgo asumido por una institución, normalmente por razones presupuestarias. Dado que la seguridad absoluta no existe, tras implantar los controles de seguridad pertinentes, queda un riesgo, o una exposición a un riesgo, que se denomina residual sin compensar.
Riesgo residual	Riesgo resultante tras implantar salvaguardas.
Robot	Programas que viajan por Internet, indexando páginas, localizando errores, etc, con el fin de alimentar a los buscadores. Estos programas son enviados y mantenidos por varias herramientas de búsqueda. Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización.
Roaming	En redes inalámbricas se refiere a la capacidad de moverse desde un área cubierta por un Punto de Acceso a otra sin interrumpir el servicio o pérdida de conectividad
Router	Dispositivo que transmite paquetes de datos a lo largo de una red. Un router está conectado al menos a dos redes, generalmente dos LANs o WANs o una LAN y la red de un ISP. Los routers emplean cabeceras y tablas de comparación para determinar el mejor camino para enviar los paquetes a su destino, y emplean protocolos como el ICMP para comunicarse con otros y configurar la mejor ruta entre varios hosts.
S	
Salvaguarda	Mecanismo capaz de reducir el riesgo y, también, acción fruto de una decisión para reducir un riesgo.

Servidor	Sistema informático (ordenador) que presta ciertos servicios y recursos (de comunicación, aplicaciones, ficheros, etc.) a otros ordenadores (denominados clientes), los cuales están conectados en red a él.
Servidor de Autenticación	Servidores que gestionan las bases de datos de todos los usuarios de una red y sus respectivas contraseñas para acceder a determinados recursos. Permiten o deniegan el acceso en función de los derechos atribuidos.
Shellcode	Conjunto de órdenes de ensamblador que, beneficiándose de fallos informáticos ejecutan un código después de sobrescribir la dirección de retorno de un programa o función mediante un desbordamiento (overflow) u otro método válido. Si el atacante consigue insertar su shellcode, cuando se produzca el desbordamiento y el salto, se ejecutará sus órdenes.
Smart Card	(véase tarjeta inteligente)
Sniffers	Programa y/o dispositivo que monitoriza la circulación de datos a través de una red. Los sniffers pueden emplearse tanto con funciones legítimas de gestión de red como para el robo de información. Los sniffers no autorizados pueden ser extremadamente peligrosos para la seguridad de una red ya que virtualmente es casi imposible detectarlos y pueden ser emplazados en cualquier lugar, convirtiéndolos en un arma indispensable de muchos piratas informáticos. Algunas herramientas sniffers conocidas son: WepCrack, Airtort o NetStumbler, entre otras...
SPAM	También conocido como <i>correo basura</i> , consiste en la práctica de enviar indiscriminadamente mensajes de correo electrónico no solicitados.
Spoofing (suplantación)	Técnica basada en la creación de tramas TCP/IP utilizando una dirección IP falseada; desde su equipo, un atacante simula la identidad de otra máquina de la red (que previamente ha obtenido por diversos métodos) para conseguir acceso a recursos de un tercer sistema que ha establecido algún tipo de confianza basada en el nombre o la dirección IP del host suplantado. Otros ataques de falseamiento conocidos son: <ul style="list-style-type: none"> • Web Spoofing: El pirata puede visualizar y modificar una página web (incluso conexiones seguras SSL) solicitada por la víctima. • E.mail Spoofing: Falsifica la cabecera de un e-mail para que parezca que proviene de un remitente legítimo. El principal protocolo de envío de e-mails, SMTP, no incluye opciones de autenticación, si bien existe una extensión (RFC 2554) que permite a un cliente SMTP negociar un nivel de seguridad con el servidor de correo. • ARP Spoofing: Hace referencia a la construcción de

	<p>tramas de solicitud y respuesta ARP falseadas, de forma que un determinado equipo de una red local envíe los paquetes a un host atacante en lugar de hacerlo a su destino legítimo.</p> <ul style="list-style-type: none"> • DNS Spoofing: En este caso se falsea una dirección IP ante una consulta de resolución de nombre (DNS) o viceversa, resolver con un nombre falso una cierta dirección IP.
Spyware	Pequeñas aplicaciones cuyo fin es el de obtener información, sin que el usuario se de cuenta, de tipo comercial. Generalmente se encuentran dentro de aplicaciones gratuitas en Internet.
SSL - Secure Sockets Layer	Precursor de TLS. Protocolo desarrollado por Netscape para la transmisión privada de documentos vía Internet cliente/servidor. Este protocolo establece un canal de comunicaciones cifrado que ayuda a prevenir la interceptación de información crítica, como números de tarjeta de crédito en la Web y en otros servicios de Internet. Además de la privacidad para los datos y mensajes, brinda autenticación de los datos logrando una mayor seguridad. Por convención, las URLs que precisen una conexión SSL comienzan con https, en lugar de http.
Stealth	Característica que tienen los virus para pasar inadvertidos ante el usuario al que infectan.

