COLEGIO OFICIAL DE INGENIEROS DE TELECOMUNICACIÓN

Correo electrónico y SPAM

Colegio Oficial de Ingenieros de Telecomunicación

Grupo de Nuevas Actividades Profesionales

Edita: COLEGIO OFICIAL DE INGENIEROS DE TELECOMUNICACIÓN
C/ Almagro, 2. 28010 Madrid
http://www.coit.es

Depósito legal:
ISBN:

Fotocomposición: Inforama, S.A.
C/ Príncipe de Vergara, 210. 28002 Madrid
Impresión: Ibergraphi 2002, S.L.L
C/ Mar Tirreno, 7bis. 28830 San Fernando de Henares (Madrid)

Presentación del Grupo de Nuevas Actividades Profesionales del COIT (Grupo NAP):

La razón primera de existencia de un Colegio Profesional es el interés social de la actividad que le caracteriza y a la que se debe. Para ordenar la profesión correspondiente dispone de las competencias legales necesarias y para defender ese interés público cuenta con el inmejorable activo de los profesionales que el propio Estado ha formado específicamente para ello, a los que el Colegio agrupa y representa.

Pero es tal el dinamismo de nuestro sector que los campos de actividad que constituyen nuestro ejercicio profesional se incrementan o se modifican cada día; de ahí que, de acuerdo con los fines colegiales, se haya considerado conveniente crear un grupo de trabajo que se ocupe de detectar las nuevas actividades que van surgiendo, de analizarlas y de evaluar su impacto. Así nació, en el año 2003, el Grupo de Nuevas Actividades Profesionales (NAP).

También es misión del Grupo analizar y proponer, en estas nuevas áreas, la conveniencia, o en su caso la obligatoriedad, de contar con la redacción de un proyecto técnico de telecomunicaciones, ya sea por su grado de complejidad, porque soporten servicios de telecomunicación de uso público, porque deban quedar garantizados unos requisitos mínimos de calidad y de seguridad, o bien porque se deba hacer un uso eficaz y eficiente de ciertos recursos públicos limitados en un régimen de mercado plenamente liberalizado.

Estoy convencido de que las líneas de trabajo que mantiene abiertas o tiene previsto abrir este Grupo NAP harán del mismo un foco de atención preferente para nuestros ingenieros y para el sector de las telecomunicaciones.

Francisco Mellado García

Vicedecano del COIT y Fundador del Grupo NAP

NAP

Grupo de Nuevas Actividades Profesionales

Colegio Oficial de Ingenieros de Telecomunicación

Autor: Grupo NAP

Miembros

José Ignacio Alonso Montes

Carlos Franco Beltrán (Coordinador)

Francisco Mellado García

Miguel Pérez Subías

José Fabián Plaza Fernández

Victoria Ramos González

COLEGIO OFICIAL DE INGENIEROS DE TELECOMUNICACIÓN

Correo electrónico y SPAM

Colegio Oficial de Ingenieros de Telecomunicación

Grupo de Nuevas Actividades Profesionales

Editor: Miguel Pérez Subías

PRÓLOGO

Cada vez que cualquiera de nosotros accede a sus cuentas de correo electrónico para recibir los mensajes que necesitamos para nuestra actividad diaria, se encuentra con un auténtico aluvión de correos no deseados que, de forma sistemática, eliminamos sin entrar en sus contenidos.

El correo electrónico es, sin duda, una de las más potentes herramientas que la tecnología ha puesto a nuestra disposición para optimizar procesos y aumentar la productividad individual y colectiva. Mandar mensajes, documentos, fotografías, archivos, desde cualquier lugar del mundo a cualquier otro de forma instantánea y tan económica es de tal trascendencia que ha cambiado, de forma definitiva, los hábitos de todos.

Pero, al tiempo, surge un cada vez mayor problema: impedir todos aquellos mensajes no deseados. Se trata de un problema que está generando un inevitable retraso en el desarrollo de la Sociedad de la Información, por la desconfianza que genera en el ciudadano el hecho de que nuestra intimidad pueda ser tan fácilmente vulnerada.

