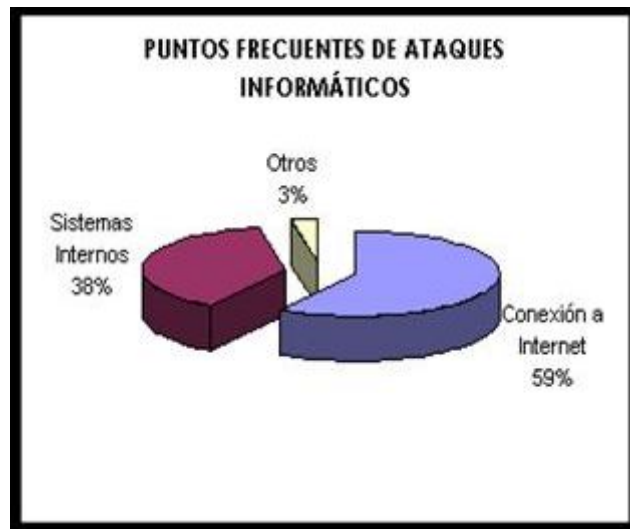


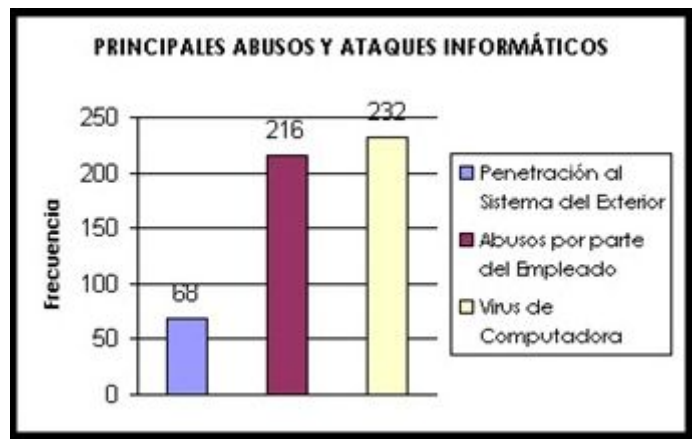
ACTIVIDAD 1 : Describir ampliamente y con detalles y ejemplos el significado de cada una de las siguientes palabras :

1. AMENAZAS

1.1. Ataques

Se trata de accesos a alguno de los sistemas internos a través de entradas o puertos desconocidos por el usuario.





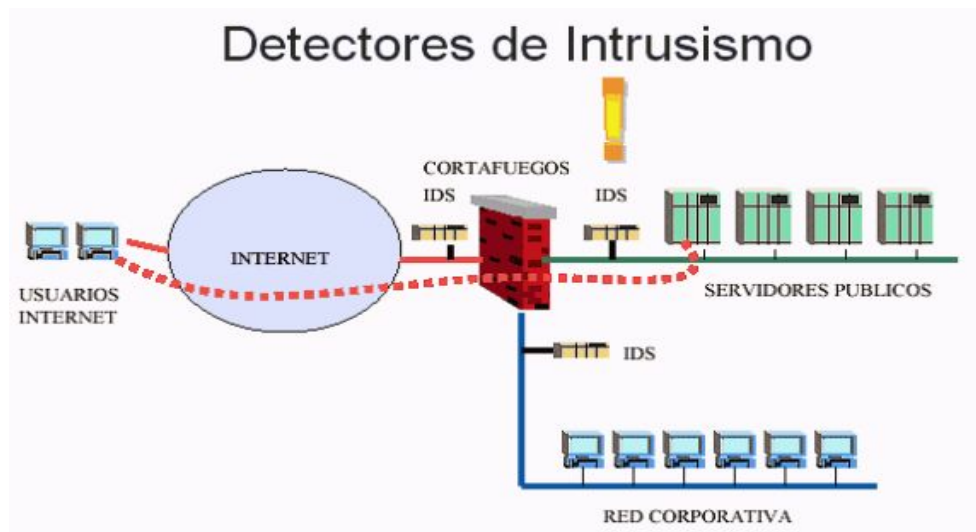
1.2. Intrusiones

Es un acceso a los sistemas informáticos puede realizarse de forma remota o directa. El acceso directo se realiza en el equipo que contiene el sistema informático ajeno. Para la intrusión informática remota se usa una red informática privada o pública. Podría pensarse que el simple acceso ya cumple con el delito prescrito, pero lo cierto es que esa intrusión debe permitir la disponibilidad de los datos contenidos en ese sistema.