T

Tarjeta Inteligente	Pequeño dispositivo electrónico del tamaño de una tarjeta de crédito que contiene memoria digital y posiblemente un circuito integrado. Para utilizarla es necesario un pequeño lector especial para estos dispositivos.
TLS - Transport Layer Security	Protocolo estándar para la seguridad en comunicaciones que usan TCP/IP. Sus características son prácticamente las mismas que SSL
Trazabilidad	Cualidad que permite que todas las acciones realizadas sobre un sistema de tecnología de la información sean asociadas de modo inequívoco a un individuo o entidad
Troyano	Programa aparentemente inofensivo. Puede de hecho parecer ser útil y engañarle para usarlo. Pero luego, mientras el programa se está ejecutando, el troyano abrirá puertas traseras y expondrá su ordenador a hackers. Normalmente, el daño inmediato es insignificante, pero deja su máquina desprotegida, permitiendo que le roben información sensible y/o tomar el control remotamente de su máquina.

V

Virus	Programa diseñado para copiarse y propagarse a sí mismo, normalmente adjuntándose en aplicaciones. Cuando se ejecuta una aplicación infectada, puede
--------------	--

	<p>infectar otros archivos. Se necesita acción humana para que un virus se propague entre máquinas y sistemas. Esto puede hacerse descargando archivos, intercambiando disquetes y discos USB, copiando archivos a y desde servidores de archivos o enviando adjuntos de e-mail infectados. Los efectos que pueden provocar varían dependiendo de cada tipo de virus: mostrar un mensaje, sobrescribir archivos, borrar archivos, enviar información confidencial mediante emails a terceros, etc. Los más comunes son los que infectan a ficheros ejecutables.</p>
Virus de acción directa	<p>No permanecen en memoria. Por tanto, su objetivo prioritario es reproducirse y actuar en el mismo momento de ser ejecutados. Al cumplirse una determinada condición, se activan y buscan los ficheros ubicados dentro de su mismo directorio para contagiarlos. Además, también realizan sus acciones en los directorios especificados dentro de la línea PATH (camino o ruta de directorios), dentro del fichero AUTOEXEC.BAT (fichero que siempre se encuentra en el directorio raíz del disco duro). Los virus de acción directa presentan la ventaja de que los ficheros afectados por ellos pueden ser desinfectados y restaurados completamente.</p>
Virus de archivo	<p>Adjuntado a un archivo de programa, normalmente un archivo .EXE o un .COM. Usa diferentes técnicas para infectar otros archivos de programas. Este tipo de virus puede transferirse a/desde todos los tipos de medios de almacenamiento (solo desde CD-ROM) y en una red.</p>
Virus de compañía	<p>Son virus de archivo que al mismo tiempo pueden ser residentes o de acción directa. Su nombre deriva de que "acompañan" a otros ficheros existentes en el sistema antes de su llegada, sin modificarlos como hacen los virus de sobreescritura o los residentes. Para efectuar las infecciones, los virus de compañía pueden esperar ocultos en la memoria hasta que se lleve a cabo la ejecución de algún programa, o actuar directamente haciendo copias de sí mismos.</p>
Virus de enlace	<p>Es un tipo de virus que modifica la dirección donde se almacena un fichero, sustituyéndola por la dirección donde se encuentra un virus (en lugar del fichero original). Esto provoca la activación del virus cuando se utiliza el fichero afectado.</p>
Virus de FAT	<p>Son virus que atacan a la tabla de asignación de ficheros o FAT, especialmente peligrosos. Impedirán el acceso a ciertas partes del disco, donde se almacenan los ficheros críticos para el normal funcionamiento del ordenador. Los daños causados a la FAT se traducirán en pérdidas de la información contenida en ficheros individuales y en directorios completos.</p>

