Charlas sobre Internet

Madrid
Agosto - 2005
Abril – 2004

Valentín Used

Incide:

Contenido:

Paginas	86
Palabras	22.146
Caracteres (sin espacios)	118.958
(con espacios)	140.289
Párrafos	1.644
Líneas	3.823

Actualizaciones:

- Versión original Abril/04
- Ampliaciones / Modificaciones:
  - **I.** Marzo/05
  - **II.** Junio/05
  - **III.** Agosto/05

CHARLAS SOBRE INTERNET

Breve historia:

Origen de Internet

1969: Surge ARPAnet, que es una Agencia de Proyectos de Investigación Avanzada de Defensa, del Departamento de Defensa de EEUU.

Es una red experimental en la cual se probaron las teorías y software en los que está basado Internet en la actualidad. Esta red no existe en la actualidad.

Esta red gestionada por DARPA, es el origen de Internet, basado en el intento de conectar esta red (ARPAnet) a otras redes mediante enlaces de satélite, radio y cableado.

Es una red experimental que apoya a la investigación militar, en concreto sobre la resistencia a fallos parciales.

La filosofía de esta red consiste en que cada uno de los ordenadores que componen la misma sea capaz de comunicarse, como elemento individual, con cualquier otra computadora de la red.

ARPAnet en principio interconectaba 4 grandes ordenadores en localizaciones secretas de EEUU.

DARPA fue quien diseñó específicamente el protocolo de comunicaciones TCP/IP (Transmission Control Protocol/Internet Protocol), extendido actualmente de forma espectacular.

Desarrollo en los 70

1972: Existen ya 40 hosts o nodos de red. Se organiza la Conferencia Internacional de Comunicaciones entre Ordenadores, con la demostración de ARPAnet entre estos 40 equipos.

Incremento de la demanda de usuarios académicos e investigadores. Primeras conexiones internacionales con ARPAnet: Inglaterra y Noruega (1973).

Además de utilizarse como medio de intercambio de datos de investigación, los usuarios comienzan a comunicarse mediante buzones personales de correo electrónico.

A su vez, la Organización de la Estandarización Internacional (ISO: International Organization for Standarization) diseñaba el último estándar para la comunicación entre ordenadores.

Los diseñadores de Internet en EEUU, en respuesta a las presiones del mercado, empezaron a poner el software IP en todo tipo de ordenadores.

En la actualidad hay del orden de 200 fabricantes que poseen el protocolo TCP/IP.

1976: Se desarrolla la tecnología UUCP (Unix to Unix CoPy) en los laboratorios Bell de AT&T. Un año después se distribuye con Unix.

Desarrollo en los 80

Progresiva conexión de ordenadores pertenecientes a Universidades y Centros de Investigación, desarrollando programas e investigaciones con usos militares.

1983: Se desarrolla el servidor de nombres (DNS), evitando direcciones numéricas (a nivel usuario). Frente al incremento de tráfico, se divide la red en MIL (Militar y restringida) y ARPA (Para el resto de comunicación).

Frente al incremento de tráfico, se divide la red en MIL (Militar y restringida) y ARPA (Para el resto de comunicación). La unión de ambas se denomina DARPA Internet.

Paralelamente, se desarrollan las redes de área local Ethernet con protocolos de comunicación de ARPANet, permitiendo el entendimiento entre redes. (En 1983 aparecen las primeras estaciones de trabajo para escritorio).

Estas redes pertenecen a Universidades, Centros de Investigación y Firmas Comerciales (Usenet, BITnet, EUNet, DECNet).

1984: La NSF (Fundación Nacional de la Ciencia) intenta hacer uso de ARPANet para facilitar el acceso a cinco Centros de Proceso de Datos, localizados en las principales universidades americanas. Por razones burocráticas no se pudo utilizar ARPANet.

1984: La NSF decide crear su propia red, denominada NSFNet, basada en la tecnología ARPANet, que acabaría convirtiéndose en la auténtica espina dorsal de Internet.

El número de hosts rebasa los 1.000.

El éxito alcanzado fue tal, que hizo necesaria sucesivas ampliaciones de la capacidad de las líneas troncales. NSFNet, es todavía una de las piezas más importantes dentro de Internet.

Debido al coste de las líneas telefónicas, se decidió crear redes regionales. El tráfico en la red se incrementó con el tiempo hasta la saturación de los ordenadores centrales y líneas telefónicas.

En 1987 se realizó un contrato para actualizar y administrar la red, con la compañía Merit Network Inc., en colaboración con IBM Y MCI (Microwave Comunnications Incorporated). Se mejoraron las líneas en un factor de 20, con hosts más poderosos.

El "gusano" (worm) de Internet, se transmite por la red, afectando a 6.000 ordenadores de los 60.000 que componían la red.

1989: El número de hosts es de 100.000.

El grupo de mayor autoridad sobre el desarrollo de la red es la Internet Society, creado en 1990 y formado por miembros voluntarios, cuyo propósito principal es promover el intercambio de información global mediante la tecnología Internet.

Desaparece ARPANet.

Desarrollo en los 90

1992: Se desarrolla World Wide Web. El número de hosts, rebasa un millón.

1993:

- Comienza a transmitir Internet Radio Talk.
- Las Naciones Unidas y el Banco Mundial están en línea.
- WWW prolifera tasas de crecimiento del 341 %
- El crecimiento de Gopher es del 997 %

A principios de 1994 comenzó a darse un crecimiento explosivo de las compañías con propósitos comerciales en Internet dando así origen a una nueva etapa en el desarrollo de la red.

Surgen los centros comerciales de Internet.

1995:
• Los sistemas tradicionales de acceso a la información vía telefónica (Compuserve, Prodigy, America On Line) comienzan a proporcionar acceso a Internet.
• El registro de dominios deja de ser gratuito.
• Espectacular aumento de nodos en Internet: 4.000.000 de nodos y 40.000.000 de usuarios.

1997: 8.000.000 de nodos y 80.000.000 de usuarios.

Internet en España

1985: Proyecto IRIS (Interconexión de Recursos Informáticos) bajo la gestión de Fundesco (Fundación para el Desarrollo de la Función Social de Comunicaciones) y con fondos del Ministerio de Educación y Ciencia.

Es una red destinada a la interconexión entre Universidades y Centros de Investigación españoles, siendo su primer servicio el correo electrónico.

A partir de los 90 se ofrece conexión a Internet por proveedores (organismos que hacen posible el acceso a Internet), tales como Goya Servicios Telemáticos, SareNet y Servicom.

1993: Utilización de todos los servicios de Internet.

¿Qué es un navegador?

Para poder acceder al World Wide Web es necesario emplear un programa cliente de este servicio.
A estos clientes se les suele denominar "browsers" o "navegadores", ya que al movernos de un servidor Web a otro es como si estuviésemos "navegando" por la red.

Los navegadores han sido fundamentales para la popularización de Internet, principalmente debido a su facilidad de manejo para usuarios no expertos en informática y que permiten capturar cualquier documento de Internet, independientemente de su localización y formato y presentarlo al usuario.

Gracias a esto no es necesario seguir los complicados pasos que requerían el conocimiento del sistema Unix para poder realizar, por ejemplo, la transferencia de un archivo por ftp.

Los navegadores ofrecen un interfaz gráfico que permite navegar por la red simplemente usando el ratón en un soporte multimedia, para poder realizar cualquier tipo de búsquedas y encontrar lo que deseamos.

Básicamente, los navegadores son visualizadores de documentos escritos en lenguaje HTML, los cuales pueden incluir texto, gráficos, sonidos, enlaces (links) a otros documentos o servidores Web.

¿Cuáles son los navegadores mas conocidos?


INTERNET EXPLORER


NETSCAPE NAVIGATOR

Los navegadores más conocidos en la actualidad son el **Netscape Navigator** y el **Microsoft Internet Explorer**.

La historia de estos dos navegadores ha estado siempre ligada a constantes enfrentamientos entre ambas empresas.

Netscape en un principio supo ver mejor las posibilidades de negocio que ofrecía Internet y rápidamente se posicionó como el navegador estándar de Internet, acaparando la mayor parte del mercado.

Microsoft, en cambio, tardó más tiempo en reaccionar, pero poco a poco y valiéndose de sus mayores medios y su posición privilegiada debido a su total dominio del mercado de los sistemas operativos domésticos con el controvertido Windows 95 y todos sus derivados consiguió ponerse a la cabeza en la lucha de los navegadores o también llamados browsers..

¿Qué es un buscador?

Un buscador es una página de Internet en la que nosotros podemos entrar y buscar todo tipo de información. Pero no nos equivoquemos, realmente la información que nosotros encontramos al realizar búsquedas en este tipo de páginas no reside en la pagina del buscador. (Salvo casos excepcionales, en los que el buscador pretenda encontrar palabras o artículos alojados en la misma página en la que nos encontramos. Como sucede en esta misma página web).

La función del buscador consiste en, según la información introducida para la consulta comparar con sus listas indexadas y comprobar cuantas páginas conoce en las que se trate dicho tema. Tras la consulta, mostrará al usuario todas aquellas coincidencias que haya encontrado, y así nosotros podremos acceder a todas ellas

¿Cómo podemos hacer una búsqueda?

Para hacer una búsqueda en cualquiera de los buscadores existentes en Internet, simplemente tendremos que acceder a la página en la que resida el buscador y escribir en el cuadro de texto que aparecerá en dicha página que es lo que queremos buscar.

Aquí te mostramos una pequeña muestra de una búsqueda directa con Yahoo España:

[Yahoo! España] opciones

Otra opción ofrecida en muchos buscadores es la de acceder a una lista de informaciones clasificada por temas, usando una estructura jerárquica en forma de directorios donde, con estructura de árbol, se irán agrupando todas las materias de un tema en común.

Ésta se trata más bien de una búsqueda selectiva, en la que iremos encontrando la información clasificada de un modo mucho más preciso, según vayamos pulsando en los diferentes enlaces.

El peligro de este sistema radica en que si no tenemos muy claro lo que buscamos, podemos perdernos, encontrar algo que nos llame la atención y terminar en un sitio al que no nos habíamos propuesto llegar.

Aquí te mostramos una pequeña muestra de una búsqueda selectiva con Yahoo España:

Arte y cultura

Literatura, Teatro, Museos...

Ciencia y tecnología

Animales, Informática, Ingeniería...

Internet y ordenadores

WWW, Aplicaciones, Revistas...

Materiales de consulta

Bibliotecas, Diccionarios...

Búsquedas avanzadas

Siempre se dice que en Internet se puede encontrar de todo. Pero ahí radica también su mayor inconveniente; debido a la enorme cantidad de información y el crecimiento espectacular que está sufriendo, es difícil, sin ayuda, encontrar algo sobre un tema concreto.

Para facilitar la labor de búsqueda, se ha desarrollado un tipo de programas que funcionan por todo el mundo y a los que se accede como a un servidor Web más: son los buscadores.

Los buscadores se nos presentan como páginas de Web y tienen, principalmente, dos formas de trabajar bien diferenciadas:

En la primera, nos encontramos ante una pantalla donde introduciremos las palabras claves relacionadas con el tema que nos interese, después elegiremos el tipo de búsqueda (un AND lógico de las palabras introducidas, un OR, etc.) y para finalizar pulsaremos en el botón con la palabra "Search" (o algo parecido). En breves instantes (o no tan breves, pues depende de lo saturada que esté la línea y de la velocidad del buscador), aparecerá una lista con varias direcciones y un pequeño resumen sobre lo que podremos encontrar en ellas (lo normal es que aparezcan en grupos de unos 20). Dependiendo de la complejidad del buscador, del algoritmo utilizado y de lo concreta que hayamos hecho la búsqueda, esta lista será más o menos grande. Un ejemplo de este tipo de buscadores es AltaVista, de la compañía Digital.

En la segunda nos encontraremos con un menú clasificado de temas a los que iremos accediendo aproximándonos sucesivamente en nuestra búsqueda.

Otra clase de búsqueda

Además de estos buscadores cuyo cometido, básicamente, es buscar términos en páginas web, también existen otros buscadores que sirven para buscar direcciones de e-mail (no siempre encuentran) y para buscar en artículos pasados y presentes de las news, cosas bastante interesantes, ya que dichos mensajes tienen un tiempo de consulta relativamente corto, sobre todo si son grupos con mucho movimiento.

Independientemente de la forma de presentar la información, la eficacia de los buscadores no sólo dependerán de la cantidad de datos (del tamaño de su base de datos) sino también del método que empleen para organizar la información y realizar la búsqueda. Existen multitud de buscadores, pero de entre ellos destacan los siguientes:

Buscadores más conocidos

Aquí tienes una lista de los buscadores, de los muchos que podéis encontrar en la Red. En los que he considerado más usuales le he acompañado de un cometario. Si quieres acceder a cualquiera e ellos, sólo tienes que pulsar en el nombre junto al icono de cada uno de ellos.

(www.altavista.com)

Es uno de los clásicos de Internet. Tiene una de las bases de datos más extensas y precisas. Puedes encontrar prácticamente cualquier cosa que busques.

Anaci (www.uk.com)

(http://www.netfind.aol.com/aolcom/webhome)

(http://www.auyantepui.com/)

(www.astalavista.box.sk)

A pesar de no ser un buscador tradicional, no podíamos dejar de lado a uno de los buscadores más usados en la actualidad para encontrar cracks de programas. Porque queramos o no la piratería tiene un hueco grande en la sociedad actual y por tanto también en Internet.

(www.astalavista.com)

Similar a la anterior

(www.buydomains.com)

(www.euroseek.com)

Buscador europeo con el que puedes encontrar muchas cosas. De creación mas o menos reciente te permite buscar cosas en cualquier idioma europeo que te puedas imaginar. Desde el croata al estonio, pasando por cualquier idioma imaginable, incluido el esperanto. Una opción muy recomendable.

(www.excite.com)

Este es otro de los clásicos que se encuentran en Internet casi desde su comienzo. Es un buscador americano que por tanto tiene muy buenos resultados a nivel mundial, pero que no resulta recomendable si lo que buscamos son cosas relacionadas con nuestro país.

(www.excite.es)

Versión en castellano del buscador Excite que soluciona en parte los problemas del anterior para encontrar en castellano. Bastante completo.

(www.fantastico.com)

(www.galaxy.com)

(www.google.es)

Buscador muy interesante y posiblemente el mas popular. Podemos encontrar cosas que no se encuentran habitualmente. En las búsquedas precisas resulta muy efectivo, encontrando muchas de las cosas que le pedimos. Uno de los mejores que puedes encontrar.

(www.go.com)

(http://goto.myway.com)

(www.grippo.com.ar)

(www.hispavista.com)

HOTBOT (www.hotbot.com)

Es uno de los mejores. Pertenece a Lycos y resulta muy recomendable. Especialmente en la búsqueda de MP3s. Es capaz de encontrar cualquier artista, canción o discografía que encontremos. Tras encontrarlo, nos clasifica los resultados, por ejemplo en el caso de la música, nos lo clasificará por MP3s, discografías, páginas relacionadas, ... Es uno de los más completos.

(www.iguana.com.mx)

(www.infocentro.com.mx)

inforseek.com (www.inforseek.com)

(www.jayde.com)

(www1.lanic.utexas.edu)

(www.lycos.es)

También pertenece al grupo de los clásicos. En un principio no tenía gran parte del mercado, pero con el tiempo ha ido colocándose en una gran posición gracias a la mejora de sus servidores y a buscadores filiales como HOTBOT.

(www.mexmaster.com)

(www.ondeir.rec.br)

(www.ozu.com)

rutaazul.com (www.rutaazul.com)

(www.sol.es)

TELEPOLIS vive Internet (www.telepolis.com)

terra (www.terra.es)

Página de Telefónica que surgió de la unión de diferentes buscadores clásicos en castellano, como fueron Olé, Ozú, etc.

Actualmente tiene muchos servicios a parte de los de buscador de información. Entre ellos están el envío de mensajes a móviles gratuito, el acceso gratuito a Internet a través del proveedor Terra o el servicio de correo electrónico gratuito. Una página muy completa, que no debes dejar de visitar.


TROVATOR www.trovator.com (http://trovator.com)

ukindex (www.ukindex.co.uk)

wanadoo (www.wanadoo.es)

WebCrawler® **WEB CRAWLER** (www.webcrawler.com)

Con éxito en Estados Unidos, pero con poca aceptación en España. Muy bueno para las búsquedas allí, pero poco completo para usarlo aquí.

WebFe.com (www.webfe.com)

(www.whatuseek.com)

(www.ya.com)

YAHOO! (www.yahoo.com)

¿Qué se puede decir de este buscador? Pues simplemente que es el buscador por excelencia en Internet. A pesar de que su diseño sigue siendo algo anticuado (conserva el diseño original, huyendo de elementos gráficos atractivos). Sigue teniendo muchísima información en sus servidores, gracias a los muchos años de experiencia con los que cuenta. Además proporciona correo gratuito a sus usuarios

YAHOO! ESPAÑA (es.yahoo.com)

Versión en castellano del famoso buscador Yahoo!.

(www.ysi.com/index.html)

(www.yuada.com)

El dominio:

El dominio es el indicador que manifiesta la propiedad o pertenencia de la Web a la que accedemos y viene representada pos los caracteres que siguen al ultimo punto del nombre.