Para prevenir las intrusiones hay los IDS (sistema de detección de intrusiones) que es un programa de detección de accesos no autorizados a un computador o a una red.

El IDS detecta, gracias a dichos sensores (obtiene datos externos sobre el tráfico de red), las anomalías que pueden ser indicio de la presencia de ataques y falsas alarmas.



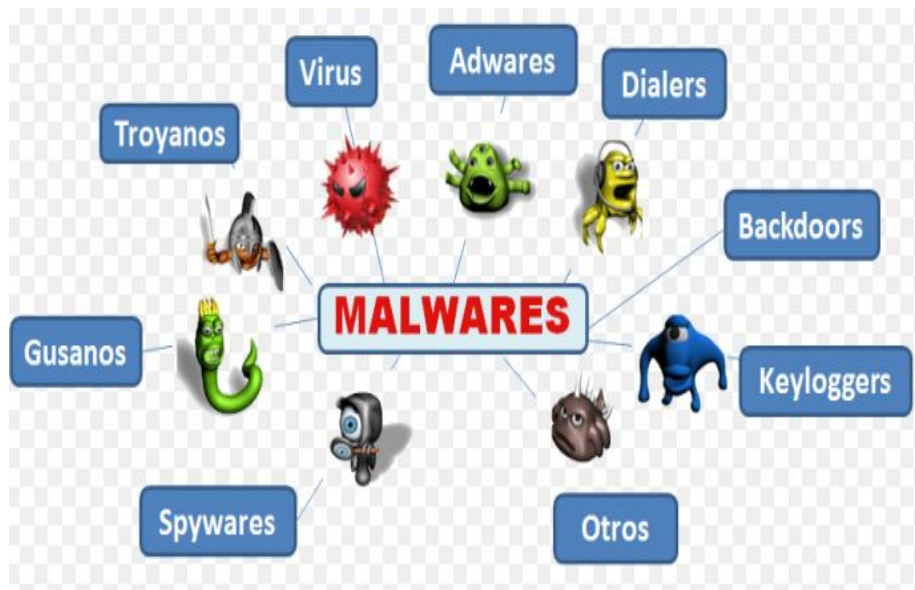
1.3. Robo de las transmisiones

Se trata de la captura de datos de índole personal o relevante cuando la información viaja a través de Internet.



1.4. Código malicioso (malware)

Se introducen programas malintencionados (virus, troyanos o gusanos) en nuestro equipo, dañando el sistema de múltiples formas.



1.5. Virus

Los Virus Informáticos son sencillamente programas maliciosos (malwares) que “infectan” a otros archivos del sistema con la intención de modificarlo o dañarlo.

Se ejecuta un programa que está infectado, en la mayoría de las ocasiones, por desconocimiento del usuario. El código del virus queda residente en la memoria RAM de la computadora, aun cuando el programa que lo contenía haya terminado de ejecutarse.

El virus toma entonces el control de los servicios básicos del sistema operativo, infectando, de manera posterior, archivos ejecutables (.exe., .com, .scr, etc) que sean llamados para su ejecución. Finalmente se añade el código del virus al programa infectado y se graba en el disco, con lo cual el proceso de replicado se completa.



1.6. Gusano

Los gusanos (o worm) son programas desarrollados para reproducirse por algún medio de comunicación como el correo electrónico (el más común), mensajeros o redes P2P.

El objetivo de los mismos es llegar a la mayor cantidad de usuarios posible y lograr distribuir otros tipos de códigos maliciosos como Troyanos, Backdoors y Keyloggers.

Estos últimos serán los encargados de llevar a cabo el engaño, robo o estafa.

Otro objetivo muy común de los gusanos es realizar ataques de DDoS (*) contra sitios webs específicos o incluso eliminar "virus que son competencia" para el negocio que se intente realizar.



1.7. Troyano

Se denomina Troyano (o 'Caballo de Troya') a un virus informático o programa malicioso capaz de alojarse en computadoras y permitir el acceso a usuarios externos, a través de una red local o de Internet, con el fin de recabar información.