Virus de Ingeniería Social	Este término es utilizado frecuentemente para describir los trucos utilizados por los virus de correo masivo para atraer a los receptores de los mensajes con archivos adjuntos infectados para ejecutarlos o visualizarlos.
Virus de macro	Pueden incluirse en todos los tipos de archivos que usen un lenguaje macro, tales como Word, Excel, Access y Word Pro. El virus se propaga de un documento a otro, y la infección tiene lugar cuando se abre el documento.
Virus de sector de arranque y de partición	A menudo están presentes en disquetes sin el conocimiento del usuario. La mayoría de los PCs están configurados para intentar arrancar de la unidad a: antes que del disco duro, cuando un usuario inicia o reinicia el ordenador, el virus de sistema infectará el sector de arranque y el sector de partición si el disco infectado está en la disquetera.
Virus de sobre-escritura	Se caracterizan por destruir la información contenida en los ficheros que infectan. Cuando infectan un fichero, escriben dentro de su contenido, su propio código, haciendo que queden total o parcialmente inservibles. También se diferencian porque los ficheros infectados no aumentan de tamaño, a no ser que el virus ocupe más espacio que el propio fichero. La única forma de limpiar un fichero infectado por un virus de sobreescritura es borrarlo, perdiéndose su contenido. Aunque existen herramientas de ficheros sobreescritos.
Virus multipartito	Virus muy avanzados, que pueden realizar múltiples infecciones, combinando diferentes técnicas para ello. Su objetivo es cualquier elemento que pueda ser infectado: archivos, programas, macros, discos, etc. Se consideran muy peligrosos por su capacidad de combinar muchas técnicas de infección y por los dañinos efectos de sus acciones.
Virus residentes	La característica principal de estos virus es que se ocultan en la memoria RAM de forma permanente o residente. De este modo, pueden controlar e interceptar todas las operaciones llevadas a cabo por el sistema operativo, infectando todos aquellos ficheros y/o programas que sean ejecutados, abiertos, cerrados, renombrados, copiados, etc. Estos virus sólo atacan cuando se cumplen ciertas condiciones definidas previamente por su creador (por ejemplo, una fecha y hora determinada). Mientras tanto, permanecen ocultos en una zona de la memoria principal, ocupando un espacio de la misma, hasta que son detectados y eliminados.
Vulnerabilidad	Fallos o huecos de seguridad detectados en algún programa o sistema informático, que los virus utilizan

	para propagarse e infectar. Estos errores de programación y/o diseño permiten que un tercero se aproveche de ellos para realizar acciones tales como ataques, intrusiones o cualquier otro uso indebido.
VPN - Red Privada Virtual VPN	Red privada que se configura dentro de una red pública. Para establecer este tipo de red, la integridad de los datos y la confidencialidad se protegen mediante la autenticación y el cifrado. Por ejemplo, los datos se pueden transmitir de forma segura entre dos sucursales a través de Internet o cifrarse entre un servidor y un cliente en una Red de área local (<i>LAN</i>).

W

WAN	Es una red de área extensa, o grupo de ordenadores que se encuentran conectados entre sí, pero distantes geográficamente. La conexión se realiza mediante línea telefónica, radioenlaces, vía satélite o cualquier sistema de intercambio de paquetes.
Warchalking	Es la práctica de dibujar en paredes o aceras una serie de símbolos para indicar a otros la proximidad de un acceso inalámbrico.
Warspamming	Acceso no autorizado a una red inalámbrica y uso ilegítimo de la misma para enviar correo masivo (spam) o realizar otro tipo de acciones que comprometan el correcto uso de un sistema.
WEP - Wired Equivalent Privacy	Protocolo para la transmisión de datos "segura" en redes inalámbricas. El cifrado puede ser ajustado a 128 bits, 64 bits o deshabilitada. La configuración de 128 bits da el mayor nivel de seguridad. También hay que recordar que todas las estaciones que necesiten comunicarse deben usar la misma clave para generar la llave de encriptación. Este protocolo tiene bastantes vulnerabilidades, existe software que permite conocer la clave fácilmente
Wi-Fi - Tecnología utilizada en Redes Inalámbricas	Abreviatura de Wireless Fidelity. Es el nombre "comercial" con que se conoce a todos los dispositivos que funcionan sobre la base del estándar 802.11 de transmisión inalámbrica. En lenguaje popular: Redes wifi.
WPA - Wireless Protected Access	Protocolo de Seguridad para redes inalámbricas. Cifra las comunicaciones de WIFI. Se basa en el estándar 802.11i
WPA2 - Wireless Protected Access	Protocolo de seguridad para redes wifi, definido en el estándar 802.11i. Reemplaza al protocolo temporal WPA. Se basa en el algoritmo AES y se debe incorporar a todos los Access Point de última generación.