Nuestro Colegio Oficial está, como siempre, preocupado por agilizar todo aquello que nos facilite el mejor y más rápido acceso de nuestro país a la revolución digital y sus consecuencias en el ciudadano. Ello ha desembocado, en esta ocasión, en la elaboración, por parte de nuestro grupo NAP, de un detallado y, al tiempo, ágil informe sobre el estado de la cuestión, que recoge las mejores recomendaciones y sugerencias para acabar, o minimizar, el fenómeno SPAM en nuestro entorno.

Es, insisto, una aportación más de nuestra profesión, los ingenieros de telecomunicación, para difundir y facilitar las cuestiones fundamentales hacia la sociedad y poner nuestros conocimientos al servicio de la colectividad.

Quiero agradecer tanto a los miembros del NAP como, especialmente, al editor del trabajo y miembro de la Junta directiva de la AEIT, Miguel Pérez Subías, el destacado trabajo que han realizado y que espero sea documento de referencia para todos y de la máxima utilidad para quien lo lea.

Enrique Gutiérrez Bueno

Decano Presidente COIT-AEIT

PRESENTACIÓN

El correo electrónico o e-mail es, sin lugar a dudas, uno de los pilares sobre los que se asienta la Sociedad de la Información, tanto por el número de usuarios como por la frecuencia con que se utiliza. En este momento es una aplicación vital para el funcionamiento diario de empresas y personas. En los últimos años, los usuarios de esta herramienta vienen siendo objeto de continuos abusos: Correo no deseado, virus, suplantación de identidad… Abusos promovidos por aquéllos que se aprovechan de las debilidades (técnicas, de explotación y funcionales) de esta aplicación, así como de las características de Internet (globalidad, bajos costes), y que consiguen sus fines eludiendo responsabilidades y trasladando las consecuencias de los costes de los mismos a los receptores.

Los Ingenieros de Telecomunicación tienen una cuádruple responsabilidad en el desarrollo presente y futuro del Correo Electrónico:

- *Son usuarios avanzados y, por tanto, sufridores habituales de estos abusos, tanto en su trabajo como en su vida privada.*

- *En muchos casos, tienen responsabilidad directa o indirecta en la generación de los contenidos de páginas Web, listas de distribución, publicación de trabajos…*

- *Otros, tienen responsabilidades en la administración de equipos y sistemas conectados a redes IP (entre los que se encuentran sus propios ordenadores personales, así como los de sus amigos, familiares y conocidos).*

- *Finalmente hay Ingenieros que tienen la responsabilidad de abordar los usos del Correo Electrónico desde la regulación, la persecución del fraude o la investigación directamente relacionada con el correo.*

El objetivo de este informe es ayudar, aportando el máximo de conocimiento para todos ellos, sabiendo que cada colectivo tendrá unas necesidades distintas. Ello ha complicado el desarrollo de este trabajo, que para unos resultará demasiado denso y para otros demasiado descriptivo.

En el informe se aborda en primer lugar el funcionamiento, los usos, los protocolos, los agentes que intervienen y las modalidades de correo electrónico, ya que ***sólo su conocimiento nos permitirá avanzar en la búsqueda de soluciones posibles****. Seguidamente se plantea el problema más importante al que se enfrenta el e-mail: El correo no deseado o Spam.* ***Cómo se genera, quién lo produce, qué razones y motivos alientan esta práctica, qué se esta haciendo para combatir este problema*** *en España y en el mundo. Finalmente se analizan las* ***posibles medidas que pueden aminorar o frenar este abuso****. Todo ello se observa desde una triple óptica: Legal, técnica y funcional (usos, hábitos y modelos de negocio).*

*El informe termina con un análisis de las principales **vulnerabilidades** del correo y las técnicas que existen para **prevenir** cada una de ellas. En los anexos se han incluido referencias a las normas técnicas (RFCs) que rigen el funcionamiento del correo entrante y saliente, así como referencias bibliográficas para todos aquellos que necesiten ampliar sus conocimientos sobre este tema. A modo de capítulo final se ha realizado una "**Guía práctica para el Ingeniero de Telecomunicación**" con consejos prácticos para prevenir y evitar abusos en el Correo Electrónico. Pretendemos que esta guía pueda serle de ayuda a este respecto, no sólo en su faceta de usuario, sino también en su faceta profesional.*

Es deseo de todos los componentes del Grupo de Nuevas Actividades Profesionales (NAP) que este trabajo contribuya a desarrollar mejor vuestra actividad personal y profesional, y que redunde en un beneficio para el desarrollo de la Sociedad de la Información, el sector y, por supuesto, de los profesionales que lo conforman.