Suele ser un programa pequeño alojado dentro de una aplicación, una imagen, un archivo de música u otro elemento de apariencia inocente, que se instala en el sistema al ejecutar el archivo que lo contiene.

Una vez instalado parece realizar una función útil (aunque cierto tipo de troyanos permanecen ocultos y por tal motivo los antivirus o antitroyanos no los eliminan) pero internamente realiza otras tareas de las que el usuario no es consciente, de

igual forma que el Caballo de Troya que los griegos regalaron a los troyanos.

Habitualmente se utiliza para espiar, usando la técnica para instalar un software de acceso remoto que permite monitorizar lo que el usuario legítimo de la computadora hace y, por ejemplo, capturar las pulsaciones del teclado con el fin de obtener contraseñas u otra información sensible.

La mejor defensa contra los troyanos es no ejecutar nada de lo cual se desconozca el origen y mantener software antivirus actualizado. Es recomendable también instalar algún software anti troyano, de los cuales existen versiones gratis aunque muchas de ellas constituyen a su vez un troyano.

Otra manera de detectarlos es inspeccionando frecuentemente la lista de procesos activos en memoria en busca de elementos extraños, vigilar accesos a disco innecesarios, etc.

1.8. Programa espía (o Spyware)

Programa capaz de extraer o robar información relevante o personal del ordenador donde están instalados, incluidos datos financieros como números de tarjeta de crédito o cuentas bancarias.

Para hacer frente a este programa hay un programa gratuito llamado : Spybot - Search & Destroy que limpia el ordenador de programas y cookies espías (además impide la instalación automática



1.9. Capturador de teclado (o Keylogger)

Se utiliza una herramienta que permite conocer todo lo que el usuario escribe a través del teclado, e incluso pueden realizar capturas de pantalla.



1.10. Programa comercial (o Adware)

Programa que se instalan en el PC para obtener beneficios comerciales. Pueden ofrecer anuncios publicitarios no solicitados en pop ups o controlar la actividad de búsqueda en la Web para fines comerciales, redirigiendo al usuario a ciertas páginas de forma automática



1.11. Marcador (o Dialer) : Broma (o Joke)

Programa capaz de marcar un nº de teléfono de pago para iniciar la conexión a Internet mediante un MODEM y sin conocimiento del usuario. Han caído en desuso desde la aparición de los routers y las conexiones a Internet con tarifa plana, pero aún causan daños económicos a usuarios con equipos con módem incorporado, generalmente portátiles.



1.12. Rumor(o Hoax)

Mensaje o alerta que advierte de un riesgo o una vulnerabilidad que resulta ser falsa. En ocasiones, usuarios que hacen caso del rumor han causado daños a la integridad del

sistema de forma involuntaria, por ejemplo, borrando ficheros vitales porque habían sido advertidos de que dichos ficheros podrían suponer un riesgo



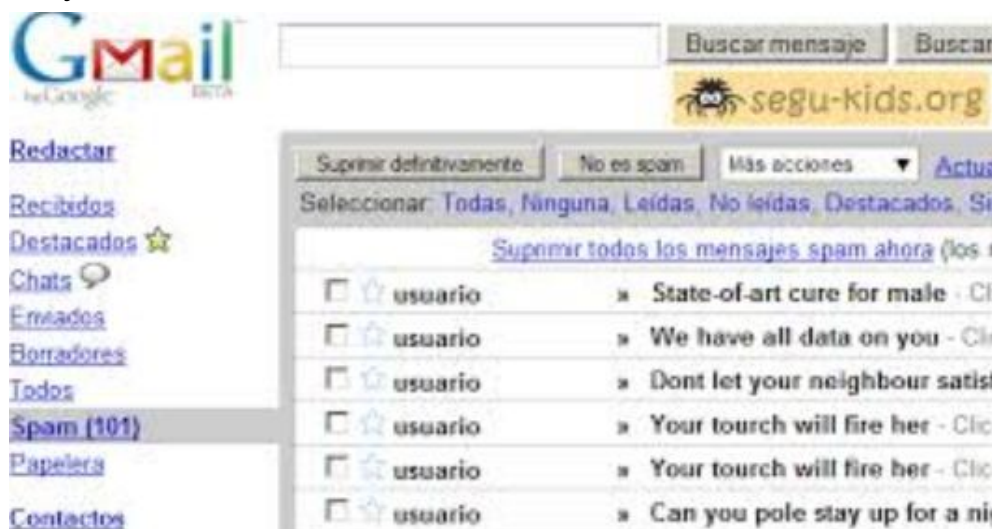
1.13. Amenaza Combinada (o Blended Threat)