Por organización

Algunos nombres de dominio:

www.pepe.adv	Abogados
www.pepe.aero	Industria aeronáutica
www.pepe.am	Empresas de radiodifusión
www.pepe.art	Artes: música, pintura, folclore
www.pepe.biz	Negocios
www.pepe.br	Buscadores
www.pepe.com	Comerciales en general
www.pepe.com	Común
www.pepe.edu	Entidades educativas
www.pepe.esp	Deportes
www.pepe.eti	Especialistas en tecnología de la información
www.pepe.fm	Empresas de radiodifusión
www.pepe.g12	Entidades de enseñanza primaria y secundaria
www.pepe.gov	Gobierno
www.pepe.ind	Industrias
www.pepe.info	Medios de información
www.pepe.int	Organizaciones internacionales
www.pepe.mil	Militares
www.pepe.museum	Museos
www.pepe.name	Personas individuales
www.pepe.net	Proveedores de comunicaciones
www.pepe.org	Organización (generalmente asistencial, no lucrativas)
www.pepe.pro	Organizaciones profesionales
www.pepe.psi	Proveedores de acceso a Internet
www.pepe.rec	Entretenimiento / Recreativos
www.pepe.tmp	Eventos
www.pepe.tur	Turismo
www.pepe.tv	Televisión
www.pepe.vet	Veterinarios

Países:

Por país

.

Español	Dominio	English
Andorra	ad	Andorra
Emiratos Árabes Unidos	ae	United Arab Emirates
Afganistán	af	Afghanistan
Antigua y Barbuda	ag	Antigua and Barbuda
Anguila	ai	Anguilla
Albania	al	Albania
Armenia	am	Armenia
Antillas Holandesas	an	Netherlands Antilles
Angola	ao	Angola
Antártida	aq	Antarctica
Argentina	ar	Argentina
Arpanet (antiguo)	arpa	Arpanet (Old style)
Samoa americana	as	American Samoa
Austria	at	Austria
Australia	au	Australia
Aruba	aw	Aruba
Azerbaiyán	az	Azerbaidjan
Bosnia-Herzegovina	ba	Bosnia-Herzegovina
Barbados	bb	Barbados
Bangladesh	bd	Bangladesh
Bélgica	be	Belgium
Burkina Faso	bf	Burkina Faso
Bulgaria	bg	Bulgaria
Bahrain	bh	Bahrain
Burundi	bi	Burundi
Benin	bj	Benin
Bermudas	bm	Bermuda
Brunei Darussalam	bn	Brunei Darussalam
Bolivia	bo	Bolivia
Brasil	br	Brazil
Bahamas	bs	Bahamas
Bután	bt	Bhutan
Isla Bouvet	bv	Bouvet Island

Botswana	bw	Botswana
Bielorusia	by	Belarus
Belice	bz	Belize
Canadá	ca	Canada
Islas Cocos (Keeling)	cc	Cocos Islands (Keeling)
República Centro Africana	cf	Central African Republic
Congo	cg	Congo
Suiza	ch	Switzerland
Costa de Marfil	ci	Ivory Coast
Islas Cook	ck	Cook Islands
Chile	cl	Chile
Camerún	cm	Cameroon
China	cn	China
Colombia	co	Colombia
Comercial (EE.UU.)	com	Commercial (mainly USA)
Costa Rica	cr	Costa Rica
Antigua Checoslovaquia	cs	Former Czechoslovakia
Cuba	cu	Cuba
Cabo Verde	cv	Cape Verde
Isla Christmas	cx	Christmas Island
Chipre	cy	Cyprus
República Checa	cz	Czech Republic
Alemania	de	Germany
Yibouti	dj	Djibouti
Dinamarca	dk	Denmark
Dominica	dm	Dominica
República Dominicana	do	Dominican Republic
Argelia	dz	Algeria
Ecuador	ec	Ecuador
Educacion (EE.UU)	edu	Educational (USA)
Estonia	ee	Estonia
Egipto	eg	Egypt
Sáhara Occidental	eh	Western Sahara
España	es	Spain
Etiopía	et	Ethiopia
Finlandia	fi	Finland
Fiyi	fj	Fidji
Islas Malvinas	fk	Falkland Islands

Micronesia	fm	Micronesia
Islas Faroe	fo	Faroe Islands
Francia	fr	France
Francia (Territorio europeo)	fx	France (European Territory)
Gabón	ga	Gabon
Gran Bretaña	gb	Great Britain
Granada	gd	Grenada
Georgia	ge	Georgia
Guayana Francesa	gf	French Guyana
Ghana	gh	Ghana
Gibraltar	gi	Gibraltar
Groenlandia	gl	Greenland
Gambia	gm	Gambia
Guinea	gn	Guinea
Estado (EE.UU)	gov	Government (USA)
Guadalupe (Francia)	gp	Guadeloupe (France)
Guinea Ecuatorial	gq	Equatorial Guinea
Grecia	gr	Greece
Islas S. Georgia y S. Sandwich	gs	S. Georgia & S. Sandwich Islands
Guatemala	gt	Guatemala
Guam (EE.UU)	gu	Guam (USA)
Guinea Bissau	gw	Guinea Bissau
Guayana	gy	Guyana
Hong Kong	hk	Hong Kong
Islas Heard y McDonald	hm	Heard & McDonald Islands
Honduras	hn	Honduras
Croacia	hr	Croatia
Haití	ht	Haiti
Hungría	hu	Hungary
Indonesia	id	Indonesia
Irlanda	ie	Ireland
Israel	il	Israel
India	in	India
Internacional	int	International
Territorios británicos en el Océano Indico	io	British Indian Ocean Territory
Irak	iq	Iraq
Irán	ir	Iran
Islandia	is	Iceland

Italia	it	Italy
Jamaica	jm	Jamaica
Jordania	jo	Jordan
Japón	jp	Japan
Kenia	ke	Kenya
Kirgistán	kg	Kyrgyzstan
Camboya	kh	Cambodia
Kiribati	ki	Kiribati
Comores	km	Comoros
Saint Kitts y Nevis Anguila	kn	Saint Kitts & Nevis Anguilla
Corea del Norte	kp	North Korea
Corea del Sur	kr	South Korea
Kuwait	kw	Kuwait
Islas Caimán	ky	Cayman Islands
Kazastán	kz	Kazakhstan
Laos	la	Laos
Líbano	lb	Lebanon
Saint Lucia	lc	Saint Lucia
Liechtenstein	li	Liechtenstein
Sri Lanka	lk	Sri Lanka
Liberia	lr	Liberia
Lesoto	ls	Lesotho
Lituania	lt	Lithuania
Luxemburgo	lu	Luxembourg
Letonia	lv	Latvia
Libia	ly	Lybia
Marruecos	ma	Morocco
Mónaco	mc	Monaco
Moldavia	md	Moldavia
Madagascar	mg	Madagascar
Islas Marshall	mh	Marshall Islands
Militar (EE.UU)	mil	Military (USA)
Macedonia	mk	Macedonia
Mali	ml	Mali
Myanmar (Birmania)	mm	Myanmar (Burma)
Mongolia	mn	Mongolia
Macao(std LE)	mo	Macau
Islas Marianas del Norte	mp	Northern Mariana Islands

Martinica (Francia)	mq	Martinique (France)
Mauritania	mr	Mauritania
Monserrat	ms	Monserrat
Malta	mt	Malta
Mauricio	mu	Mauritius
Maldivas	mv	Maldives
Malawi	mw	Malawi
Méjico	mx	Mexico
Malasia	my	Malaysia
Mozambique	mz	Mozambique
Namibia	na	Namibia
Nueva Caledonia (Francia)	nc	New Caledonia
OTAN	nato	NATO
Niger	ne	Niger
Red	net	Network
Isla Norfolk	nf	Norfolk Island
Nigeria	ng	Nigeria
Nicaragua	ni	Nicaragua
Holanda	nl	Netherlands
Noruega	no	Norway
Nepal	np	Nepal
Nauru	nr	Nauru
Zona neutral	nt	Neutral Zone
Niue	nu	Niue
Nueva Zelanda	nz	New Zealand
Omán	om	Oman
Organizaciones benéficas	org	Non-Profit Making Organisations
Panamá	pa	Panama
Perú	pe	Peru
Polinesia (Francia)	pf	Polynesia (France)
Papúa Nueva Guinea	pg	Papua New Guinea
Filipinas	ph	Philippines
Pakistán	pk	Pakistan
Polonia(std LE)	pl	Poland
Saint Pierre y Miquelon	pm	Saint Pierre & Miquelon
Isla Pitcairn	pn	Pitcairn Island
Puerto Rico	pr	Puerto Rico
Portugal	pt	Portugal

Palao	pw	Palau
Paraguay	py	Paraguay
Qatar	qa	Qatar
Reunión (Francia)	re	Reunion (France)
Rumanía	ro	Rumania
Federación Rusa	ru	Russian Federation
Ruanda	rw	Rwanda
Arabia Saudí	sa	Saudi Arabia
Islas Salomón	sb	Solomon Islands
Seychelles	sc	Seychelles
Sudán	sd	Sudan
Suecia	se	Sweden
Singapur	sg	Singapore
Santa Elena	sh	Saint Helena
Eslovenia	si	Slovenia
Islas Svalbard y Jan Mayen	sj	Svalbard and Jan Mayen Island
Republica Eslovaca	sk	Slovak Republic
Sierra Leona	sl	Sierra Leone
San Marino	sm	San Marino
Senegal	sn	Senegal
Somalia	so	Somalia
Surinam	sr	Surinam
Saint Tomé y Príncipe	st	Saint Tome & Principe
Antigua URSS	su	Former USSR
El Salvador	sv	El Salvador
Siria	sy	Syria
Suazilandia	sz	Swaziland
Islas Turks y Caicos	tc	Turks & Caicos Islands
Chad	td	Chad
Territorios Franceses del Sur	tf	French Southern Territories
Togo	tg	Togo
Tailandia	th	Thailand
Tayiquistán	tj	Tadjikistan
Tokelau	tk	Tokelau
Turquestán	tm	Turkmenistan
Túnez	tn	Tunisia
Tonga	to	Tonga
Timor Oriental	tp	East Timor

Turquía	tr	Turkey
Trinidad y Tobago	tt	Trinidad & Tobago
Tuvalu	tv	Tuvalu
Taiwán	tw	Taiwan
Tanzania	tz	Tanzania
Ucrania	ua	Ukraine
Uganda	ug	Uganda
Reino Unido	uk	United Kingdom
Minor Outlying Islands (EE.UU.)	um	Minor Outlying Islands (USA)
Estados Unidos de América	us	United States of America
Uruguay	uy	Uruguay
Uzbekistán	uz	Uzbekistan
Ciudad del Vaticano	va	Vatican City
Saint Vincent y Grenadines	vc	Saint Vincent & Grenadines
Venezuela	ve	Venezuela
Islas Vírgenes (Reino Unido)	vg	Virgin Islands (Britain)
Islas Vírgenes (EE.UU)	vi	Virgin Islands (USA)
Vietnam	vn	Vietnam
Vanuatu	vu	Vanuatu
Islas Wallis y Futuna	wf	Wallis & Futuna Islands
Samoa	ws	Samoa
Yemen	ye	Yemen
Mayotte	yt	Mayotte
Yugoslavia	yu	Yugoslavia
Sudáfrica	za	South Africa
Zambia	zm	Zambia
Zaire	zr	Zaire
Zimbabwe	zw	Zimbabwe

¿Como buscar?

Es conveniente leer en el icono de ayuda de cada buscador para informarnos de las herramientas de búsqueda que posee, a menudo nos encontraremos con herramientas específicas en un determinado programa de búsqueda. De forma casi genérica estas herramientas, conceptos o argumento son:

- Las palabras que utilizamos como argumento de búsqueda siempre tienen que ir separadas por un espacio. Adicionalmente podemos añadir algunos signos que servirán como incluyentes o excluyentes de otras palabras, también podemos usar los signos para buscar textos concretos.
- Si hay únicamente espacio entre palabras indica "o". La primera palabra o la segunda o la tercera, etc.
- **+** Las palabras que van precedida por este signo indican: además de. La primera palabra y la segunda y la tercera, etc.
- **-** Las palabras que van precedidas por este signo son excluyentes. Las palabras buscadas menos la primera palabra, menos la segunda palabra, etc.
- **" "** Indica que buscara por el texto incluido ente las comillas escrito de la misma forma y orden en el que nosotros lo hemos indicado.
- ***** Sirve para completar palabras. Ejemplo: podemos poner la palabra *cine* como argumento de búsqueda y nos encontrara un determinado número de lugares en la red que contengan esta palabra. Pro si ponemos *cine** buscara por todas aquellas que comienzan por cine ... y encontrara palabras como cinéfilo, cinematógrafo, cineasta, etc.
- **site:** Algunas palabras, cuando se anexan con dos puntos, tienen un significado especial para Google. Una de esas palabras es el operador "site:". Para buscar en un sitio o dominio específico, use la sintaxis *site:ejemplodedominio.com*, o también puede buscar por *articulo site: www.google.com*
- **Mayúsculas – Minúsculas:** Utilice solamente minúsculas, salvo si usted desea efectuar una búsqueda que contenga dicho caso. Si usted busca la palabra **Café**, no encontrará mas que los sitios que contienen esta palabra escrita con la mayúscula inicial. Si usted busca **café** usted encontrará las páginas donde esta palabra esté escrita es decir: café, **CAFÉ**, así como todas las combinaciones posibles de mayúsculas y minúsculas.
- Prácticamente, son pocos los buscadores que tiene en cuenta los diferentes signos de acentuación.
- Todos los buscadores disponen de un icono denominado "Búsqueda Avanzada", esto nos permitirá ser aun más selectivo en nuestra búsqueda y seleccionar por idiomas, país, fecha etc.

Ejemplos:

Tenemos intención de hacer una remodelación en nuestra casa en la que procederemos, entre otras muchas cosas, al cambio de todas las ventanas. Hace tiempo que un amigo de la familia nos comento de un fabricante que las hacia bien y baratas, pero no recordamos el nombre así que lo intentaremos buscar en Internet.

Primero llamaremos a un programa buscador, por ejemplo el www.google.es y como argumento de búsqueda pondremos separadas por un **espacio**:

fabricante puertas

El programa nos responderá posiblemente que ha encontrado 35.900 webs con este argumento. Lo que hemos hecho ha sido realizar una búsqueda diciendo que nos identificara todo aquel lugar que tuviese la palabra "fabricante" **o** "puertas". Con el fin de hacerlo mas selectivo le incluiremos el signo **+**:

+fabricante +puertas

En este caso el argumento de búsqueda ha sido que contengan las palabras "fabricante" **y** "puertas". La respuesta será de 14.600 lugares encontrados, como nuestra intención es poner ventanas de madera, intentaremos eliminar otros tipos de materiales, para lo cual incluiremos el signo **-**:

+fabricante +puertas –hierro –aluminio

Con este argumento le hemos indicado que **no seleccione** determinadas palabras. La respuesta es de 9.670 lugares encontrados. Como todavía son muchos y nos hemos dado cuenta que entre las seleccionadas hay fabricantes de Sudamérica intentaremos eliminarlos de nuestra búsqueda:

+fabricante +puertas –hierro –aluminio +españa

Se ha utilizado un signo incluyente para excluir a todas aquellas webs que no lo contengan. La respuesta será de 3.460 páginas encontradas. Mientras estábamos escribiendo nos ha venido a la memoria que nuestro amigo nos comento que creía que la fabrica estaba en Valencia. Así que la incluiremos como otros argumento de búsqueda con el fin de hacer esta mas selectiva:

+fabricante +puertas –hierro –aluminio +españa +valencia

Ahora, el numero de lugares encontrados es de 108

+fabricante +puertas –hierro –aluminio +españa +valencia +"pobla de vallbona"

Resultado es de 5 lugares donde consultar. En este caso ya nos resulta fácil encontrar aquello por lo que se inicio la búsqueda.

Correo Electrónico

El “Correo Electrónico”, “Correo-e” o “e-mail” es uno de los servicios más populares de Internet.

Te permite acceder a tu cuenta de correo o buzón desde cualquier lugar u ordenador conectado a Internet. Desde un cibercafé, una biblioteca, el trabajo o tú casa. Tu dirección de correo es la misma y podrás acceder a tu cuenta fácilmente, estés donde estés. Además, generalmente una cuenta de correo se puedes utilizar para comprobar otras cuentas de correo que tengas.

Una vez conseguida tu dirección de correo, esta es permanente. Podrás mantener tu cuenta de Correo el tiempo que desees y en función de los términos y condiciones aceptados. Tu dirección será la misma aún cuando cambies de ciudad o país, cambies de proveedor de acceso a Internet. Puedes tener una dirección de correo permanente para el resto de tu vida.