Carlos Franco Beltrán (Coordinador)

Miguel Pérez Subías (Editor)

INDICE

CAPÍTULO 1. RESUMEN EJECUTIVO

El correo electrónico (e-mail) es, sin duda, uno de los pilares sobre los que se apoya la Sociedad de la Información, cientos de millones de usuarios utilizan en sus ámbitos profesionales y privados esta gran herramienta de comunicación. Sus ventajas son múltiples: Envía con gran rapidez mensajes a un usuario o grupo de usuarios, permite adjuntar archivos, su coste es bajo… Los primeros capítulos de este informe están dedicados al análisis de esta herramienta. Se realizará una clasificación del correo electrónico atendiendo a diversos parámetros, se estudiará la estructura de un mensaje y la arquitectura que sustenta esta tecnología, para ilustrar al lector acerca del funcionamiento de esta aplicación tan cotidiana.

Ante estas múltiples ventajas podría predecirse que el uso del correo electrónico va a crecer en los próximos años, a medida que aumente la penetración de Internet en la sociedad. Sin embargo, sorprendentemente, esta predicción ha de matizarse, la causa es un importante enemigo que ha surgido para restar eficiencia a esta herramienta: El Spam o correo basura.

En estos momentos el e-mail es objeto de un número cada vez mayor de abusos, hasta el punto de que en la actualidad más del 60% de los correos que circulan por la red son correos basura. Los costes asociados a estos abusos, para el año 2004 y según estimaciones de la OCDE, superan los 130.000 millones de dólares. Como abordaremos en el informe, este elevado número de correos basura incide de forma negativa en la confianza de los usuarios y frena el desarrollo de la Sociedad de la Información. Y es que el Spam es la puerta por la que se cuelan más del 90% de las incidencias de seguridad en las empresas y hogares.

Las razones del rápido crecimiento del Spam se encuentran en los bajos costes de entrada (el 98% de los costes son soportados por los receptores), en la posibilidad de ubicar la emisión de Spam en maquinas de terceros (a través de virus, servidores mal configurados o alojados en máquinas de países dónde esta práctica no esta penalizada) y en la falta de seguridad del protocolo utilizado en el envío y la recepción del correo (POP y SMTP).

Aunque resulte sorprendente hay agentes que están claramente a favor de estas prácticas: Los que directamente practican el Spam, los que crean herramientas y servicios para los Spammers, y los que trafican con bases de datos y direcciones. En el otro extremo se encuentran los gobiernos de países industrializados, las empresas y los usuarios que claramente están en contra de estos abusos. Como siempre, hay una zona intermedia en la que podemos ubicar a los que se benefician indirectamente de esta situación: Empresas que proveen soluciones y servicios para combatir el Spam, y organizaciones de marketing directo que ven en el correo electrónico una gran herramienta de marketing, siempre que se use de forma adecuada.

Las propuestas de tipo técnico que intentan acabar con el Spam, para ser efectivas, requieren una cierta coordinación entre la industria, ya que de nada sirven actuaciones que sólo sean puestas en marcha por un pequeño grupo de usuarios. Por otro lado, es necesario hacerlas compatibles con el protocolo actual, que no está preparado para incorporar funciones que aumenten su seguridad. Esta última característica provoca grandes problemas a los administradores de sistemas y un cierto desasosiego por la falta de medidas que eviten el problema en su origen.

La mayor parte de los avances técnicos se centran, en consecuencia, en aminorar los efectos del Spam una vez que se ha recibido. Esto no evita su crecimiento, provocando además una alocada carrera "técnica" entre los Spammers y los que administran los servidores de correo, la cual parece no tener un final cercano.

En el ámbito legislativo las iniciativas en el contexto europeo intentan prohibir el correo no solicitado, salvo que el usuario lo autorice al emisor (opt-in). En EE.UU. se ha optado por permitir el correo no solicitado, salvo que el usuario indique lo contrario apuntándose en alguna lista de control (opt-out).

En los países industrializados hay una tendencia a endurecer las medidas legislativas y los castigos de quienes las infrinjan, dotando para ello de recursos a los que deben ocuparse de las labores de investigación e inspección en los diferentes gobiernos.