Se trata del uso combinado de distintos tipos de malware. Por ejemplo, un fichero aparentemente inofensivo (Troyano) podría contener un virus que se reprodujera y entrara en acción al cabo de un tiempo y un gusano encargado de enviarse continuamente a través del correo electrónico, facilitando así su propagación masiva. Este tipo de amenazas malware son la más peligrosas y cada vez, más comunes.



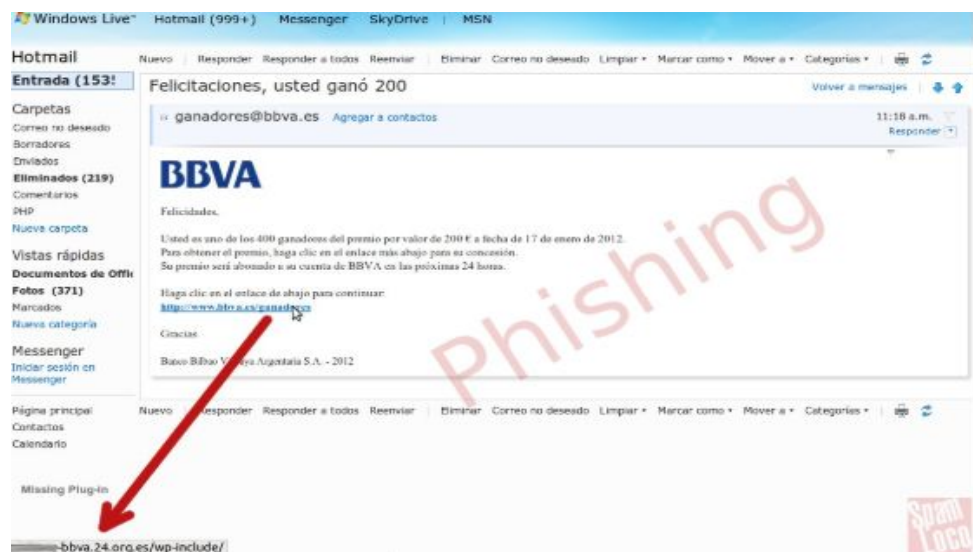
1.14. Correo basura (o Spam)

Mensajes electrónicos no deseados o no solicitados. Los hay de muchos tipos y van desde anuncios publicitarios legítimos a publicidad engañosa y mensajes de phishing destinados a engañar a los destinatarios para que faciliten información personal y financiera.



1.15. Phishing

Se engaña al usuario para obtener su información confidencial suplantando la identidad de un organismo o página web de internet.



1.16. Contenidos Web inadecuados

La información almacenada en Internet es inmensa y en ocasiones no todos los contenidos son adecuados para todo el mundo, ocasionando riesgos a distintas escalas. Por ejemplo, los niños pueden verse afectados visitando sitios Web con contenidos para adultos o con violencia explícita, etc. También supone un riesgo de pérdida de productividad la visita de sitios Web con contenidos de ocio o lúdicos. Por último, hay páginas Web con contenidos considerados potencialmente peligrosos si se descargan, pues incluyen ficheros malware, troyanos, adwares, etc.