Generalmente la cuenta de correo viene acompañada de útiles herramientas, que pueden incluir:

- Espacio de almacenamiento gratuito en el disco del servidos
- Programa de guardia o protección, suele estar diseñado para reducir radicalmente la cantidad de mensajes no solicitados que recibes diariamente en tu buzón, y de esta forma enviar la mayoría de estos mensajes a la carpeta de lotes de correo para ayudarte a administrar mejor tu correo.
- Acceso a otras cuentas de correo. Puedes configurar tu cuenta de correo para recuperar mensajes de otras cuentas de correo de las que disponen de acceso POP. Una cuenta con acceso POP es aquella a la que puedes acceder con un programa de correo estándar, como Outlook, Eudora o Netscape.
- Bloquear direcciones. Con esta herramienta puedes bloquear un buen número de direcciones de correo. Resultará muy útil si no paras de recibir correo publicitario o molesto de las mismas direcciones. Es más, los mensajes de estas direcciones se eliminarán automáticamente. Después de introducir y guardar las direcciones que quieres bloquear, no tendrás que hacer nada más.

- Respuestas automáticas: Si te vas de vacaciones o vas a estar ausente cierto tiempo, puedes programar el envío de mensajes automáticos a todos los que te escriban durante este periodo. Funciona igual que un contestador de teléfono. Cuando alguien te escribe y estás fuera, se le enviará un mensaje que tú mismo redactas, por ejemplo, notificándole cuánto tiempo estarás fuera o con quién debe hablar mientras no estés.
- Personalización de tus preferencias. Con esta herramienta, como usuario de correo podrás personalizar cómo se visualiza el correo en tu bandeja de entrada, si deseas ver el encabezado completo o breve de los mensajes entrantes.

Servidores de Correo Electrónico

Hay multitud de Web's que ofrecen servicios gratuitos de correo con una capacidad de almacenamiento que oscila entre los 3 y 10 Mb., adicionalmente algunas de estas compañías ofrecen mayor capacidad bajo previo, con precios razonables. La capacidad del disco virtual que ofrecen es la que disponemos para almacenar nuestro correo, tanto entrante como saliente (notas recibidas o enviadas), si nuestro deseo es almacenar las notas durante un periodo de tiempo o si recibimos ficheros con fotografías, es muy probable que saturemos su capacidad en un periodo corto de tiempo.

Esta es la razón por la que es aconsejable el instalar un gestor de correo en nuestro PC (ejemplo: el Outlook). La función básica que realiza el gestor es la de mover todo el correo que recibamos, desde el disco virtual que disponemos en nuestro servidor (ejemplo: Terra o hotline) hasta nuestro disco duro del nuestro PC. De la misma forma nos gestionara nuestras notas enviadas y las copias que conservemos las almacenara en el disco duro de nuestro PC y no en el virtual de nuestro servidor.

¿Quién Ofrece Servidores de Correo Gratuito?

Además de algunas empresas privadas que ofrecen este servicio gratuito para sus empleados o clientes (ejemplo; algunos bancos). En cada país hay multitud de Web's que lo ofrecen. En España, entre otras, las mas conocidas son:

terra www.terra.es

www.ya.com

www,yahoo.es

www.hotmail.com

www.qdq.com

www.tiscali.es

www.wanadoo.es

¿Con Quién Contratamos un Servicio de Conexión de Internet?

Básicamente con cualquier operadora de telefonía, algunas de ellas están ya representadas en el párrafo anterior, al que habría que añadir la compañía que domina el mercado español y gran parte del continente americano:

Algunas de estas compañías también ofrecen números de teléfonos a los cuales se puede llamar para conectarse a Internet sin contrato previo, pero tiene el inconveniente que en este caso se paga la llamada, lo cual, generalmente resulta mas caro.

¿Qué Tipo de Servicio se debe Contratar?

Esta es, posiblemente, una de las preguntas mas personales y mas difícil de contestar de una forma genérica. Cada uno de nosotros es un caso diferente y por tanto cada uno debemos de analizar nuestras necesidades, condiciones y circunstancias.

De esta forma nos podemos encontrar, entre otras, con una de las siguientes opciones:

- Una línea telefónica compartida para Internet y para llamadas, tiene el problema de no poder realizar los dos servicios simultáneamente, o se esta

conectado a Internet o se esta hablando por teléfono. Dependiendo de la compañía, los servicios que se pueden contratar serian:
    - Por bloques de horas
    - Tarifa plana en segmentos horarios
    - Tarifa plana 24 horas
- Dos líneas telefónicas. Una dedicada a llamadas y la otra para llamadas y conexión a Internet. Esta opción no presenta las limitaciones del caso anterior y las posibilidades de contratación son las mismas ya descritas en el párrafo anterior.
- Una línea ADSL que nos permitirá hablar por teléfono y poder estar conectado a Internet. Esta opción tiene la ventaja de la simultaneidad y la velocidad de transmisión, también es la opción posiblemente más cara. Al igual que se ha descrito en el primer párrafo, nos encontraremos con diferentes servicios y precios,
- Otra posibilidad es la contratación de una línea RDSI, pero parece ser que actualmente ha caído en desuso.

A la vista de lo descrito es evidente que cada uno optara por la que mejor le convenga en función de sus necesidades. No tiene nada que ver aquella persona que dedica unos minutos a la semana para despachas unas pocas notas o cartas con aquellos que se pasan el día entero “chatenado” en diferentes foros, consultando todo tipo de información en la Red o con aquellos que casi permanentemente están conectados, bajándose música o películas de video.

¿Cómo registrarse?

Se ha tomado como ejemplo el documento de inscripción de la Web de Yahoo, esto no quiere decir que sea la mas fácil ni la recomendada, cada uno elegirá la que mejor le convenga o la misma con la que ha contratado el servicio de conexión a la RED. Antes de inscribirse en una Web de Correo Electrónico es conveniente hacer un repaso por cada una de ellas (o consultar a nuestros amigos o hijos), para ver que facilidades u opciones nos ofrecen; de esta forma es conveniente valorar la capacidad de disco que nos dan, la posibilidad de antivirus, antispan, agendas, directorios, etc. Primero hay que leer un amplio documento en el que se estipula los términos y condiciones bajo los cuales queda fijado el uso de la cuenta de correo. Es conveniente imprimirlo para su mejor lectura y comprensión.

Ejemplo de formulario:

ID de Yahoo!: [ ] **@ yahoo.es**

(ejemplos: **pepito_grillo** o **webosfritos**)

Contraseña: [ ]

Reintroducir contraseña: [ ]

Elige tu ID
Utilizarás esta ID cada vez que accedas a Yahoo! **Atención**: ¡Distinguimos entre mayúsculas y minúsculas!

Si olvidas tu contraseña o necesitas ayuda del equipo de atención al cliente, necesitarás confirmar la siguiente información:

Pregunta de seguridad: [ ]

Tu respuesta: [ ]

Cumpleaños: [ ] [ ] [ ] (Día, mes, año)

Correo-e actual (opcional): [ ]

Avisos de cambio en la cuenta serán enviados a esta dirección, **incluyendo pedidos de nueva contraseña**.

Contraseña y correo alternativo
Esta información es la única forma de verificar tu identidad. Para proteger tu cuenta, asegúrate de que "Tu respuesta" es **recordable para tí** pero **difícil de adivinar para otras personas**.

Nombre: [ ] Apellidos: [ ]

País: [España]

Personalizar Yahoo!
Yahoo! te ofrecerá el contenido y publicidad más

Cód. Postal: Sexo:

Sector: [Elige el sector]

Título: [Elige uno]

Especialización: [Elige la especialización]

Directorio de busca tu gente: Incluir mi nueva dirección de Correo Yahoo! gratuitamente

El directorio muestra el nombre real, la ciudad, la provincia y el país.

publicidad más relevantes según la información que indicas en esta página y los productos y servicios de Yahoo! que utilizas.

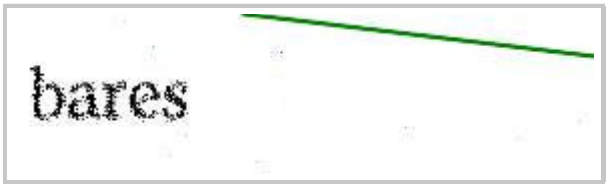
Entrad en contacto conmigo de forma ocasional para informarme de ofertas, promociones, servicios y/o productos de Yahoo! y/o de terceros.

Sondeos de HI Europe: Deseo recibir más información sobre cómo apuntarme al panel "Hi Europe Opinion Poll" (Ofrecido por Harris International) y tener la posibilidad de ser premiado al participar en encuestas diversas.

Intereses (opcional):

Ocio	Negocios e inversiones	Compras
Hogar y familia	Ordenadores y tecnología	Deportes y actividades al aire libre
Salud	Finanzas personales	Viajes
Música	Pymes	Sorteos y promociones

Introduce la palabra que aparece en la imagen en este campo:



Verificación de palabra
Este paso nos ayuda a impedir registros automáticos.

Si no puedes ver la imagen, por favor, haz clic aquí.

Enviar

El Chat

¿Qué es el chat?

El chat ("charla" en inglés) consiste en una tecnología que permite mantener una conversación en tiempo real con otras personas que también estén conectadas al mismo servidor o web que nosotros. Gracias al teclado y al monitor podrás conocer gente nueva y comunicarte con tus amigos a través de la web.
Normas en el chat

Normas de uso

- *Al entrar y salir del chat.*
  Se considera una falta de educación el llegar a un sitio nuevo y no saludar, no sólo en el chat sino en la vida real, así que es más que recomendable ser educado y cortés al comenzar y finalizar la charla.
- *Normas básicas de comportamiento.*
  Es un standard en los chats que escribir en mayúsculas equivale a gritar. No abuses de las mayúsculas salvo para casos muy concretos, el resto de la gente te lo agradecerá.
  No acosar, violentar, amenazar o causar molestias a cualquier otro usuario o a un tercero.
  No enviar a través del chat ninguna información, datos, textos, enlaces, comunicados o cualquier otro material considerado ilegal, perjudicial, amenazador, abusivo, hostil, difamatorio, obsceno; racial o éticamente incorrecto, o referencias discriminatorias sobre tendencias sexuales.
- *No es oro todo lo que reluce.*
  Ten en cuenta que lo que dice o afirma un usuario no tiene porque ser cierto. Sé cauto con lo que cuentas, con las informaciones que puedas facilitar y con lo que puedas creer de lo que cuentan otros usuarios.
- *Todos hemos sido principiantes alguna vez.*
  Siempre hay una primera vez para todo, todos hemos sido, alguna vez, principiantes. Por lo tanto, si otro usuario hiciera algo mal, ayúdale, hazle notar su error en una conversación privada y no se te olvide que es muy probable que ese mismo error ya lo haya cometido con anterioridad.

Cómo chatear

El Alias
Lo primero que has de hacer es introducir tu alias, el nombre con el cual te conocerán todas las personas con las que hables. Para elegir tu alias tendrás que tener en cuenta las siguientes reglas:
El alias no podrá tener como primer carácter un número.
Podrás utilizar todas las letras españolas y los números.
Los siguientes caracteres también están permitidos: -[\]^_`{|}~
El número máximo de caracteres permitidos es de nueve.

Además tendrás que tener en cuenta que tu alias es el nombre con el que te van a identificar el resto de usuarios.

Los privados
Si lo que quieres es chatear en privado con un usuario, basta con que pinches sobre el alias de la persona en cuestión y escojas la opción de abrir privado, inmediatamente se abrirá una ventana flotante en la que podrás mantener una conversación privada.

Recursos gráficos
Para hacer más amena la conversación, tanto en el canal general, como en un privado cuentas con diferentes opciones:
Puedes cambiar tantas veces como quieras el color del texto, escribir en negrita o subrayar las frases, introducir "emoticonos", con ellos podrás expresar tu estado de ánimo, sensaciones e impresiones generadas por la dinámica de la charla, también puedes introducir una serie de dibujos. No te olvides de los sonidos, mientras hablas puedes reproducir una serie de sonidos que podrás oír mientras se desarrolla la conversación, para poder deshabilitarlos bastará con pinchar en sonidos, en la barra superior en opciones - sonidos - opción activada ¿Deseas desactivarla?.

Categorías
Son muchas y muy variadas, su clasificación o disponibilidad depende de la web a la que estamos conectados. Un ejemplo puede ser:

- Actualidad Ponte al día de las noticias nacionales e internacionales.
- Alimentación Recetas, trucos, dietas, vinos y mucho más.
- Amigos El rincón de los amigos y las nuevas amistades de la red.
- Cine Noticias, salas, películas, críticas. ¿Y tú que has visto el último fin de semana?
- Coches Habla sobre las últimas novedades en el mercado, 4x4, tunning, coches clásicos...

- Cultura y Ciencia Para mentes inquietas. Arte, libros, eventos culturales y temas científicos.
- Deportes ¿Quieres charlar de fútbol? ¿O de baloncesto?... Hazlo con otros aficionados.
- España Conoce a gente de todos los rincones del país.
- Finanzas Divisas, acciones, brokers, etc. Comparte con otros tus inversiones.
- Joven Habla de tus ídolos y los programas que más te gustan con fanáticos como tú.
- Juegos Para que hables de las últimas novedades, evaluaciones de juegos y...
- Motos Más que una afición, un estilo de vida. Forma parte de él.
- Mujer Sólo para vosotras. Noticias, belleza, padres, pareja, tiempo libre.
- Música Para los fans incondicionales. Habla de los conciertos, festivales o lanzamientos...
- Tecnología Los fanáticos -y no tan fanáticos- de la informática se encuentran aquí.
- Turismo ¿Necesitas algunas buenas ideas para tus próximas vacaciones?

Las web utilizadas en las charlas

¿Como recordar las webs que nos interesan?

Frecuentemente nos encontraremos con la necesidad de volver a utilizar una pagina de una web o continuar trabajando o leyendo donde lo habíamos dejado anteriormente.

De forma genérica, haciendo un “copy” y “paste” de la dirección a un documento.
Si estamos trabajando con el “Explorer”, como navegador, podemos recordarlo utilizando el icono de “Favoritos” y “Agregar ...”
Si estamos utilizando el “Netscape”, podemos recordarlo utilizando el icono de “Bookmarks” y a continuación el “File Bookmark ...”
Recordar que en estos dos últimos casos podéis clasificar las direcciones por carpetas de actividad, origen, destino, etc.

¿Qué Tipo de PC Necesito para Acceder a Internet?

En el supuesto caso que utilizásemos un PC dedicado en exclusiva para conectarnos a Internet y solamente para hacer las consultas habituales, tendríamos suficiente con un procesador de 200 Mhz y una memoria RAM de 120 Mb. Sin embargo la realidad es otra muy diferente pues el uso de programas de antivirus nos obliga a utilizar procesadores mas rápidos y mayores capacidades de memoria. De esta forma, la mínima configuración que debemos de tener para podernos conectar con cierta soltura es de un procesador de 600 Mhz y una memoria de 250 Mb o superior.

¿Qué Sistema Operativo debo de Tener?

Hoy en día el mas extendido a nivel popular es el “Windows” que ofrece unos resultados aceptables para usuarios como nosotros que no utilizamos grandes programas de calculo, diseño grafico, etc. Aunque a comienzos del 2.004, Microsoft ha dejado de dar soporte al Windows 95, debemos de utilizar la versión mas próxima a la fecha de fabricación de nuestro PC, aunque esta sea el W/95, el que deje de tener soporte no significa que deje de funcionar. Lo que si debemos te tener presente, sea cualquiera la versión que tengamos instalada, es que periódicamente tenemos que conectarnos a la Web de Microsoft y actualizar al ultimo nivel nuestra versión de sistema operativo. Esto sin duda necesita de cierta pericia que iremos adquiriendo paulatinamente y sin embargo nos proporcionara la

tranquilidad de corregir todos aquellos fallos con los que apareció, nuestra versión, en el mercado y los que posteriormente se han detectado.

Seguridad

Podríamos hacernos extensos en este capitulo, pero lo mas prudente es ceñirnos a las recomendaciones de Las Fuerzas y Cuerpos de Seguridad del Estado.

Guardia Civil:

Consejos de seguridad para usuarios de Internet (http://www.guardiacivil.org/telematicos/consejos1.htm)

Si para proteger nuestra vivienda invertimos en puertas blindadas o alarmas de seguridad, para proteger nuestra intimidad, invirtamos en medidas de seguridad para nuestros sistemas informáticos.

Actualiza constantemente el sistema operativo y el software instalado. Los sistemas operativos más utilizados así como los programas más utilizados tienen una función configurable de actualización (update) automática.

- Instala un programa cortafuegos o firewall. En la red hay multitud de estas aplicaciones, algunas de ellas gratuitas y de contrastada eficacia. No te preocupe no tener el mejor, preocúpate de tener uno instalado.
- Utiliza un software antivirus. Si adquieres un antivirus no registrado de forma que no se actualiza, resulta inútil pasados unos días. Mensualmente se generan entre 600 y 800 virus. Es preciso que nuestro antivirus esté actualizado.
- No abras mensajes de correo electrónico no solicitados o de procedencia desconocida. Elimínalos directamente sin previsualizarlos. El principal método de propagación de virus es a través del correo electrónico.
- Si recibes mensajes que piden su reenvío a tus conocidos, informando de noticias llamativas o que apelan a tu caridad, desconfía por sistema. Son cadenas “HOAXES” que buscan direcciones de correo electrónico para prospectivas comerciales.
- Uno de los fraudes actuales de mayor incidencia es el de los de acceso a Internet a través de 906. Una gran parte de contenidos para adultos aparentemente gratuitos, requieren la aceptación de condiciones en las que de forma confusa se informa de la activación de una nueva conexión a través de números de tarificación especial (906xxxxxx).Hispasec Sistemas, ha

diseñado y desarrollado un programa gratuito, "CHECKDIALER", que te previene frente a este fraude.
- Utiliza siempre software legal. Evita las descargas de programas de lugares no seguros de Internet.