La cooperación internacional ha empezado a reaccionar en el último año y en este momento ya hay iniciativas en la OCDE, la ITU, la UE, EE.UU., IETF y en foros empresariales. El inconveniente es que éstas adolecen de un espacio o punto de encuentro común a todas ellas y, sobre todo, les falta capacidad de influencia para que determinadas propuestas se lleven a la practica en los diferentes agentes de cada país, lo cual resta eficiencia a todas ellas. A esto debemos sumar la posición de los países en vías de desarrollo que se convierten en focos emisores de correo basura, por la facilidad de ubicar negocios relacionados con estas prácticas en sus ámbitos geográficos.

En el caso de España, la responsabilidad de la regulación en materia de e-mail recae en el Ministerio de Industria (antes de Ciencia y Tecnología) que literalmente prohíbe el envío de correo no solicitado en la LSSI aprobada en 2002, mientras que la inspección y persecución de abusos corresponde en la actualidad a la Agencia de Protección de Datos.

En lo que respecta a la concienciación y coordinación de acciones contra el Spam, éstas siempre han estado promovidas desde el ámbito de los usuarios (iniciativa PePi-II.com de la Asociación de Usuarios de Internet), de la universidad (proyecto ACE de Red Iris) y de las redes informales de administradores de sistemas, que han buscado espacios de intercambio de ideas y opiniones a través de listas de correo temáticas.

Actuaciones y propuestas

No hay una solución mágica en el corto plazo contra el "Spam" y otros abusos relacionados con el e-mail, pero sí existen algunas formas de aminorar sus efectos.

Es necesario crear puntos de encuentro entre todos aquéllos que quieren combatir estos abusos. Asimismo es importante que este asunto se convierta en una prioridad para los que tienen la responsabilidad de desarrollar la Sociedad de la Información en cada país. El intercambio de experiencias y conocimientos entre los sectores público, privado y los propios usuarios debe enfocarse con criterios de efectividad para conseguir aminorar sus efectos.

Las medidas para combatir los abusos en el correo deben agruparse en los siguientes frentes:

- **Educación y sensibilización de los usuarios de correo electrónico**: Deben conocer cómo protegerse, evitar ser blanco de los Spammers y ser capaces de reaccionar adecuadamente ante los abusos.

- **Soluciones tecnológicas**: De especial importancia para aquellos que tienen la responsabilidad de administrar los servidores de las organizaciones y los servicios de correo (webmail, listas de correo, contenidos), ya que ellos son los que permiten el envió y los que reciben los correos antes de entregárselos a sus usuarios y clientes.

- **Regulación y autorregulación**: Los gobiernos son responsables de legislar y hacer que las leyes se cumplan. También pueden ser un catalizador para que surjan propuestas de autorregulación entre los agentes que participan en la cadena de valor.

- **Coordinación internacional**: Estamos en una red global y sólo las acciones soportadas por un conjunto de países de forma coordinada pueden hacer que determinadas prácticas (legislativas y tecnológicas) se adopten en el conjunto de la red.

CAPÍTULO 2. EL CORREO ELECTRÓNICO, UNO DE LOS PILARES DE LA SOCIEDAD DE LA INFORMACIÓN

Internet está, poco a poco, pasando a ser parte integral de nuestro desarrollo. Su uso y aplicaciones siguen experimentando un crecimiento exponencial en todos los países industrializados, pronto se superarán los 1.000 millones de usuarios en todo el mundo.

Uno de los pilares que sustenta el desarrollo de Internet es el correo electrónico o e-mail, hasta el punto de que algunos la consideran como la aplicación de referencia ("killer application"). Su funcionalidad y sencillez lo han convertido en una herramienta de comunicación en todos los ámbitos: Personal, financiero y administrativo.

Las **facilidades que aporta el e-mail** frente a otros sistemas son, fundamentalmente:

- No requiere una presencia simultánea de los dos extremos de la comunicación (como sí ocurre en el caso del teléfono o la mensajería instantánea)
- Permite una comunicación personal frente a otros sistemas
- Resulta más barato que otros sistemas
- Es fácil de utilizar
- Posibilita su uso desde diferentes dispositivos
- Admite su uso en movilidad (terminales móviles) y con ubicuidad (desde diferentes terminales)

El e-mail es **una de las primeras aplicaciones que aparece en Internet**, anterior incluso al html y a la navegación web tal y como la conocemos en este momento. En sus orígenes, los usuarios del correo electrónico pertenecían a comunidades y grupos de usuarios e investigadores bastante reducidos y con un alto nivel de confianza entre ellos.