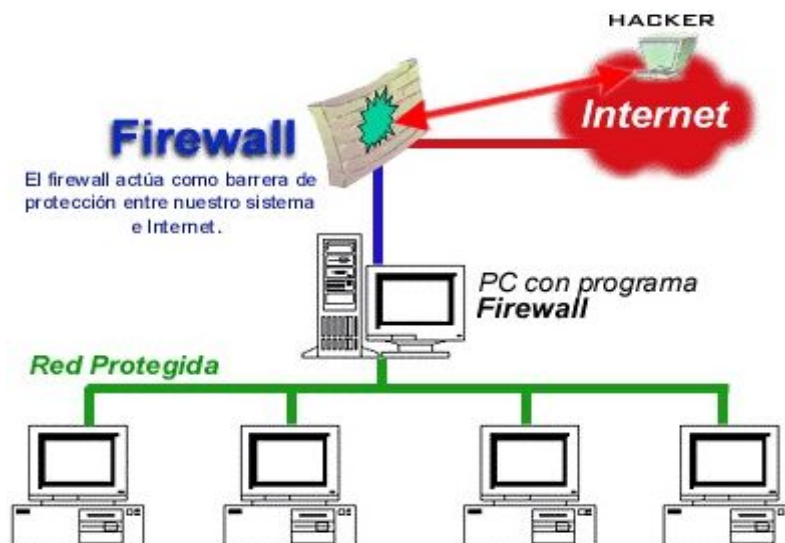
Exposición a contenidos inadecuados



2. TECNOLOGÍA

2.1. Firewall

También llamado cortafuegos, es una barrera informática por la que pasa toda la información y evita que los ordenadores de una red se comuniquen directamente con sistemas informáticos externos. El software del firewall analiza la información que pasa entre ambas partes y la rechaza si no se ajusta a unas reglas predeterminadas. Es la tecnología utilizada para eludir los ataques a nivel de red.



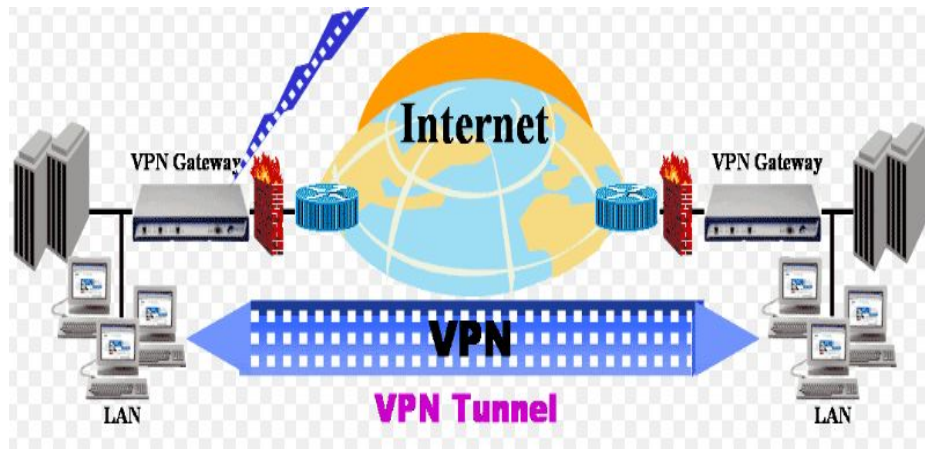
2.2. Sistema de Prevención de Intrusiones (o IPS)

Es un conjunto de reglas que impide el mal uso de las conexiones establecidas entre dos sistemas o dos redes. Evita las Intrusiones a nivel de red.

2.3. Red Privada Virtual (o VPN)

Es una tecnología que permite enviar la información a través de Internet de forma protegida. Toda la información viaja

cifrada y si alguien es capaz de capturar la información resulta inútil. Evita el robo de las transmisiones a nivel de red.



2.4. Software Antivirus/Antimalware

Programas que exploran la memoria de un ordenador o las unidades de disco en busca de virus u otros malware. Si los encuentran, la aplicación informa al usuario y éste tiene la posibilidad de limpiar, eliminar o poner en cuarentena los archivos, directorios o discos infectados por el código malintencionado.

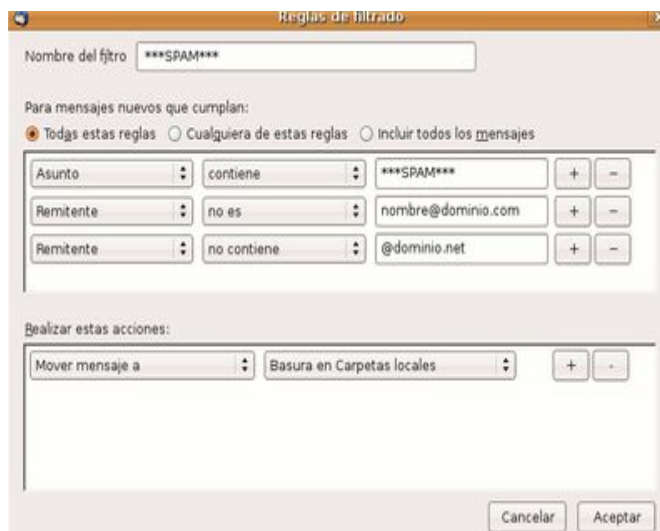


2.5. Filtro de correo no deseado (o Antispam)

Programa que detecta correo electrónico no deseado (spam) y evita que llegue al buzón del usuario.