La adopción de estas medidas no garantiza la seguridad de nuestros sistemas pero reduce en un 90% su vulnerabilidad.

Consejos para el comprador en el Comercio Electrónico:

- Compre preferiblemente en aquellos comercios electrónicos que le inspiran suficiente confianza, bien por la empresa que lo ofrece, por las acreditaciones que tiene o por referencias de amistades. Si tiene dudas realice consultas en buscadores o en webs de asociaciones de defensa o atención al consumidor.
- Desconfíe de precios ridículos, gangas o superofertas que no ofrezcan garantías y estén fuera de la lógica comercial. Nadie regala o pierde dinero al vender. En un mercado de libre competencia los márgenes comerciales no son muy amplios.
- Los portales de subastas o ventas de segunda mano, en los que se produce una relación comercial de cliente a cliente (c2c), son el escenario más frecuente de fraudes al consumidor de comercio electrónico.
- Preferiblemente compre en comercios electrónicos que utilicen servidores seguros (aquellos que empiezan por https://www….).
- Si puede escoger el método de pago, elija contrareembolso o pago con tarjeta de crédito. Rehuya de las transferencias bancarias.
- Conserve todos los justificantes y resguardos hasta que reciba y verifique la mercancía.
- Si en el plazo establecido, no recibe el producto solicitado, y no recibe respuesta del comerciante, acuda rápidamente a su entidad bancaria para anular o rechazar el cargo.
- Si recibe un producto de inferiores características al contratado, exija su inmediata reposición. No lo conserve amparado en falsas promesas de sustitución. Si esta no se produce, denúncielo rápidamente y anule el cargo en su entidad bancaria.
- Si, lamentablemente, Vd. ha sido víctima de un fraude en comercio electrónico, informe de ello en las webs de atención al consumidor o atención al internauta. Su información ayudará a que otros usuarios desconfíen de ese comercio electrónico y no se conviertan en nuevas víctimas.

El comercio electrónico supone un potencial nuevo mercado que ofrece innumerables ventajas. Diariamente se producen miles de operaciones de comercio electrónico y únicamente una parte insignificantes son fraudes. Como en la vida real, allí donde hay posibilidad de engaño, acudirán los estafadores.

Consejos para los "Papas y Abuelos"

La sociedad de la información se caracteriza por el uso de nuevas tecnologías que evolucionan a ritmo de vértigo. No todos los ciudadanos acceden a esas nuevas tecnologías a la misma velocidad ni se adaptan igual. Estadísticamente la juventud se ha adaptado mucho mejor que el resto de la sociedad, por ello, no es extraño ver a padres que saben menos que sus hijos sobre el uso de la informática e Internet, esto no ha de ser obstáculo para educar a nuestros hijos en hábitos de navegación segura y dentro de la ley.

- Internet y la informática ofrecen numerosas ventajas, por ello debemos animar a nuestros hijos en el uso de estas tecnologías, pero no en el abuso. Limite las horas que sus hijos dedican a estar frente al ordenador o conectados a Internet. Procure estar presente cuando su hijo se conecta a Internet para poder ver a que contenidos accede
- Internet también ofrece riesgos. El fraude y la provocación sexual son los principales riesgos a los que sus hijos se pueden enfrentar. Insístales en que no deben proporcionar datos personales, ni nombre y horario de colegios. No debe establecer citas reales con nadie sin su conocimiento.
- Si su hijo le informa de contenidos que le han hecho sentir incómodos (de contenido sexual) denúncielo.
- Los contenidos para adultos son de fácil acceso. En algunos casos, detrás de ellos se esconden intereses comerciales. Se paga el acceso a esos contenidos mediante conexiones a Internet a través de teléfonos de tarificación especial (906xxxxxx). Bajo avisos y contratos poco claros para un menor se cambia la conexión a estos números con un incremento alarmante de la facturación telefónica. Conciencie a su hijo que no debe acceder a esos contenidos y el peligro que supone.
- Idénticas situaciones se producen con adquisición aparentemente gratuita de logos y tonos para teléfonos móviles o salvapantallas con las fotografías de personajes populares para la juventud. Alerte a su hijo sobre las descargas de éstos exigiéndole su supervisión.
- No permita que su hijo efectúe el solo compras a través de Internet, no le deje su número de tarjeta sin su conocimiento. Supervise Vd. las compras.
- Eduque a su hijo sobre las consecuencias negativas de vulnerar las leyes. El que “mucha gente lo haga” no implica que sea legal. La piratería digital tiene como única solución la educación del ciudadano.

Consejos para los "Pequeños Cibernautas"

- No des nunca tu nombre, no digas donde vives ni como se llaman tus padres, no envíes fotografías tuyas ni de tu familia. No informes de tu horario de colegio ni de quien te va recoger.
- Si alguien te dice algo que te resulta incómodo o molesto díselo rápidamente a tus padres.
- No quedes nunca con nadie que hayas conocido en Internet sin el conocimiento y la autorización de tus padres.
- Nunca compres nada por Internet sin el conocimiento y consentimiento de tus padres.
- Si navegando accedes a páginas de pornografía, sal rápidamente y no intentes ver más imágenes. Seguramente, tendrás que pagar más en la factura del teléfono.
- No te descargues ningún programa ni salvapantallas sin el conocimiento de tus padres, aunque la página diga que es gratuito.
- No descargues logos ni tonos de llamada de teléfono móvil, aunque parezca gratuito

Dirección General de la Policía (Brigada de Investigación Tecnológica)

De la misma forma, podríamos enumerar estas recomendaciones, pero dada la similitud con las anteriores, las dejamos a la libre voluntad de cada uno que las quiera leer en: www.policia.es/indes.htm

¿Es Necesario el Uso de Programas Antivirus?

En teoría y con un determinado cuidado o disciplina no debiéramos de necesitarlo, pues muchos de las compañías a las que se les contrata el servicio de conexión o del correo poseen este tipo de contramedidas. Sin embargo la realidad es otra muy diferente ya que somos vulnerables a mil y unas variedades de virus que desde el comienzo de la Red circulan por ella. En definitiva y con independencia de los servicios que nos puedan aportar las compañías suministradoras tenemos que instalar en nuestro PC un programa antivirus y asegurarnos que se actualiza periódicamente a través de la Red.

¿Qué Programa Antivirus Tengo que Comprar?

Frecuentemente, cuando compramos un PC ya viene cargado un programa con una validez que puede variar hasta un máximo de un año. Tenemos que asegurarnos que periódicamente se actualiza a través de la Red y cuando finalice el periodo de vida o garantía, contratar inmediatamente la renovación que generalmente también se hace por el mismo sistema. Actualmente los más conocidos o con mayor prestigio en el mercado son:

www.norton.com

www.macaffe.com

www.panda.es

En el supuesto caso de necesitar comprar un programa de este tipo, déjate aconsejar por un profesional, (a ser posible por mas de uno), en tiendas de informática y evita las copias piratas, los bajados de la red y algunos de los que se venden en quioscos, este tipo de programas no cuentan con mantenimiento o actualización posterior.

Adicionalmente, y dentro del área de seguridad, tenemos que tener instalado un programa que nos proteja de los accesos desde la Red a nuestro PC. Este tipo de programa se le denomina:

"Cortafuegos o Firewall" y generalmente nos lo ofrece el fabricante de del sistema operativo, como es el caso de Microsoft. Al igual que los antivirus se ha de actualizar periódicamente.

¿Qué programas debemos de tener en nuestro PC para acceder a Internet?

Los programas mínimos recomendables son:

- Netscape
- Explorer
- Windows Media Player, o
- QuickTime Player

- Acrobat Reader
- Adobe Acrobat

Al igual que el sistema operativo (por ejemplo el Windows), los antivirus y cortafuegos; todos los programas que tengamos cargados en nuestro PC con licencia, debemos de actualizarlos periódicamente conectándonos a la Web del fabricante. Esto no evitará fallos de programa o interrelación con otros programas.

¿Qué programas debemos de tener para gestionar nuestro correo de Internet?

Hay diferentes gestores de correo e-mail en el mercado desde los más complejos o potentes como podría ser el Lotus Notes a los más sencillos ofrecidos frecuentemente y de forma gratuita con publicaciones o prensa.

Los más usados son:
- Outlook Express
- Outlook

Posiblemente este segundo es el que mas utilizado, ambos vienen con el programa de sistema operativo de Windows.

Glosario:

Definiciones técnicas y expresiones utilizadas en el mundo de la informática e Internet, necesarias para comprender mejor los mecanismos de su funcionamiento o errores. Hay que tener en cuenta que de la misma manera que crecen los usuarios de Internet, crecen las expresiones para manifestar los actos que en ella ocurren. (Este capitulo se confecciono en agosto del 2005)

A

Acceso de escritura o Permiso de escritura: Operación o derecho asociado a un usuario o a un programa, para escribir en un disco, o cualquier otro dispositivo de almacenamiento informático.

Acción directa: Es una categoría o tipo de virus específico.

Active X: Es una tecnología utilizada, entre otras cosas, para dotar a las páginas Web de mayores funcionalidades, como animaciones, vídeo, navegación tridimensional, etc. Los controles Active X son pequeños programas que se incluyen dentro de estas páginas. Lamentablemente, por ser programas, pueden ser el objetivo de algún virus.

Actualizar o Actualización: Los antivirus evolucionan continuamente hacia versiones más potentes y adaptadas a las nuevas tecnologías empleadas por los virus. Para no quedar obsoletos, detectan todos los nuevos virus que surgen a diario. Para ello, cuentan con el denominado Archivo de Identificadores de Virus. Este fichero incluye todas las características que identifican a cada uno de los virus, haciendo posible detectarlos y actuar en consecuencia. La incorporación de la última versión de dicho fichero y de otros al antivirus, es lo que se conoce como actualización.

Administrador: Es la persona o programa encargado de gestionar, realizar el control, conceder los permisos, etc. de todo un sistema informático o red de ordenadores.

Administrador de servicios: Es un applet con el que cuenta Windows XP/2000/NT, encargado de administrar (configurar y controlar) los Servicios del sistema.

ADSL (Asymmetric Digital Subscriber Line): Se trata de un tipo de conexión a Internet y de una clase de módem que se caracterizan por su elevada velocidad.

Adware: Son aquellos programas que muestran publicidad utilizando cualquier tipo de medio, por ejemplo: ventanas emergentes, banners, cambios en la página de inicio o de búsqueda del navegador, etc. Puede instalarse con el consentimiento del usuario y su plena conciencia, pero en ocasiones no es así. Lo mismo ocurre con el conocimiento o falta del mismo acerca de sus funciones.

Agencia de Protección de Datos -- APD (Data Protection Agency): Oficina u Organismo oficial creado en España en 1993 como consecuencia de la aprobación de la LORTAD (Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal). Su finalidad es la de proteger a los ciudadanos contra las invasiones a su intimidad, realizadas con medios informáticos, según establece en la Constitución Española.

Agent = (agente): En Internet un agente (también llamado agente inteligente) es un programa que recoge información o realiza algún otro servicio de forma planificada, y sin la presencia o intervención directa del usuario. Habitualmente, un programa agente, utilizando parámetros suministrados por el usuario, busca en toda Internet, o en parte de ella, información de interés para el mismo y se la facilita de forma periódica.

Algoritmo: La definición formal de algoritmo es: "conjunto ordenado de operaciones que permite hallar la solución de un problema".

Alias: (Apodo) Cada virus tiene asignado un determinado nombre y sin embargo, muchas veces es más fácil reconocerlo por alguna de sus características más destacadas. En estos casos, el virus cuenta además con un segundo nombre (a modo de nombre de pila) que hace referencia a dicha característica. Dicho nombre es lo que se conoce como alias de un virus. P.e.: el virus CIH se conoce con alias Chernobyl

Análisis heurístico: Consiste en el método, estrategia o técnica empleada para hacer más fácil la resolución de problemas. Aplicado al mundo informático, se entiende como una técnica utilizada para detectar virus que en ese momento son desconocidos.

ANSI (American National Standards Institute): Es un estándar definido y establecido en materia de informática.

Anti-Debug o Antidebugger: Se trata del conjunto de técnicas que los virus emplean para evitar ser investigados.

Antivirus o Programas antivirus: Son todos aquellos programas que permiten analizar la memoria, las unidades de disco y otros elementos de un ordenador, en busca de virus.

Anulación (opt-out): El proceso de rechazar la posibilidad de recibir mensajes desde una fuente comercial o anular la suscripción del destinatario que ya está suscrito a la lista de correo.

API (Application Programming Interface): Es una propiedad mediante la cual los programas pueden solicitar peticiones para ser atendidos o utilizar un servicio del sistema operativo y de otros programas.

Applets Java o Java Applets: Son pequeños programas, que se pueden incluir en algunas páginas Web, con la finalidad de aportar más y mejores funcionalidades a dichas páginas.

Archivo, Documento o Fichero: Es la información que se encuentra en un soporte de almacenamiento informático: textos, documentos, imágenes, bases de datos, ficheros de sonido, hojas de cálculo, etc. Se identifica por un nombre, un punto y una extensión (indica de qué tipo es el fichero).

Archivo de Identificadores de Virus: Es el fichero que permite a los antivirus detectar a los virus. También es conocido con el nombre de Fichero de Firmas.

Armouring: Es una técnica que utilizan los virus para esconderse e impedir ser detectados por los antivirus.

ASCII: Es un código (American Standard Code for Information Interchange) estándar definido y establecido para representar los caracteres (letras, números, signos de puntuación, caracteres especiales, etc.) de forma numérica.

ASP (Active Server Page): Es un tipo de páginas Web que permiten ser personalizadas a medida de las características y necesidades del usuario visitante. Además, también hace referencia a Application Service Provider. Es decir, proveedor de servicios de aplicaciones.

Ataque (Nuke): Caída o pérdida de la conexión de red, provocada de forma intencionada por alguna persona. El ordenador sobre el que se realiza un nuke, además puede quedar bloqueado.

Ataque de denegación de servicio (DoS): Tipo de ataque que se produce cuando un hacker envía archivos adjuntos u otros mensajes poco habituales o en masa para intentar colapsar sistemas de e-mail.

Ataque de diccionario: Programa que bombardea un servidor de e-mail con millones de direcciones electrónicas generadas por orden alfabético con el propósito de adivinar correctamente algunas de ellas. Esta técnica también se usa para conseguir contraseñas.

Ataque de recolección de directorios (DHA): Cuando un grupo de spammers bombardea un dominio con miles de direcciones de e-mail generadas con el propósito de recolectar direcciones de e-mail válidas de una organización o empresa.

Atributos: Son determinadas características que se asocian y determinan el tipo de fichero y directorio.

Autocrifrado o Cifrado: Es una técnica utilizada por algunos virus que se codifican a sí mismos (o parte de ellos), para tratar de evitar a los antivirus

Autoencriptación: Operación mediante la cual un virus codifica -cifra- parte de su contenido, o éste en su totalidad. Esto, en el caso de los virus, dificulta el estudio de su contenido.

Autofirma: Se trata de un texto o contenido que se introduce automáticamente cuando se crea un nuevo mensaje de correo electrónico.

Automarcador, Diales o Dialer: Es un programa que suele ser utilizado para redirigir, de forma maliciosa, las conexiones mientras se navega por Internet. Su objetivo es colgar la conexión telefónica que se está utilizando en ese momento (la que permite el acceso a Internet, mediante el marcado de un determinado número de teléfono) y establecer otra, marcando un número de teléfono de tarificación especial (por ejemplo: un 906). Esto supondrá un notable aumento del importe en la factura telefónica.

B

Backdoor o Puerta trasera: Se trata de un programa que se introduce en el ordenador y establece una puerta trasera a través de la cual es posible controlar el sistema afectado, sin conocimiento por parte del usuario.

Bandeja de acceso rápido en Windows (Quick Launch): Zona próxima al menú o botón Inicio de Windows, donde se encuentran diversos iconos que dan un acceso rápido y directo a determinados elementos y/o programas: correo electrónico, Internet, al antivirus, etc. En inglés se conoce como Quick Launch.

Bandeja de entrada: Es una carpeta existente en los programas de correo electrónico, que contiene todos los mensajes que se han recibido.

Bandeja de sistema, en Windows: Zona situada en la Barra de tareas de Windows (habitualmente en la parte inferior derecha de la pantalla y junto al reloj del sistema), que muestra diversos iconos para configurar opciones del sistema, visualizar el estado de la protección antivirus, etc. En inglés se conoce como System Tray.

Banner: Es un anuncio mostrado en una página web, sobre un determinado producto o servicio propio o ajeno a la página y que, al ser pulsado, lleva al sitio del anunciante.

Barra de estado: Sección inferior que aparece en las ventanas de algunos programas de Windows, con información sobre el estado del programa o de los ficheros con los que se trabaja.