2.6. Filtro de Web o de URLs

Protección que analiza las peticiones de páginas Web y la compara con una base de datos de reputación, decidiendo si la página es adecuada o no para el usuario, basándose en los contenidos de la misma o la categoría en la que se halle dicha página. El sistema puede bloquear el acceso a la página o simplemente advertir al usuario del contenido inadecuado de la misma.



Reglas de filtrado

Nombre del filtro: ***SPAM***

Para mensajes nuevos que cumplan:

☒ Todas estas reglas ☐ Cualquiera de estas reglas ☐ Incluir todos los mensajes

Asunto	:	contiene	:	***SPAM***	+	-
Remitente	:	no es	:	nombre@dominio.com	+	-
Remitente	:	no contiene	:	@dominio.net	+	-

Realizar estas acciones:

Mover mensaje a	:	Basura en Carpetas locales	+	-
-----------------	---	----------------------------	---	---

Cancelar Aceptar

3. PERSONAS

3.1. Hacker

Expertos informáticos con una gran curiosidad por descubrir las vulnerabilidades de los sistemas pero sin motivación económica o dañina

3.2. Hacker ético (o Sneaker)

Expertos que suele ser contratado por empresas para descubrir huecos o vulnerabilidades de seguridad en sus sistemas y así mejorar la protección.

Fases del Ethical Hacking.



3.3. Craker

Un hacker que, cuando rompe la seguridad de un sistema, lo hace con intención maliciosa, bien para dañarlo o para obtener un beneficio económica

3.4. Pirata

Experto en ingeniería inversa capaz de modificar los programas legales para eliminar su protección y utilizarlos de forma ilegítima. Por extensión, cualquier persona que hace uso ilegítimo de un programa, ya sea de pago obligado o Shareware.

3.5. Ciberdelincuente

Término que agrupa a Piratas, Crackers y otros usuarios malintencionados, que se valen de Internet para cometer delitos como robo de identidad, secuestro de PC, envío ilegal de spam, phishing, pharming y otros tipos de fraude.

4. TÉCNICAS

4.1. Firma

Es un patrón de búsqueda, con forma de cadena simple de caracteres o bytes, que se encuentra en un virus particular o en una familia de virus. Los programas antivirus las utilizan para identificar virus específicos. La firma suele contener el código de remediación o vacuna contra ese virus. De este modo, existen ficheros infectados que pueden ser reparados y recuperados para su uso normal.

4.2. Falso negativo

Error que sucede cuando el programa antivirus no es capaz de indicar que un archivo que contiene un virus, está infectado. Los falsos negativos son comunes en antivirus basados únicamente en firmas, al aparecer virus nuevos o modificados, ya

que son desconocidos y es necesaria una protección proactiva adicional.

4.3. Falso positivo

Error que sucede cuando el programa antivirus indica, erróneamente, que un archivo está infectado. Puede producirse con programas que tienen características de comportamiento similares a los virus aunque en realidad no lo son.

4.4. Análisis Heurístico

Modo de detección de malware desconocido que consiste en comparar el código de un fichero con múltiples patrones de distintos tipos de virus para comprobar si alguno de estos patrones correlacionados con otros están presentes en el código del fichero. De este modo se puede determinar que un fichero es sospechoso de contener malware.

4.5. Análisis Bayesiano

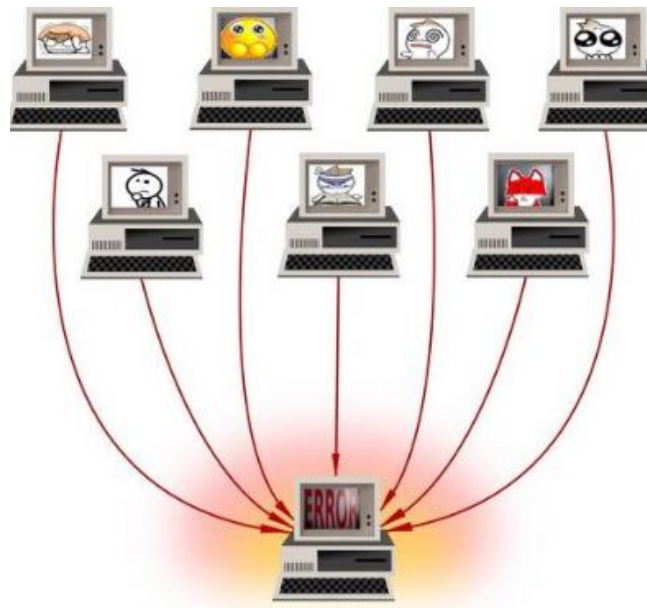
Técnica que aplica el teorema de Bayes a la detección de amenazas, mediante aproximaciones de probabilidad de diversas variables, se puede determinar con más o menos certeza que un fichero es malware o no, que un correo es spam, etc.

4.6. Protección proactiva

Los sistemas de seguridad más potentes utilizan técnicas proactivas para detectar ficheros sospechosos de contener malware o amenazas que aún no han sido catalogadas (malware desconocido) y ejecutar acciones de contención del fichero hasta que se determine fehacientemente si se trata de malware o no.

4.7. Denegación de Servicio (DoS)

Tipo de ataque al sistema que provoca un funcionamiento anormal en el que los usuarios autorizados no pueden acceder al servicio. Los hackers pueden efectuar un ataque de denegación de servicio con la destrucción o modificación de datos, o con la sobrecarga de los servidores del sistema hasta que el servicio a los usuarios autorizados se retrase o se paralice. Es un ataque muy común y de ahí, su popularidad. Las técnicas para llevarlo a cabo son muy variadas (smurfing, ping flood, teardrop attack, Nuke ...)



4.8. Sitio Web manipulado

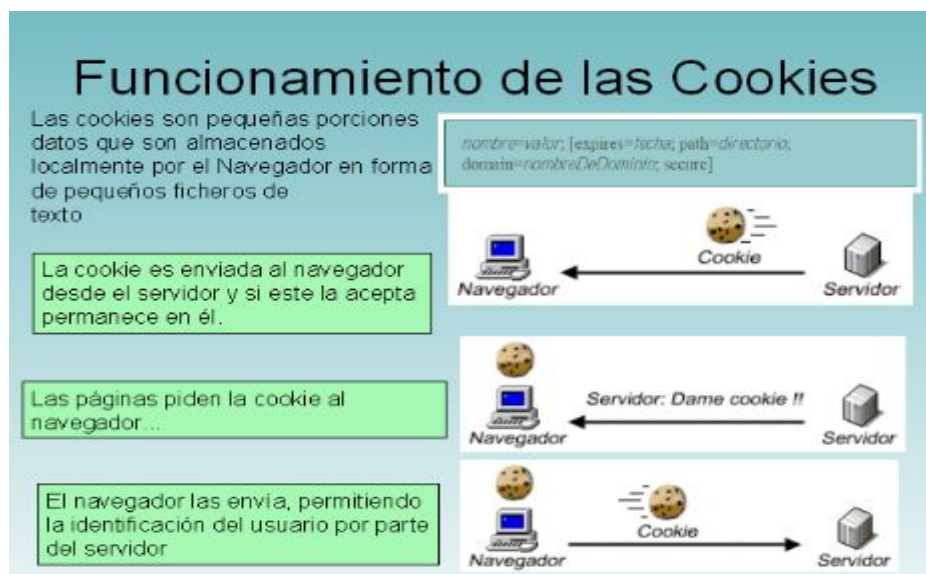
Web que imita con exactitud el sitio real de una empresa (sobre todo sitios de servicios financieros) para robar información privada (contraseñas, números de cuenta) a las personas que engañan para que lo visiten. Está vinculado a las estafas de phishing.

4.9. Pharming

Es una técnica por la que un dominio de Internet es redirigido automáticamente a otro creado por un cracker. El dominio de destino, no tiene porqué tener el mismo aspecto que el original, en cuyo caso se relacionaría con el phishing.