Barra de tareas de Windows: Barra que aparece en la sección inferior de la pantalla cuando se trabaja en Windows. Esta barra contiene, entre otras cosas, el botón Inicio de Windows, el reloj del sistema, iconos que representan cada uno de los programas residentes en la memoria en ese momento y botones de acceso rápido que permiten la ejecución inmediata de ciertos programas.

Barra de título: Es un área que aparece en la sección superior de las ventanas de Windows. En ella, se muestra generalmente el nombre del programa al que corresponde la ventana y el título del fichero con el que se está trabajando.

Base de datos: Es un conjunto de ficheros que contienen datos y los programas que gestionan la estructura y la forma en la que éstos se almacenan, así cómo la forma en la que deben relacionarse entre sí. Algunos ejemplos de sistemas de bases de datos, son: Access, Oracle, SQL, Parados, dBase, etc.

BBS (Bulleting Board System): Es un sistema o servicio utilizado en Internet, que permite a los usuarios -mediante una suscripción previa- leer y responder a los mensajes que otros usuarios han escrito (en un foro de debate o grupo de noticias, por ejemplo).

BHO (Browser Helper Object): Es un plugin que se ejecuta automáticamente junto con el navegador de Internet, y extiende sus funciones. Algunos se emplean con fines maliciosos, como por ejemplo monitorizar las páginas web visitadas.

BIOS (Basic Input / Output System): Conjunto de programas que permite arrancar el ordenador (parte del sistema de arranque).

Bit (Binary digit): Es la unidad más pequeña de la información digital con la que trabajan los ordenadores (sistemas informáticos).

Bomba lógica: Es un programa, en principio de apariencia normal e inofensiva, que puede actuar provocando acciones dañinas, al igual que cualquier otro virus.

Boot o Master Boot Record (MBR): También conocido como Sector de Arranque, es el área o la sección de un disco donde se almacena información sobre sus características y la capacidad del disco para arrancar el ordenador.

Bucle: Se trata del conjunto de comandos u órdenes que un programa realiza de forma, en un número concreto y reiterado de ocasiones.

Buffer: Es una memoria intermedia utilizada para guardar temporalmente la información que se transfiere entre diferentes dispositivos informáticos (o entre los componentes de un mismo sistema informático).

Bug: Este término se emplea para indicar un fallo o error en un programa informático. Cuando uno de ellos tiene errores, se dice que tiene bugs.

Bus: Canal de comunicación entre los diferentes componentes de un ordenador (señales de datos, de direcciones de control, etc.).

Byte: Es una unidad que mide la cantidad de información, tamaño y capacidad de almacenamiento. Un Byte, equivale a 8 Bits.

C

Caballo de Troya o Troyano: En sentido estricto, un troyano no es un virus, aunque se considere como tal. Realmente se trata de un programa que llega al ordenador de manera encubierta, aparentando ser inofensivo, se instala y realiza determinadas acciones que afectan a la confidencialidad del usuario afectado. La historia mitológica El Caballo de Troya ha inspirado su nombre.

Cabecera (de un fichero): Es la parte de un fichero, donde se guarda información sobre éste y su ubicación.

Caché: Es una pequeña sección correspondiente a la memoria de un ordenador.

Cadena o Cadena de caracteres: Es una consecución de caracteres de texto, dígitos numéricos, signos de puntuación, caracteres especiales o espacios en blanco consecutivos.

Camuflaje: Técnicas de ocultación de datos por parte de los spammers para evitar ser detectados. También tiene lugar cuando los destinatarios del e-mail usan HTML o Java script para camuflar enlaces de e-mail y direcciones de correo para que las direcciones se puedan leer y se pueda hacer clic sobre ellas, pero no pueden ser recolectadas.

Capturador de teclado o Keylogger: Programa que recoge y guarda una lista de todas las teclas pulsadas por un usuario. Dicho programa puede hacer pública la lista, permitiendo que terceras personas conozcan estos datos -lo que ha escrito el usuario afectado (información introducida por teclado: contraseñas, texto escrito en documentos, mensajes de correo, combinaciones de teclas, etc.)-.

Carpeta o Directorio: Divisiones, secciones (no físicas) mediante las cuales se estructura y organiza la información contenida en un disco. Los términos carpeta y directorio hacen referencia al mismo concepto. Pueden contener ficheros y otros directorios (sub-directorios o sub-carpetas).

Categoría o Tipo: No todos los virus son iguales. Éstos pueden ser agrupados por características concretas que conforman un tipo concreto de virus.

Cavity: Técnica utilizada por algunos virus y gusanos para dificultar su localización. Aplicando dicha técnica consiguen no variar el tamaño de cada uno de los ficheros infectados o afectados (utilizan solamente las cavidades del fichero afectado).

Certificado o Certificación: Fichero que emite una compañía o servidor, que se aloja en el navegador de nuestro sistema y sirve para identificarle, a él o a uno de los usuarios.

CGI (Common Gateway Interface): I interface para que programas externos (pasarelas) puedan rodar bajo un servidor de información. Actualmente, los servidores de información soportados son servidores HTTP (hypertext Transfer Protocol).

Cifrado o Autocrifrado: Es una técnica utilizada por algunos virus que se codifican a sí mismos (o parte de ellos), para tratar de evitar a los antivirus.

Cilindro: Sección de un disco que se puede leer por completo en una sola operación.

Clave del Registro de Windows: Son secciones del Registro de Windows, en las cuales se almacenan determinados valores correspondientes a la configuración del ordenador.

Cliente: Sistema informático (ordenador) que solicita ciertos servicios y recursos de otro ordenador (denominado servidor), al que está conectado en red.

Cluster: Son varios sectores consecutivos de un disco.

CMOS (Complementary Metal Oxide Semiconductor): Es una sección de la memoria de un ordenador en la que se guarda la información y los programas que permiten arrancar el ordenador (BIOS).

Código: Contenido de los ficheros de un virus o código del virus, escrito en un determinado lenguaje de programación-. También hace referencia a los sistemas de representación de información. En sentido estricto, puede definirse como conjunto de normas sistemáticas que regulan unitariamente una materia determinada, o combinación de signos que tiene un determinado valor dentro de un sistema establecido.

Compañía, Virus de compañía o Spawning: Se trata de un tipo de virus que no se incluye dentro de otros programas, sino que se asocia a ellos.

Comprimido, Comprimir, Compresión o Descomprimir: La compresión de ficheros es una operación por la que uno o un grupo de ellos, se incluye dentro de otro fichero que los contiene a todos, ocupando menos espacio.

Condición de activación (Trigger): Son las condiciones bajo las cuales un virus se activa o comienza a realizar sus acciones en el ordenador infectado.

Consentimiento (opt-in): El proceso de aceptar recibir mensajes desde una fuente comercial. La "doble confirmación" hace referencia al procedimiento de confirmar por segunda vez que quiere apuntarse a la lista de correo.

Constructor de virus: Es un programa malicioso que permite crear nuevos virus sin necesidad de tener conocimientos de programación, mediante una interfaz a

través de la cual se eligen las características del malware creado: tipo, efectos, archivos que infectará, encriptación, polimorfismo, etc.

Contraseña o Password: Es una cadena de caracteres con la que se restringe o permite el acceso, de ciertos usuarios, a un determinado lugar o fichero. El ejemplo más habitual es la contraseña de una tarjeta de crédito.

Controlador o Driver: Es un programa, conocido como controlador, que permite la gestión de los dispositivos conectados al ordenador (generalmente, periféricos como impresoras, unidades de CD-ROM, etc.).

Control de red (Control DNS inverso): Cuando un motor anti-spam utiliza una base de datos de sistema de nombre de dominio para comprobar que la dirección IP de un e-mail se cree en un dominio o dirección de Web válidos.

Control complejo de diccionario: Función del software anti-spam que examina el texto en busca de palabras ofensivas y que no se deja engañar por trucos, como la sustitución de letras por números o caracteres similares (como "t@sa de interés").

Control remoto: Acceso al ordenador de un usuario (con su consentimiento, o sin él), desde otro ordenador que se encuentra en otro lugar. Dicho acceso puede suponer una amenaza, si no es realizado convenientemente, o con buenas intenciones.

Cortafuegos o Firewall: Su traducción literal es muro de fuego, también conocido a nivel técnico como cortafuegos. Es una barrera o protección que permite a un sistema salvaguardar la información al acceder a otras redes, como por ejemplo Internet.

Cookie: Es un fichero de texto que, en ocasiones, se envía a un usuario cuando éste visita una página Web. Su objetivo es registrar la visita del usuario y guardar cierta información al respecto.

Cracker: Es una persona interesada en saltarse la seguridad de un sistema informático.

CRC (número o código CRC): Es un código numérico asociado de forma única a cada uno de los ficheros. Es como el número de pasaporte de dicho fichero.

CVP (Content Vectoring Protocol): Protocolo desarrollado en 1996 por Check Point que permite integrar una protección antivirus en un servidor firewall.

Ch

Chat, Chat IRC o Chat ICQ: Son las conversaciones escritas en Internet, en tiempo real.

Chivato (web bug): Pequeño gráfico insertado en un e-mail o página Web que avisa a un spammer cuando un mensaje se ha leído o previsualizado.

D

Daño potencial, Nivel de daños o Perjuicio: Se trata de un valor que indica el grado de efectos que el virus puede producir en un ordenador afectado. Este dato se emplea para el cálculo del Índice de peligrosidad.

DdoS o Denegación de servicios distribuida: Es un ataque de Denegación de servicios (DoS) realizado al mismo tiempo desde varios ordenadores, contra un servidor.

Debug / Debugger o Desensamblaje: Herramienta informática con la que se puede leer el código fuente en el que están escritos los programas.

Denegación de servicios distribuida o DdoS: Es un ataque de Denegación de servicios (DoS) realizado al mismo tiempo desde varios ordenadores, contra un servidor.

Derechos de administrador: Conjunto de acciones u operaciones, que sólo uno o varios usuarios concretos pueden realizar dentro de una red de ordenadores.

Descarga o Download: Es la acción por la cual se obtienen ficheros de Internet (de páginas Web o de lugares FTP dispuestos para este fin).

Descomprimir, Comprimido, Comprimir o Compresión: La compresión de ficheros es una operación por la que uno o un grupo de ellos, se incluye dentro de otro fichero que los contiene a todos, ocupando menos espacio.

Desinfección: Es la acción que realizan los antivirus cuando detectan a un virus y lo eliminan.

Detección actualizada: Es la fecha en que se actualizó por última vez la detección de un malware dentro del Archivo de Identificadores de Virus.

Diales, Automarcador o Dialer: Es un programa que suele ser utilizado para redirigir, de forma maliciosa, las conexiones mientras se navega por Internet. Su objetivo es colgar la conexión telefónica que se está utilizando en ese momento (la que permite el acceso a Internet, mediante el marcado de un determinado número de teléfono) y establecer otra, marcando un número de teléfono de tarificación especial (por ejemplo: un 906). Esto supondrá un notable aumento del importe en la factura telefónica.

Directorio o Carpeta: Divisiones, secciones (no físicas) mediante las cuales se estructura y organiza la información contenida en un disco. Los términos carpeta y directorio hacen referencia al mismo concepto. Pueden contener ficheros y otros directorios (sub-directorios o sub-carpetas).

Directorio raíz: Es la carpeta o directorio principal (más importante) de un disco.

Disco de emergencia o Disco de rescate: Disquete que permite analizar el ordenador sin utilizar el antivirus que se encuentra instalado en él, sino con lo que se conoce como el antivirus en línea de comandos.

Disco de inicio, de sistema, o de arranque: Disco (disquete, CD-ROM o disco duro) con el que es posible arrancar el sistema operativo del ordenador.

DLL (Librería de enlace dinámico): Es un tipo especial de fichero, con extensión DLL.

DNS (Sistema de Nombres de Dominio): Sistema que facilita la comunicación entre ordenadores conectados a una red (o a Internet), su localización, etc., asignando nombres (cadenas de texto más comprensibles) a las direcciones IP de cada uno de ellos. Los servidores DNS, son aquellos ordenadores en los que se relacionan, administran y gestionan todos esos nombres (de dominio) y se relacionan con sus correspondientes direcciones IP.

Documento, Fichero o Archivo: Es la información que se encuentra en un soporte de almacenamiento informático: textos, documentos, imágenes, bases de datos, ficheros de sonido, hojas de cálculo, etc. Se identifica por un nombre, un punto y una extensión (indica de qué tipo es el fichero).

DoS / Denegación de servicios: Es un ataque, causado en ocasiones por los virus, que evita al usuario la utilización de ciertos servicios (del sistema operativo, de servidores Web, etc.).

DOS (Disk Operating System): Sistema operativo básico, anterior al Windows, Unix o Linux, en el que se trabaja escribiendo órdenes para todas las operaciones

que se desean realizar en lugar de hacerlas con el ratón. También se le conoció como MS-DOS por haberse realizado en Microsoft

Download o Descarga: Es la acción por la cual se obtienen ficheros de Internet (de páginas Web o de lugares FTP dispuestos para este fin).

Dropper: Es un fichero ejecutable que contiene varios tipos de virus en su interior.

E

EICAR: European Institute of Computer Anti-Virus Research. Se trata de una institución informática que ha creado un método para evaluar la fiabilidad y el comportamiento de los antivirus: el test EICAR.

Elementos eliminados: Es una carpeta existente en los programas de correo electrónico, que contiene todos los mensajes que se han borrado o eliminado (los que no se han borrado definitivamente). En el caso de borrar el mensaje de un virus, es conveniente acceder a esta carpeta y eliminarlo también en ella.

Elementos enviados: Es una carpeta existente en los programas de correo electrónico, que contiene todos los mensajes que se han enviado a otros destinatarios.

ELF -ficheros- (Executable and Linking Format): Ficheros ejecutables (programas), propios del sistema operativo Unix/Linux.

Empaquetar: Operación por la cual un grupo de ficheros (o uno sólo) se incluyen dentro de otro fichero, ocupando así menos espacio. El empaquetado es similar a la compresión de ficheros, pero es más común llamarlo así en sistemas Uníx o Lunix. La diferencia entre empaquetado y compresión es la herramienta con que se realiza la operación. Por ejemplo, la herramienta se utiliza para empaquetar, mientras que la herramienta zip o gzip -WinZip- se utiliza para comprimir.

En circulación: Se dice que un virus está en circulación, cuando se están realizando detecciones de él, en cualquier parte del mundo, durante un período de tiempo.

EPO (Entry Point Obscuring): Técnica para infectar programas mediante la cual un virus intenta ocultar su punto de entrada para evitar ser detectado. El virus, en lugar de tomar el control y realizar sus acciones al principio del programa (de su

utilización o ejecución), permite el correcto funcionamiento de éste hasta un cierto momento en el que comienza a actuar.

Escanear -puertos, direcciones IP-: Acción por la cual se chequean los puertos de comunicaciones y/o las direcciones IP de un ordenador, para localizarlos y obtener información sobre su estado. En ocasiones, puede considerarse un ataque o amenaza.

Escritorio de Windows: Es el área principal de Windows, que aparece al arrancar el ordenador. Desde ella se accede a todas las herramientas, utilidades y programas instalados en el ordenador, mediante iconos de acceso directo, opciones de menú existentes en el botón Inicio de Windows, la Barra de tareas de Windows, etc.

Estación, Puesto o Workstation: Es uno de los ordenadores conectados a una red local que utiliza los servicios y los recursos existentes en dicha red. Por lo general, no presta servicios al resto de ordenadores de la red como lo hacen los servidores.

Estafa o timo (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.).

Executable and Linking Format (ELF -ficheros): Ficheros ejecutables (programas), propios del sistema operativo Unix/Linux.

Excepciones: Se trata de una técnica utilizada por los antivirus para la detección de virus.

Exploit: Es una técnica o un programa que aprovecha un fallo o hueco de seguridad una vulnerabilidad existente en un determinado protocolo de comunicaciones, sistema operativo, o herramienta informática.

Explorador de Windows: Programa o aplicación disponible en Windows que permite gestionar los ficheros disponibles en el ordenador. Es de gran utilidad para visualizar estructuras de directorios de forma organizada.

Extensión: Los ficheros se representan asignándoles un nombre y una extensión, separados entre sí por un punto: NOMBRE.EXTENSIÓN. El fichero puede tener cualquier nombre NOMBRE, pero la EXTENSIÓN (si existe) tendrá como máximo 3 caracteres. Dicha extensión es la que indica el formato o tipo de fichero (texto, documento de Word, imagen, sonido, base de datos, programa, etc.).

F

Falso negativo: Cuando un programa anti-spam no consigue identificar un mensaje de spam como tal.

Falso positivo: Cuando un programa anti-spam identifica erróneamente un mensaje legítimo como spam

Familia o Grupo: Existen virus con nombres muy parecidos y características similares, incluso idénticas. Estos grupos de virus, que tienen hermanos, conforman lo que se denomina una familia de virus. Cada uno de ellos, en lugar de denominarse hermanos, se denominan variantes de la familia o del virus original (el que apareció primero, el padre).

FAT (File Allocation Table): Es una sección de un disco en la que se define la estructura y las secciones del citado disco. Además en ella se guardan las direcciones para acceder a los ficheros que el disco contiene.

Fecha de aparición: Es la fecha en la que se tuvo la primera noticia de la existencia de un virus concreto.

Fecha de detección: Es la fecha en la que se incluyó la detección de un determinado malware dentro del Archivo de Identificadores de Virus.

Fichero, Archivo o Documento: Es la información que se encuentra en un soporte de almacenamiento informático: textos, documentos, imágenes, bases de datos, ficheros de sonido, hojas de cálculo, etc. Se identifica por un nombre, un punto y una extensión (indica de qué tipo es el fichero).

Ficheros de proceso por lotes (Batch): Son ficheros que tienen extensión BAT y que permiten automatizar operaciones.

Ficheros SCR: Este tipo de ficheros tienen extensión SCR y pueden ser salvapantallas de Windows o ficheros cuyo contenido es lenguaje Script.

Filtrado bayesiano: Enfoque estadístico para determinar si un e-mail es spam.

Firewall o Cortafuegos: Su traducción literal es muro de fuego, también conocido a nivel técnico como cortafuegos. Es una barrera o protección que permite a un sistema salvaguardar la información al acceder a otras redes, como por ejemplo Internet.

FireWire: Es un tipo de canal de comunicaciones externo caracterizado por su elevada velocidad de transferencia, empleado para conectar ordenadores y periféricos a otro ordenador.

Firma o Identificador: Se trata del número de pasaporte de un virus. Es decir, una cadena de caracteres (números, letras, etc.) que representa de forma inequívoca a un virus.

Flooder: Programa que envía el mismo mensaje o texto de manera reiterada y masiva, pretendiendo así producir un efecto de saturación, colapso o inundación (de ahí su nombre, inundador) en sistemas de correo como MSN Messenger.

Formateo o Formatear: Dar formato a una unidad de disco, eliminando todo su contenido.

Freeware: Es todo aquel software, legalmente distribuido, de forma gratuita.

FTP (File Transfer Protocol): Es un mecanismo que permite la transferencia de ficheros a través de una conexión TCP/IP.

G

Gateway: Es un ordenador que permite las comunicaciones entre distintos tipos de plataformas, redes, ordenadores o programas. Para lograrlo traduce los distintos protocolos de comunicaciones que éstos utilizan. Es lo que se conoce como pasarela o puerta de acceso.

GDI (Graphics Device Interface): Es el sistema (Interfaz de Dispositivos para Gráficos,) que permite al sistema operativo Windows mostrar presentaciones en pantalla y en las impresoras.

GNU: La Fundación para el Software Libre (FSF - Free Software Foundation) está dedicada a eliminar las restricciones de uso, copia, modificación y distribución del software. Promueve el desarrollo y uso del software libre en todas las áreas de la computación. Específicamente, la Fundación pone a disposición de todo el mundo un completo e integrado sistema de software llamado GNU. La mayor parte de este sistema está siendo ya utilizado y distribuido.

Groupware: Es el sistema que permite a los usuarios de una red local (LAN) la utilización de todos los recursos de ésta como, programas compartidos, accesos a Internet, intranet y a otras áreas, correo electrónico, firewalls, proxys, etc.

Grupo o Familia: Existen virus con nombres muy parecidos y características similares, incluso idénticas. Estos grupos de virus, que tienen hermanos, conforman lo que se denomina una familia de virus. Cada uno de ellos, en lugar de denominarse hermanos, se denomina variantes de la familia o del virus original (el que apareció primero, el padre).

Grupo de noticias: Es uno de los servicios de Internet, mediante el cual varias personas se conectan para discutir e intercambiar información sobre temas concretos de interés común.

Gusano (Worm): Es un programa similar a un virus que, a diferencia de éste, solamente realiza copias de sí mismo, o de partes de él.

H

Hacker: Persona que accede a un ordenador de forma no autorizada e ilegal.

Hardware: Término que hace referencia a cada uno de los elementos físicos de un sistema informático (pantalla, teclado, ratón, memoria, discos duros, microprocesador, etc.).

Herramienta de hacking: Programa que puede ser utilizado por un hacker para causar perjuicios a los usuarios de un ordenador (pudiendo provocar el control del ordenador afectado, obtención de información confidencial, chequeo de puertos de comunicaciones, etc.).

Hijacker: Literalmente, secuestrador. 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.

Hiperenlace, Referencia, Salto o Link: Estos cuatro términos hacen referencia al mismo concepto. Se trata de elementos o secciones dentro de una página Web (texto, imágenes botones, etc.), que permiten el acceso a otra página o área dentro de la misma página, cuando se pincha sobre ellos.

Hoax: No es un virus, sino falsos mensajes de alarma (bromas o engaños) sobre virus que no existen.

Host: Este término se refiere a un ordenador que actúa como fuente de información.

HTTP (HyperText Transfer Protocol): Es un sistema de comunicación que permite la visualización de páginas Web, desde un navegador.

I

Identificador o Firma: Se trata del número de pasaporte de un virus. Es decir, una cadena de caracteres (números, letras, etc.) que representa de forma inequívoca a un virus.

IFS (Instalable File System): Sistema que se encarga de gestionar las transferencias de información de entrada y de salida, correspondientes a un grupo de dispositivos informáticos (de la red o de otras redes) y ficheros.

IIS (Internet Information Server): Es un servidor de Microsoft (Internet Information Server), destinado a la publicación, mantenimiento y gestión de páginas y portales Web.

IMAP (Internet Message Access Protocol): Es un sistema de comunicación que permite el acceso a los mensajes de correo electrónico.

In The Wild: Se trata de una lista oficial en la que se enumeran mensualmente los virus que más incidencias han ocasionado (los más extendidos).

Índice de peligrosidad: Es un valor calculado que permite medir lo peligroso que puede llegar a ser un virus.

Infección: Es la acción que realizan los virus, consistente en introducirse en el ordenador o en áreas concretas de éste y en determinados ficheros.

Ingeniería social: Engañar a los destinatarios de e-mail para abrir mensajes, dar a conocer contraseñas o proporcionar información confidencial aprovechándose de su curiosidad, credulidad o inexperiencia informática.

Interfaz o Interface: Es el sistema que permite a los usuarios dialogar (comunicarse e interactuar) con el ordenador y el software que éste tiene instalado. A su vez, este software (programas) se comunica mediante un sistema de interfaz con el hardware del ordenador.

Internet: Es la red de redes. Nacida como un experimento del Ministerio de Defensa Americano, posteriormente ampliada al ámbito científico-universitario. Este embrión se extendido, hoy día, por todo el mundo. Desde el punto de vista técnico,

Internet es un gran conjunto de redes de ordenadores interconectadas (la mayor red mundial). Desde otro punto de vista, Internet es un fenómeno sociocultural. Un usuario desde su consola, tiene acceso a la mayor fuente de información que existe. En cuanto a funcionamiento interno, Internet no se ajusta a ningún tipo de ordenador, tipo de red, tecnología de conexión o medios físicos empleados. Internet no tiene una autoridad central, es descentralizada. Cada red mantiene su independencia y se une cooperativamente al resto respetando una serie de normas de interconexión. La familia de protocolos TCP/IP es la encargada de aglutinar esta diversidad de redes. A principios de 1.992 fue creada la Internet Society (ISOC). Se trata de una sociedad profesional sin ánimo de lucro, formada por organizaciones e individuos de todos los sectores involucrados de una u otra forma en el desarrollo de Internet (usuarios, proveedores, fabricantes de equipos, administradores, etc.). El principal objetivo es fomentar el crecimiento de Internet en todos sus aspectos (número de usuarios, nuevas aplicaciones, infraestructuras, etc...).

Interrupción: Es una señal mediante la cual se consigue hacer una pausa momentánea en las labores que lleva a cabo el cerebro del ordenador (el microprocesador).

IP (Internet Protocol) / TCP-IP: La IP es la dirección o código que identifica exclusivamente a cada uno de los ordenadores existentes. El protocolo TCP/IP es el sistema utilizado para la interconexión de dichos ordenadores, sin provocar conflictos de direcciones. Se utiliza en Internet.

IRC (Chat IRC): Son conversaciones escritas a través de Internet (en las que además pueden transferirse ficheros), conocidas vulgarmente como Chat.

ISP (Internet Service Provider): Es un proveedor de acceso a Internet que además ofrece una serie de servicios relacionados con Internet (Proveedor de Servicios Internet).

J

Java: Es un lenguaje de programación que permite generar programas independientes de la plataforma, es decir, que pueden ejecutarse en cualquier sistema operativo o hardware (lenguaje multiplataforma).

Java Applets o Applets Java: Son pequeños programas, que se pueden incluir en algunas páginas Web, con la finalidad de aportar más y mejores funcionalidades a dichas páginas.

JavaScript: Es un lenguaje de programación que aporta características dinámicas (datos variables en función del tiempo y el modo de acceso, interactividad con el usuario, personalización, etc.) a las páginas Web, escritas en lenguaje HTML.

Joe job (mensaje incriminatorio): Es una campaña de spam falsificada para que aparente proceder de una parte inocente, con la intención de incriminar o echarle la culpa a esa parte. La parte inocente podrá verse inundada con un aluvión de mensajes devueltos por la campa de spam.

Joke: No es un virus, sino bromas de mal gusto que tienen por objeto hacer pensar a los usuarios que han sido afectados por un virus.

JPEG (Join Photographic Expert Group): Formato gráfico comprimido desarrollado por la 'Join Photographic Expert Group'. El formato JPEG soporta 24 bits por pixel y 8 bits por pixel en imágenes con escala de grises. Realiza un buen trabajo con imágenes (imágenes escaneadas)

K

Kernel: Es el núcleo, la parte más importante o el centro del sistema operativo.

Keylogger (Capturador de teclado): Programa que recoge y guarda una lista de todas las teclas pulsadas por un usuario. Dicho programa puede hacer pública la lista, permitiendo que terceras personas conozcan estos datos -lo que ha escrito el usuario afectado (información introducida por teclado: contraseñas, texto escrito en documentos, mensajes de correo, combinaciones de teclas, etc.)-.

L

Lavado de lista: Proceso de eliminar direcciones de e-mail de una lista de correo a petición de los remitentes.

Ladrón de contraseñas: Programa que obtiene y guarda datos confidenciales, como las contraseñas de acceso de un usuario (utilizando keyloggers u otros medios). Dicho programa puede hacer pública esta información, permitiendo que terceras personas puedan utilizarla en perjuicio del usuario afectado.

LAN (Local Area Network): Es una red de área local, o grupo de ordenadores conectados entre sí dentro de una zona pequeña geográfica (generalmente en una misma ciudad, población, o edificio).

Lenguaje de programación: Conjunto de instrucciones, órdenes, comandos y reglas que permite la creación de programas. Los ordenadores entienden señales eléctricas (valores 0 ó 1). Los lenguajes permiten al programador indicar lo que debe hacer un programa, sin tener que escribir largas cadenas de ceros y unos, sino palabras (instrucciones) más comprensibles por las personas.

Librería de enlace dinámico (DLL): Es un tipo especial de fichero, con extensión DLL.

Libreta de direcciones: Fichero con extensión WAB, donde se almacenan datos de contacto de otros usuarios, como la dirección de correo electrónico (entre otros).

Link, Referencia, Salto o Hiperenlace: Estos cuatro términos hacen referencia al mismo concepto. Se trata de elementos o secciones dentro de una página Web (texto, imágenes botones, etc.), que permiten el acceso a otra página o área dentro de la misma página, cuando se pincha sobre ellos.

Lista de tareas: Es la relación -el listado- de todos los programas y procesos que se encuentran activos (en funcionamiento), en un determinado momento (generalmente en el sistema operativo Windows).

Linux: Es una implementación independiente con "espíritu" POSIX (especificación para sistemas operativos). Tiene extensiones System V y BSD, y ha sido escrito completamente a base de aportaciones. Linux no tiene código propietario. Linux está distribuido libremente bajo "GNU Public License". Actualmente solo trabaja en IBM PC (o compatibles) y con arquitecturas ISA e EISA, y requiere un procesador 386 o superior. El kernel de Linux está escrito por Linux Torvalds (Torvalds@kruuna.helsinki.fi), desde Finlandia y otros voluntarios de otras partes del mundo. La mayoría de los programas que ruedan bajo Linux son freeware, y muchos de ellos del Proyecto GNU. Linux tiene todas las características que se pueden esperar de un moderno y flexible UNIX. Incluye multitarea real, memoria virtual, librerías compartidas, dirección y manejo propio de memoria y TCP/IP. Usa las características hardware de la familia de procesadores 386 para implementar las capacidades anteriores. En cuanto a software que funciona en Linux, podemos citar GCC, Emacs, Windows, todas la utilidades del Unix estándar, TCP/IP (incluyendo SLIP y PPP) y cientos de programas que cualquiera pueda compilar y llevar a esta plataforma. En cuanto a hardware, admite bus local VESA y PCI. No rueda en MCA (MicroChannel, bus propietario de IBM). Existe un proyecto para llevar Linux a la máquinas basadas en el 68000 de Motorola (como por ejemplo, Comodore Amiga y Atari), hay otro proyecto para llevar Linux a la arquitectura PowerPC.

Lista blanca: Lista de direcciones de e-mail, direcciones IP y dominios desde los cuales se envían mensajes que son aceptados por la empresa o usuarios. Todos los mensajes procedentes de estas direcciones se entregan al destinatario sin pasar por los filtrados de spam.

Lista de agujero negro: Lista publicada, normalmente comercial, de direcciones IP conocidas como fuentes de spam que puede usarse para crear una lista negra para filtrar el correo procedente de esas direcciones.

Lista de agujero negro de sistema de nombre de dominio (DNSBL): Listas comerciales de redes que o bien permiten a los spammers usar sus sistemas para enviar spam o bien no han tomado medidas para impedir a spammers abusar de sus sistemas.

Lista de agujero negro en tiempo real (RBL): A diferencia de la lista de agujero negro, la lista de agujero negro en tiempo real rechaza todos los mensajes de spam, válidos o no, procedentes de direcciones conocidas por enviar spam o acoger a spammers. No obstante, esto podría llevar a los proveedores de servicios de Internet a tomar medidas anti-spam.

Lista de tareas: Es la relación -el listado- de todos los programas y procesos que se encuentran activos (en funcionamiento), en un determinado momento (generalmente en el sistema operativo Windows).

Lista gris: Los remitentes que no están en una lista negra (excluidos) o en una lista blanca (aceptados) pueden colocarse en una lista gris. Algunos programas anti-spam pueden enviar a las direcciones de la lista gris una respuesta automática solicitando al remitente que confirme su legitimidad.

Lista negra: Función del software anti-spam que permite al usuario designar direcciones IP, nombres de dominio y direcciones individuales de e-mail desde las que no aceptan mensajes.

M

Macintosh: Familia de ordenadores fabricados por Apple Computer. Posee un sistema operativo basado en ventanas. El entorno es intuitivo, eliminando el teclado de los comandos del sistema. Prácticamente todo puede hacerse a través de menús desplegables y de ratón. A todos los objetos se le asigna una representación gráfica (iconos).

Macro: Una macro es una secuencia de instrucciones u operaciones que definimos para que un programa (por ejemplo, Word, Excel, PowerPoint, o Access) las realice de forma automática y secuencial. Por ser programas, pueden verse afectadas por los virus. Los virus que utilizan las macros para realizar infecciones, se denominan virus de macro.

Mail: El correo electrónico es el servicio más básico, antiguo, y más utilizado dentro de Internet. El envío de mensajes electrónicos es el medio más eficaz y más rápido de comunicación, permite intercambiar además de mensajes, programas, audio, vídeo e imágenes. Cada usuario dentro de un sistema posee una dirección de e-mail formada por: usuario@ordenador.dominio.subdominio

Mail drop: Dirección de e-mail configurada para recibir las respuestas a mensajes de spam enviados desde un proveedor de acceso a Internet diferente. Con el fin de evitar la detección, el spammer cancela la cuenta desde la que envó el spam.

Mailing lists: Listas de correo o listas de distribución, establecen foros de discusión privados a través de correo electrónico. Las listas de correo están formada por direcciones e-mail de los usuarios que la componen. Cuando uno de los participantes envía un mensaje a la lista, ésta reenvía una copia del mismo al resto de usuarios de la lista (inscritos en ella).

Malware: Cualquier programa, documento o mensaje, susceptible de causar perjuicios a los usuarios de sistemas informáticos. MALicious softWARE.

Mapeo, Mapear o Mapeado: Es la acción por la cual se asigna una letra a una unidad de disco, que se encuentra compartida en una red de ordenadores, como si de un disco más del ordenador se tratase.

MAPI (Messaging Application Program Interface): Es un sistema empleado para que los programas puedan enviar y recibir correo electrónico mediante un sistema de mensajería concreto. Tambien es el conjunto de especificaciones que permite intercambiar texto y ficheros con juegos de caracteres diferentes (entre ordenadores con idiomas diferentes, (por ejemplo).

Máscara (de red o de dirección): Es un número -de 32 bits- que identifica la dirección IP de una red concreta. Esto permite que el protocolo de comunicaciones conocido como TCP/IP, pueda saber si una dirección IP asociada a un ordenador, pertenece a una red u a otra.

Master Boot Record (MBR) o Boot: También conocido como Sector de Arranque, es el área o la sección de un disco donde se almacena información sobre sus características y la capacidad del disco para arrancar el ordenador.