4.10. Cookies

Ficheros de texto instalados en el directorio del navegador que guardan información sobre preferencias y datos diversos del usuario durante la navegación. Estos ficheros personalizan la navegación y activan ciertas respuestas por parte de las páginas Web a las que se conecta. No tienen porqué suponer una amenaza, sin embargo, en muchas ocasiones se utilizan para permitir accesos de gusanos o adware, sin conocimiento del usuario



4.11. Shareware (programas compartidos)

Software distribuido sin coste alguno para su evaluación. Pasado el período de prueba el usuario debe pagar al autor en concepto de derechos o borrar el programa. Utilizar shareware sin registrar después del plazo de evaluación es un acto de piratería informática

Licencias

- **Shareware:** software que primero se prueba y luego se paga.
- La garantía, es absoluta y el riesgo nulo.
- Si después del periodo de prueba el usuario decide quedarse el programa, deberá comunicarse con los autores y pagar el dinero establecido (**registrarse**).
- **Ejemplos:** manejador de archivos *Total Commander*, y la mayoría de los antivirus.



4.12. Freeware (programas gratuitos)

Programas distribuidos de forma gratuita sin ninguna restricción. Se suelen confundir con el Shareware, pero el uso de los programas Freeware no supone ningún delito

	S. LIBRE
NAVEGADOR	 MOZILLA FIREFOX
SUITE OFIMÁTICA	 LibreOffice
REPRODUCTOR DE VIDEO	 VLC
REPRODUCTOR DE SONIDO	 AMAROK
SISTEMA OPERATIVO	 Linux
EDITOR DE IMAGENES	 GIMP
EDITOR DE VIDEOS	 Open Movie Editor
EDITOR DE AUDIO	 Audacity
PROGRAMA DE ANIMACIÓN	 Koon

4.13. Zombie o Robot

PC infectado con un virus o un troyano que lo somete al control remoto de un secuestrador online. Se utilizan para generar spam o lanzar ataques de denegación de servicio a terceros

4.14. Red de Robots (o Botnet)

Grupo de ordenadores secuestrados y controlados a distancia por un cracker que los utiliza para enviar correo basura y lanzar ataques de denegación de servicio sin consentimiento (y sin conocimiento) del propietario del equipo.





4.15. Que es el Centro Nemesys

Es la unidad de Telefónica que atiende incidencias que puedan surgir por el uso indebido de las redes de Telefónica en Internet (abusos de Internet), ya sea de Internet hacia clientes de Telefónica o viceversa.

Estas incidencias se reciben en buzones específicos destinados en exclusiva para esta finalidad.

El centro Nemesys de Telefónica es un servicio que identifica a los usuarios que envían spam, virus, o que realizan intentos de intrusión, hacking, etc. Si caemos en su lista negra, la consecuencia es que se nos prohibirá el envío de correos a cualquier dirección de Telefónica, o incluso nos bloquee el envío de cualquier correo electrónico a cualquier dominio si el usuario o empresa accede a Internet

Registro de incidencias en la red IP y RIMA

Cumpliendo con la obligación legal, ponemos a su disposición los medios necesarios para la atención de denuncias de incidencias y abusos de carácter delictivo en Internet con origen en la red RIMA (red IP propiedad de Telefónica de España).

Las incidencias que nos puede hacer llegar a través de este medio son, entre otras, las relativas a:

- **Correo electrónico no solicitado (spam):** Mensajes no solicitados, habitualmente de tipo publicitario, enviados en cantidades masivas.
- **Hacking:** Uso de procedimientos ilegales con el objetivo de piratear sistemas informáticos y redes de comunicación.
- **Ataques de denegación de servicio:** Saturación de un servidor con peticiones falsas hasta dejarlo fuera de servicio.
- **Sniffing y spoofing:** Obtención ilegal de la información que circula a través de Internet.

Para continuar, le solicitaremos que detalle los hechos denunciados.

Si su PSI (Proveedor de servicios de Internet) no es Telefónica de España, le solicitaremos:

- El nombre de su PSI
- La dirección de correo electrónico de su PSI

La información aportada será enviada al administrador de la red RIMA (red IP de Telefónica de España) para que, tras su análisis, se tomen las medidas oportunas.