Mensaje incriminatorio (Joe job): Es una campaña de spam falsificada para que aparente proceder de una parte inocente, con la intención de incriminar o echarle la culpa a esa parte. La parte inocente podrá verse inundada con un aluvión de mensajes devueltos por la campa de spam.

Mensaje recuperado: Mensaje que el destinatario no considera spam.

Menú contextual: Listado de definiciones que se pueden seleccionar cuando se pulsa con el botón secundario del ratón (generalmente el derecho) sobre un determinado elemento o área de la ventana, de un programa. Dichas opciones suelen estar escogidas dentro de un contexto, es decir, seleccionadas para acceder directamente a determinadas áreas del programa.

Método de infección: Es una de las características más importantes de un virus. Se trata de cada una de las operaciones que el virus realiza para llevar a cabo su infección en el ordenador afectado.

Método de propagación: Es una de las características más importantes de un virus. Se trata de cada una de las operaciones que el virus realiza para transmitirse a otros ordenadores.

Microprocesador o Procesador: Es el corazón electrónico e integrado de un ordenador o sistema informático, popularmente conocido como Pentium (I, II, III, IV,...), 486, 386, 286, 8086, etc. Se trata del chip (pastilla o circuito integrado -CI- de silicio, con elementos electrónicos microscópicos -transistores, resistencias etc.-) que gobierna todas y cada una de las operaciones que se realizan en el sistema.

Microsoft windows (sistema operativo): Sistema operativo gráfico de Microsoft basado en ventanas. Es el más popular en entornos PC. Permite el acceso a Internet mediante TCP/IP y Winsockets.

MIME (Multipurpose Internet Mail Extensions): Extensiones Multipropósito del Correo Internet. Es el conjunto de especificaciones que permite intercambiar texto y ficheros con juegos de caracteres diferentes (entre ordenadores con idiomas diferentes, por ejemplo).

Mirror: Término usado en Internet para hacer referencia a un FTP, WEB o cualquier otro recurso que es espejo de otro. Estos “mirrors” se realizan

automáticamente y pretenden tener una copia exacta del lugar del que hacen "mirror".

Módem: Es un elemento físico (un periférico), también conocido como MOdulador DEMmodulador, que se utiliza para convertir las señales eléctricas (analógicas y digitales). Su objetivo es facilitar la comunicación entre ordenadores y otros tipos de equipos. Su utilidad más habitual, en la actualidad, es conectar los ordenadores a Internet.

Módulo: En términos informáticos, consiste en el conjunto o agrupación de macros existentes dentro de un documento de Word, o una hoja de cálculo de Excel, etc.

MS-DOS (Disk Operating System): Es un sistema operativo, anterior a Windows, en el que se trabaja escribiendo órdenes para todas las operaciones que se desean realizar.

MSDE (Microsoft Desktop Engine): Es un servidor para el almacenamiento de datos, compatible con SQL Server 2000.

MTA (Message Transfer Agent): Es un sistema organizado de correo electrónico que se encarga de recibir los mensajes desde diversos lugares y distribuirlos entre los usuarios. Los MTAs también transfieren los mensajes a otros servidores de correo. Exchange, sendmail, qmail y Postfix son ejemplos de MTAs.

Multipartite: Es una propiedad que caracteriza a determinados virus avanzados. Éstos realizan infecciones utilizando combinaciones de técnicas de infección que otros tipos de virus emplean en exclusiva.

Munging: Técnica para proteger direcciones de e-mail para que no puedan ser recolectadas. Se indica a los destinatarios como decodificar la direccón para que puedan responder a una dirección válida.

Mutex: Técnica utilizada por algunos virus (un mutex) para controlar el acceso a recursos (programas u otros virus) y evitar que más de un proceso utilice el mismo recurso al mismo tiempo. Esto dificulta la detección por parte de los antivirus. Los virus que utilizan mutex pueden incluir otros virus en su interior, al igual que lo hacen otros tipos de virus como, por ejemplo, los polimórficos.

N

Navegador: Un navegador Web o navegador 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 o browsers son: Internet Explorer, Netscape Navigator, Opera, etc.

News: Es el tablón de anuncios electrónico. Permite al usuario identificar la información recientemete incorporada.

Nivel de daños, Daño potencial o Perjuicio: Se trata de un valor que indica el grado de efectos que el virus puede producir en un ordenador afectado. Este dato se emplea para el cálculo del Índice de peligrosidad.

Nivel de propagación o Nivel de distribución: Se trata de un valor que indica cómo de rápido se puede extender o se ha extendido el virus por todo el mundo. Este dato se emplea para el cálculo del Índice de peligrosidad.

Nombre común: Es el nombre por el que se conoce vulgarmente a un virus.

Nombre técnico: Es el nombre real de un virus, utilizado, además, para indicar su tipo o clase.

Nuke (ataque): Caída o pérdida de la conexión de red, provocada de forma intencionada por alguna persona. El ordenador sobre el que se realiza un nuke, además puede quedar bloqueado.

Nuker: Persona o programa que realiza una operación de nuke, provocando el bloqueo de un ordenador o impidiendo que éste pueda acceder a la red donde está conectado.

O

Objeto OLE (Object Linking and Embedding): Es un estándar que permite la incrustación y vinculación de objetos (imágenes, clips de vídeo, sonido MIDI, animaciones, etc) dentro de ficheros (documentos, bases de datos, hojas de cálculo, etc). También hace posible la inclusión de controles ActiveX y la comunicación entre ellos.

Ocultamiento, Ocultación o Stealth: Es una técnica utilizada por algunos virus para intentar pasar desapercibidos ante los ojos del usuario afectado y de algunos antivirus (de forma temporal).

Opt-in (Consentimiento): El proceso de aceptar recibir mensajes desde una fuente comercial. La "doble confirmación" hace referencia al procedimiento de confirmar por segunda vez que quiere apuntarse a la lista de correo.

OS (Operating System): Sistema operativo desarrollado por IBM, anterior al Windows 95 y similar a este en su forma de funcionamiento. Aun teniendo unas muy significativas prestaciones mejores que este, IBM lo retiro del mercado.

P

P2P (Peer to peer): Programas -o conexiones de red- empleados para prestar servicios a través de Internet (intercambio de ficheros, generalmente), que los virus y otros tipos de amenazas utilizan para distribuirse. Algunos ejemplos de estos programas son KaZaA, Emule, eDonkey, etc.

Page-jacking: Se trata del robo del contenido de una Web. Se copian algunas páginas y se colocan en una Web que parece ser legítima y el contenido se incluye en los principales buscadores, de manera que algunos usuarios visiten la página ilegítima.

País de origen: Indica el país o zona geográfica en la que apareció o se tuvo constancia de la existencia de un virus, por primera vez.

Papelera de reciclaje: Es una sección o carpeta del disco duro en la que se guardan los ficheros que se han borrado (siempre que no se hayan eliminado definitivamente).

Parámetro: Es un dato variable que indica a un programa informático cómo debe comportarse en cada situación.

Parche de seguridad: 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.

Partición: Es una de las áreas en las que se puede dividir el disco duro de un ordenador, para que el sistema operativo pueda reconocerla como si de otro disco duro se tratase. Cada partición de un disco duro, puede contener un sistema operativo diferente.

Password o Contraseña: Es una cadena de caracteres con la que se restringe o permite el acceso, de ciertos usuarios, a un determinado lugar o fichero. El ejemplo más habitual es la contraseña de una tarjeta de crédito.

Payload: Son los efectos producidos por un virus.

PDA (Personal Digital Assistant): Es un ordenador portátil de tamaño muy reducido (de bolsillo), que tiene su propio sistema operativo, lleva programas instalados y permite intercambiar información con ordenadores convencional, Internet, etc. Algunos de los más conocidos son Palm, PocketPC, etc.

PE (Portable ejecutable): El término PE (Portable ejecutable) hace referencia al formato de ciertos programas.

Perjuicio, Nivel de daños o Daño potencial: Se trata de un valor que indica el grado de efectos que el virus puede producir en un ordenador afectado. Este dato se emplea para el cálculo del Índice de peligrosidad.

Perl (Lenguaje): Perl es un lenguaje para manipular textos, ficheros y procesos de forma fácil y legible. Podría decirse que Perl está a caballo entre un lenguaje de alto nivel (tipo C) y una 'Commands shell'.

Pesca de información (phishing): Creación de réplicas de páginas Web para "pescar" a usuarios y hacerles enviar información personal, financiera o contraseñas.

Phreaking (Piratería informática): Se trata del acceso ilegal en una red telefónica para hacer llamadas de larga distancia gratuitas o intervenir llamadas.

Pharming: Acción en el que un impostor redirige a los usuarios de Internet desde paginas legitimas a otras fraudulentas.

Phishing: Acrónimo para Password Harvesting Fishing (Pesca y Recolección de Contraseñas). Es un tipo de ataque de ingeniería social, en el cual alguien que pretende ser una fuente confiable engaña al usuario para que desvele información privada (contraseñas, número de tarjeta de crédito, etc.), que será empleada con fines fraudulentos (por ejemplo, suplantación de identidad).

Piratería informática (phreaking): Se trata del acceso ilegal en una red telefónica para hacer llamadas de larga distancia gratuitas o intervenir llamadas

Pista: Es una sección circular existente en cualquier tipo de disco de almacenamiento informático.

Plantilla o Plantilla global: Se trata de un fichero que determina las características iniciales que debe tener un documento, antes de comenzar a trabajar con él.

Plataforma: Hace referencia a un sistema operativo, que funciona en equipos informáticos concretos y bajo unas determinadas condiciones (tipos de programas instalados, etc.).

Plugin: Es un equipo o programa que añade nuevas funciones a un determinado sistema ya existente. Tambien es referido a un determinado trafico de señales en la linea telefonica para identificación.

Polimórfico o Polimorfismo: Es la técnica que utilizan algunos virus para cifrar (codificar) su firma de forma diferente en cada ocasión y además las instrucciones para realizar dicho cifrado.

Política de privacidad: Es el documento que especifica los procedimientos, reglas, y prácticas de seguridad de datos que realiza una empresa, con las que garantiza el mantenimiento de la integridad, confidencialidad y disponibilidad de la información que recoge de sus clientes y de otros interesados titulares de datos, de conformidad con la legislación vigente, las necesidades de seguridad informática y objetivos de negocio que persiga.

POP (Post Office Protocol): Se trata de un protocolo para recibir y obtener los mensajes de correo electrónico.

Prepending: Técnica para infectar ficheros que incluye el código de un virus al principio del fichero infectado. Esto asegura la activación del virus cuando se utiliza o abre el fichero afectado.

Procesador o Microprocesador: Es el corazón electrónico e integrado de un ordenador o sistema informático, popularmente conocido como Pentium (I, II, III, IV,...), 486, 386, 286, 8086, etc.

Programa: Son elementos que permiten realizar operaciones concretas de forma automática (generalmente ficheros con extensión EXE o COM).

Programas antivirus o Antivirus: Son todos aquellos programas que permiten analizar la memoria, las unidades de disco y otros elementos de un ordenador, en busca de virus.

Programa espía: Son aquellos programas que recopilan datos sobre los hábitos de navegación, preferencias y gustos del usuario. Dichos datos son transmitidos a los propios fabricantes o a terceros, cabiendo la posibilidad de que sean almacenados de alguna manera para ser posteriormente recuperados. El Spyware puede ser instalado en el sistema por numerosas vías, a veces sin que medie consentimiento expreso del usuario, así como con su conocimiento o falta del mismo respecto a la

recopilación y/o uso de los datos ya mencionados. El spyware puede ser instalado con el consentimiento del usuario y su plena conciencia, pero en ocasiones no es así. Lo mismo ocurre con el conocimiento de la recogida de datos y la forma en que son posteriormente utilizados.

Protección contra escritura: Es una técnica mediante la cual se permite la lectura del contenido de un disco u otros dispositivos de almacenamiento, pero se impide la escritura de contenido en él (por ejemplo, guardar ficheros).

Protección permanente: Se trata de un análisis continuo que algunos antivirus realizan sobre todos los ficheros que intervienen en cualquier tipo de operación (realizada por el usuario o por el propio sistema operativo). También es conocido como centinela o residente.

Protección proactiva: Capacidad de proteger el ordenador de malware desconocido basándose en su comportamiento, y sin necesidad de disponer de un archivo de identificadores de virus que deba ser periódicamente actualizado.

Protector de pantalla o Salvapantallas: Es un programa que muestra animaciones en la pantalla del ordenador. Su objetivo es que la imagen de la pantalla no quede fija -por ejemplo, cuando el ordenador lleva un rato sin utilizarse-, para evitar que ésta se queme. Actualmente son utilizados por más por razones estéticas o incluso de seguridad.

Protocolo: Es el sistema, reglas y conjunto de normas que establece, gobierna y permite la comunicación entre dispositivos informáticos (la transferencia de datos).

Proxy: Un servidor proxy actúa como un intermediario entre una red interna (por ejemplo, una intranet) y una conexión externa a Internet. De esta forma, se puede compartir una conexión para recibir ficheros desde servidores Web.

Puerta trasera o Backdoor: Se trata de un programa que se introduce en el ordenador y establece una puerta trasera a través de la cual es posible controlar el sistema afectado, sin conocimiento por parte del usuario.

Puesto, Estación o Workstation: Es uno de los ordenadores conectados a una red local que utiliza los servicios y los recursos existentes en dicha red. Por lo general, no presta servicios al resto de ordenadores de la red como lo hacen los servidores.

Puerto de comunicaciones o Puerto: Punto de acceso a un ordenador o medio a través del cual tienen lugar las transferencias de información (entradas / salidas), del ordenador con el exterior y viceversa (vía TCP/IP).

R

RAM (Random Access Memory): Es la memoria principal del ordenador, donde se colocan todos los ficheros cuando se utilizan y todos los programas cuando se ejecutan.

Ratonera: Técnica que utilizan los page-jackers para que los usuarios que han sido engañados en visitar una Web ilegítima solo obtengan páginas adicionales y no solicitadas cuando hacen clic en el botón de "Atrás" para intentar salir.

Ratware: Software que usan los spammers para automatizar campañas de spam, coordinar servicios de spam y generar, enviar y monitorizar mensajes de spam.

RDSI (Red Digital de Servicios Integrados): Éste es uno de los tipos de conexiones de red, utilizados para la transmisión digital de cualquier tipo de información (datos, voz, imágenes, etc.).

Red: Grupo de ordenadores o dispositivos informáticos conectados entre sí a través de cable, línea telefónica, ondas electromagnéticas (microondas, satélite, etc), con la finalidad de comunicarse y compartir recursos entre ellos. Internet es una inmensa red a la cual están conectadas otras sub-redes y a la cual también se conectan millones de ordenadores.

Redireccionar: Acceder a una determinada dirección mediante otra.

Recolección: El proceso de escanear Internet para identificar direcciones de e-mail para crear listas a las que enviar spam.

Recolector de direcciones: Programa que examina páginas Web y filtra mensajes de listas de correo para obtener direcciones de email a las que enviar spam.

Referencia, Salto, Link o Hiperenlace: Estos cuatro términos hacen referencia al mismo concepto. Se trata de elementos o secciones dentro de una página Web (texto, imágenes botones, etc.), que permiten el acceso a otra página o área dentro de la misma página, cuando se pincha sobre ellos.

Registro de Windows (Registry): Es un fichero que almacena todos los valores de configuración e instalación de los programas que se encuentran instalados y de la propia definición del sistema operativo Windows.

Registro Online: Sistema mediante el cual se permite la inscripción (o registro) a través de Internet, como usuario de un determinado producto y/o servicio (en este caso, un programa y sus servicios asociados). Para realizar un registro, es necesario contar con un código de activación o de registro, facilitado previamente por el fabricante del programa. Después de registrarse, se podrá utilizar dicho programa y los servicios que incluye, mediante un nombre de usuario y contraseña (facilitados por el fabricante).

Reinicio: Acción por la cual el ordenador se apaga momentáneamente y se vuelve a encender de inmediato.

Relay abierto: Un servidor de correo SMTP que permite la optención de mensajes por parte de terceros. La función de relay es una parte de los servidores SMTP y tiene usos legítimos, pero los spammers han aprendido cómo localizar servidores desprotegidos y secuestrarlos para enviar spam

Renombrar o Rename: Acción por la cual se da un nuevo nombre a un fichero, directorio u otro elemento del sistema informático.

Réplica: Entre otras acepciones, se trata de la acción por la cual los virus se propagan o hacen copias de sí mismos, con el único objetivo de realizar posteriores infecciones.

Residente o Virus residente: Se denomina fichero o programa residente a todo aquel fichero que se coloca en la memoria del ordenador, de forma permanente, controlando las operaciones realizadas en el sistema.

Riesgo de seguridad: Todo aquello que puede ser utilizado con fines malintencionados para causar perjuicios a los usuarios de un ordenador. Por ejemplo, un programa dedicado a crear virus o troyanos.

Ring: Es el sistema de estados correspondiente a los niveles de privilegio sobre las operaciones que se pueden realizar en el microprocesador, su protección y funcionamiento. Existen varios niveles: Ring0 (administrador), Ring1 y Ring2 (administrador con menos privilegios), Ring3 (usuario).

ROM (Read Only Memory): Es un tipo de memoria en la que no se puede escribir de forma normal, pero que mantiene su contenido de forma permanente (éste no se borra si desaparece la alimentación eléctrica).

Rutina: Secuencia invariable de instrucciones, que forma parte de un programa y se puede utilizar repetidamente.

S

Salvapantallas o Protector de pantalla: Es un programa que muestra animaciones en la pantalla del ordenador. Su objetivo es que la imagen de la pantalla no quede fija -por ejemplo, cuando el ordenador lleva un rato sin utilizarse-, para evitar que ésta se queme. Actualmente son utilizados por más por razones estéticas o incluso de seguridad.

Salto, Referencia, Link o Hiperenlace: Estos cuatro términos hacen referencia al mismo concepto. Se trata de elementos o secciones dentro de una página Web (texto, imágenes botones, etc.), que permiten el acceso a otra página o área dentro de la misma página, cuando se pincha sobre ellos.

Scam (estafa o timo): 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.).

Script : El término script hace referencia a todos aquellos ficheros o secciones de código escritas en algún lenguaje de programación, como Visual Basic Script (VBScript), JavaScript, etc.

Sector: Es una sección de un disco de almacenamiento informático.

Servicio: Es el conjunto de prestaciones que un ordenador o sistema informático facilita a otros sistemas informáticos, o a otros ordenadores que están conectados a él.

Servicios del sistema: Son aplicaciones que normalmente se inician de manera autónoma al poner en marcha el sistema y se cierran, también de manera autónoma, al cerrar el sistema. Los servicios del sistema llevan a cabo tareas fundamentales como, por ejemplo, mantener en funcionamiento el servidor SQL o el detector de servicios Plug&Play.

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.

Shareware: Son versiones de evaluación de un producto software, de uso gratuito, que sirven básicamente para probar el producto antes de adquirirlo definitivamente.

Shell: Intérprete de comandos. Interpreta y activa los comandos o utilidades introducidos por el usuario. Es un programa ejecutable cuya particularidad es que

sirve de interface entre el Kernel y el usuario. Es también un lenguaje de programación.

Síntomas de infección: Son cada una de las acciones o efectos que un virus puede realizar cuando ha producido su infección y además las condiciones de activación.

Síntomas de infección: Son cada una de las acciones o efectos que un virus puede realizar cuando ha producido su infección y además las condiciones de activación (si éste cuenta con ellas).

Sistema de Nombres de Dominio (DNS): Sistema que facilita la comunicación entre ordenadores conectados a una red (o a Internet), su localización, etc, asignando nombres (cadenas de texto más comprensibles) a las direcciones IP de cada uno de ellos.

Sistema operativo (S.O.): Es el conjunto de programas y ficheros que permiten la utilización del ordenador.

SMTP (Simple Mail Transfer Protocol): Es el protocolo que se utiliza en Internet para el envío (exclusivamente) de correo electrónico.

Sobrepasamiento o Tunneling: Es una técnica que utilizan algunos virus para impedir la protección antivirus.

Sobrescritura: Es la acción por la cual un determinado programa o un virus escribe encima del contenido de un fichero, haciendo que se pierda su contenido original y que éste ya no se pueda recuperar.

Software: Son los ficheros, programas, aplicaciones y sistemas operativos que nos permiten trabajar con el ordenador o sistema informático. Se trata de los elementos que hacen funcionar al hardware.

Spam: Es correo electrónico no solicitado, normalmente con contenido publicitario, que se envía de forma masiva. Este tipo de mensajes pueden causar graves molestias y provocar pérdidas de tiempo y recursos.

Spam CSS: Mensaje que utiliza estilos en cascada (Cascading Style Sheets o CSS), que se usa para controlar el aspecto de páginas Web, y ocultar mensajes de spam. Los grupos de spammers también usan CSS para reciclar antiguos trucos basados en lenguaje HTML que engañan a los filtrados de spam que no entienden CSS.

Spam NDR: Mensaje que utiliza una falsa notificación de entrega fallida (non-delivery report o NDR) que el destinatario considera autentica, hecho que le llevará a abrir un adjunto que es spam. Los spammers pueden enviar una NDR directamente o hacer que un servidor legítimo la envíe, de manera que parecerá más creíble.

Spambot: Programa que utilizan los spammers para recolectar direcciones electrónicas desde Internet.

Spammer: Programa que permite el envío masivo de mensajes de correo electrónico con contenido publicitario y la consiguiente recepción masiva de éstos. Puede ser también empleado para el envío masivo de amenazas tales como gusanos y troyanos.

Spawning, Compañía o Virus de compañía: Se trata de un tipo de virus que no se incluye dentro de otros programas, sino que se asocia a ellos.

Spoofing: Se produce cuando grupos de spammers falsifican una dirección de e-mail para ocultar el origen del mensaje de spam. Grupos de timadores por e-mail o creadores de virus también utilizan este método. Los primeros falsifican las direcciones para hacer creer a los usuarios que el e-mail procede de una fuente legítima, como por ejemplo un banco online. Del mismo modo, los creadores de virus han circulado supuestos parches de seguridad, pretendiendo hacer creer que proceden del soporte técnico de Microsoft.

Spyware: Programas que monitorizan secretamente que páginas se visita, lo que puede violar la intimidad y relantizar los ordenadores.

SQL (Structured Query Language): Lenguaje de Consulta Estructurado. Es un lenguaje de programación estándar, destinado a la gestión, administración y comunicación de bases de datos, muy utilizado en la Web (por ejemplo, Microsoft SQL Server, MySQL, etc).

Stealth, Ocultamiento o Ocultación: Es una técnica utilizada por algunos virus para intentar pasar desapercibidos ante los ojos del usuario afectado y de algunos antivirus (de forma temporal).
Subtipo: Cada uno de los subgrupos en los que se divide un tipo. En este caso, grupo de virus o amenazas con características y/o comportamientos comunes, incluida dentro de un tipo o categoría.

Subtipo: Cada uno de los subgrupos en los que se divide un tipo. En este caso, grupo de virus o amenazas con características y/o comportamientos comunes, incluida dentro de un tipo o categoría.

T

Tabla de particiones: Área de un disco que contiene información correspondiente a cada una de las secciones o áreas -particiones- en las que está dividido éste.

Tarpit o Teergrube: Servicio de mensajería deliberadamente lento que pretende localizar a spammers que usan programas de recolección de direcciones

Tarpitting: Monitorización del tráfico de red para identificar las direcciones IP remotas sospechosas de enviar un gran volumen de e-mail. El acceso al sistema de e-mail procedente de direcciones sospechosas de enviar spam se puede reducir o suspender temporalmente.

Tarro de miel: Sistema informático programado para atraer y atrapar a grupos de spammers y hackers. Normalmente se trata de un servidor de correo configurado para aparentar un relay abierto.

Teergrube o Tarpit: Servicio de mensajería deliberadamente lento que pretende localizar a spammers que usan programas de recolección de direcciones.

Terminador de procesos: Programa que finaliza las acciones o procesos que se encuentren en funcionamiento (activos) en un ordenador, pudiendo provocar riesgos de seguridad.

Trampa de spam: Opción preseleccionada por defecto en un formulario online, de manera que los usuarios desprevenidos escojan recibir spam. También hace referencia al filtrado de software que bloquea direcciones de e-mail conocidas por enviar spam.

Transformació3n: Método que usa un spammer para evitar la detección de un programa anti-spam mediante la modificación de la cabecera del e-mail.

Trigger (Condición de activación): Son las condiciones bajo las cuales un virus se activa o comienza a realizar sus acciones en el ordenador infectado

Tipo o Categoría: No todos los virus son iguales. Éstos pueden ser agrupados por características concretas que conforman un tipo concreto de virus.

Trackware: Es todo programa que realiza el seguimiento de las acciones que realiza el usuario mientras navega por Internet (páginas visitadas, banners que pulsa, etc.) y crea un perfil que utiliza con fines publicitarios.

Troyano o Caballo de Troya: En sentido estricto, un troyano no es un virus, aunque se considere como tal. Realmente se trata de un programa que llega al ordenador de manera encubierta, aparentando ser inofensivo, se instala y realiza determinadas acciones que afectan a la confidencialidad del usuario afectado. La historia mitológica El Caballo de Troya ha inspirado su nombre.

TSR (Terminate and Stay Resident): Característica que permite a determinados programas permanecer en memoria, después de haberse ejecutado.

Tunneling o Sobrepasamiento: Es una técnica que utilizan algunos virus para impedir la protección antivirus.

U

UPX: Es una herramienta de compresión de ficheros (Ultimate Packer for eXecutables) que además permite ejecutar los programas que están comprimidos con dicha utilidad, sin necesidad de descomprimirlos.

URL (Uniform Resource Locator): Dirección a través de la cual se accede a las páginas Web en Internet (o a otros ordenadores).

V

Vacunación: Es una técnica antivirus que permite almacenar información sobre los ficheros, con el fin de detectar posibles infecciones de éstos, posteriormente.

Variante: Una variante es una versión modificada de un virus original, que puede infectar de forma similar o distinta y realizar las mismas acciones u otras.

Vector de interrupciones: Es una técnica o utilizada para que un ordenador gestione correctamente las interrupciones que se solicitan al microprocesador. Así se facilita al microprocesador la dirección de memoria a la que debe acceder para dar servicio a la dicha interrupción.

Ventana emergente: Es una ventana que aparece repentinamente, por regla general cuando el usuario selecciona una opción con su ratón o pulsa una tecla de función especial.

Virus: Los virus son programas que se pueden introducir en los ordenadores y sistemas informáticos de formas muy diversas, produciendo efectos molestos, nocivos e incluso destructivos e irreparables.

Virus de boot: Es un virus que afecta al sector de arranque de los discos de almacenamiento.

Virus de compañía, Compañía o Spawning: Se trata de un tipo de virus que no se incluye dentro de otros programas, sino que se asocia a ellos.

Virus de enlace: 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. Después de producirse la infección, es imposible trabajar con el fichero original.

Virus de macro: Es un virus que afecta a las macros contenidas en documentos de Word, hojas de cálculo de Excel, presentaciones de PowerPoint, etc.

Virus residente o Residente: Se denomina fichero o programa residente a todo aquel fichero que se coloca en la memoria del ordenador, de forma permanente, controlando las operaciones realizadas en el sistema.

Vista Previa: Es una característica por la cual los programas de correo electrónico permiten visualizar el contenido de los mensajes, sin necesidad de abrirlos.

Volumen: Es una partición de un disco duro, o una referencia a un disco duro completo. Este término se emplea mucho en las redes de ordenadores donde existen unidades de disco compartidas.

Vulnerabilidades: Fallos o huecos de seguridad detectados en algún programa o sistema informático, que los virus utilizan para propagarse e infectar.

W

WAIS: es un sistema de recuperación de información distribuido. Permite al usuario la búsqueda en bases datos en la red (bases de datos WAIS) usando un interface fácil de usar. Las bases de datos son en su mayoría colecciones de documentos, aunque pueden contener sonido, imágenes o video. WAIS es capaz de buscar por el contenido de un documento. WAIS usa el modelo Cliente/Servidor.

WAN (Wide Area Network): Es una red de área extensa, o grupo de ordenadores encuentran conectados entre sí, pero distantes geográficamente. La conexión se realiza mediante línea telefónica, radioenlaces, o vía satélite).

Web bug (Chivato): Pequeño gráfico insertado en un e-mail o página Web que avisa a un spammer cuando un mensaje se ha leído o previsualizado.

WINS (Windows Internet Name Service): Es el servicio que gestiona los nombres asociados a los ordenadores de una red y, por lo tanto, el acceso y la posibilidad de trabajar con cada uno de ellos. Un ordenador contiene la base de datos con las direcciones en formato IP (por ejemplo, 125.15.0.32) y los nombres comunes asignados a cada ordenador de la red (por ejemplo, SERVIDOR1).

WinZip: Programa de Windows para empaquetar ficheros y de esa forma reducir su ocupación o tamaño.

Workstation, Estación o Puesto: Es uno de los ordenadores conectados a una red local que utiliza los servicios y los recursos existentes en dicha red. Por lo general, no presta servicios al resto de ordenadores de la red como lo hacen los servidores.

Worm (Gusano): Es un programa similar a un virus que, a diferencia de éste, solamente realiza copias de sí mismo, o de partes de él.

WSH (Windows Scripting Host): Es el sistema que permite el funcionamiento de ficheros de proceso por lotes y el acceso a funciones de Windows, mediante lenguajes de programación como Visual Basic Script y Java Script (lenguajes de script).

WWW Robots: Son programas que automáticamente atraviesan el universo WWW recogiendo enlaces. La mayoría de los robots siguen un protocolo muy simple, del cual es fácil proteger a los servidores de su acceso.

WWW (World Wide Web): Servidor de información, desarrollado en el CERN (Laboratorio Europeo de Física de Partículas), buscando construir un sistema distribuido hipermedia e hipertexto. También llamado WEB y W3.

X

XOR (OR-Exclusive): Operación que muchos virus utilizan para cifrar su contenido.

Z

Zip: Es un formato correspondiente a los ficheros comprimidos con la herramienta WinZip.

Zombi: Ordenador o servidor Web no seguro utilizado de forma ilegítima para enviar spam o lanzar un ataque de denegación de servicio.

Zoo (virus de zoo): Son aquellos virus que no están extendidos y que solamente se pueden encontrar en determinados lugares, como laboratorios, donde son analizados para conocer mejor sus características y las técnicas que emplean.

. **(punto):** El signo punto tiene gran importancia en Internet pues se le utiliza en la identificación de todo tipo de direcciones como separador de campos.

@ **(arroba)**: Este signo es uno de los componentes de las direcciones de correo electrónico y separa el nombre del usuario de los nombres de dominio del servidor de correo (ejemplo: nombre@dominio.es

® **"copyright ":** Elemento, programa o rutina con marca registrada y/o derechos reservados.

2: El número "2" ha adquirido un significado muy específico en Internet desde el nacimiento del comercio electrónico en sus diversas modalidades. Dado que el número 2, (two en inglés), tiene en esta lengua una pronunciación muy similar a la preposición to, sustituye a ésta en numerosos acrónimos. (B2B es el acróF3nimo de Business-to-Business).

401 Unauthorized (401 No autorizado): 401 es un código de estado frecuente indicando que un usuario de Web no está autorizado para acceder a una determinada página. Esta y otros códigos de estado, forman parte del protocolo HTTP de WWW.

404 Not found (404 No encontrado): 404 es un código de estado frecuente, indica al usuario que no se ha encontrado (Not found) una determinada página. 404 y otros códigos de estado forman parte del protocolo HTTP de WWW.

Notas:

Comentario Final

Un hombre que estaba prejubilado y quería ocupar parte de su tiempo en un empleo, acude a Microsoft, para solicitar el trabajo de conserje. El gerente de recursos humanos lo entrevista, le hace una prueba (barrer el piso) y le dice:

- "El trabajo es suyo... Déme su e-mail y yo le enviaré un formulario para que lo rellene, y en el mismo mensaje le indicaré la fecha y hora en que deberá presentarse para el trabajo".

El hombre responde que no tiene computador y mucho menos e-mail.

El gerente de recursos humanos le dice que lo lamenta, pero si no tiene e-mail, quiere decir que virtualmente no existe y, como no existe, no puede tener el trabajo.

El hombre sale desconcertado, sin saber que hacer, solamente con un billete de 10€ en el bolsillo. Entonces decide ir al supermercado y comprar una caja de 10 kilos de tomates. Va de puerta en puerta vendiendo los tomates y en menos de 2 horas, había conseguido duplicar el capital.

Repite la operación tres veces más y vuelve a casa con 60€. Entonces, se da cuenta que puede sobrevivir de esa manera, sale de la casa cada día más temprano y vuelve cada vez mas tarde, y así triplica y cuadruplica el dinero cada día.

Poco tiempo después, compra un furgón que más tarde cambia por un camión y transcurrido el tiempo llega a tener una pequeña flota de vehículos de distribución.

Pasan 5 años, el hombre es dueño de una de las más grandes distribuidoras de alimentos del País.

Pensando en el futuro de su familia, decide sacar un seguro de vida. Llama al agente, elige un plan y cuando termina la conversación, el agente le pide su e-mail para enviarle la póliza. El hombre dice que no tiene e-mail. El corredor, sorprendido le dice:

- "Curioso, Vd. que no tiene e-mail, llegó a construir este imperio, imagínese lo que usted sería si tuviese e-mail.

El hombre se queda pensativo y responde:

- "Sería conserje de Microsoft..."

Moraleja 1: Internet no soluciona tú vida.
Moraleja 2: Si tú quiere ser conserje de Microsoft, procura tener un e-mail.
Moraleja 3: Si tú no tienes e-mail y trabajas mucho, puedes ser millonario.
Moraleja 4: Si tú has seguido el contenido de este folleto y realizado las prácticas recomendadas para el manejo de Internet, está más cerca de ser conserje que de ser millonario.
Moraleja 5: En consecuencia, yo que las he escrito y propagado, estoy en las Misma situación.
Moraleja 6: No seremos millonarios... ¡pero cómo nos entretenemos!