Quizás por esta razón no se plantearon mecanismos de seguridad o autenticación que evitasen los abusos que se están produciendo en la actualidad. La popularización del uso del correo electrónico ha traído consigo el incremento exponencial de aquéllos que hacen un mal uso del mismo.

En estos momentos **más del 67% de los correos que circulan por la red son correos no deseados, popularmente conocidos como correos basura o "Spam"**. El Spam está haciendo incurrir a proveedores y usuarios en un nivel de molestias y gastos que en algunos casos obliga incluso a cerrar empresas y cuentas de correo.

Más del 80% de los problemas de seguridad que hay en los ordenadores, y un porcentaje alto de los timos y estafas que sufren los usuarios de Internet, tienen como origen un programa, un mensaje o un ataque que se ha propagado o iniciado a través del correo electrónico.

Los que abusan se amparan en la debilidad de los protocolos de correo, la globalidad, las diferencias en las legislaciones y el bajo coste que tiene el envío masivo (por lo general, casi siempre es el que recibe el que carga con el coste).

En estos momentos el problema, lejos de remitir, sigue creciendo. Si no se toman medidas de forma coordinada entre técnicos, legisladores, proveedores y usuarios, probablemente nos encontremos con graves dificultades para continuar utilizando el correo electrónico.

En la actualidad el número de mensajes de correo basura se ha duplicado. La media está en **29 por empleado** y esto a pesar de que las empresas **filtran más del 60% del Spam** que reciben. Se calcula que el coste medio por empleado y año del correo basura **supera los 1.500 euros**.

CAPÍTULO 3. TIPOS DE CORREO ELECTRÓNICO

Existen varias clasificaciones del correo electrónico en función del parámetro al que se atienda. En este capítulo se analizan cuatro posibles agrupaciones, presentadas de forma esquemática en la siguiente figura.

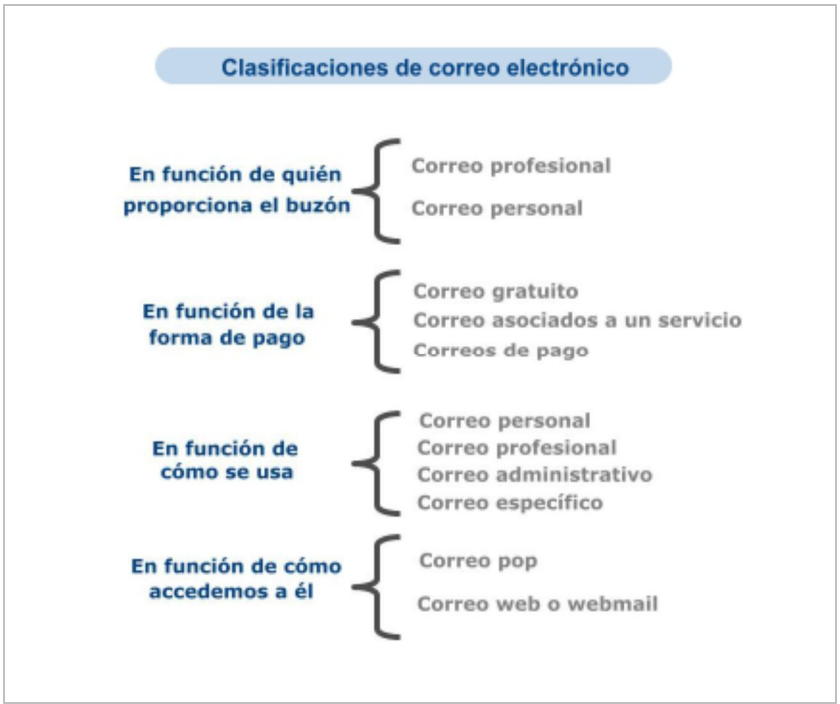

Figura 1

3.1. En función de quién proporciona el buzón

Podemos realizar una primera clasificación atendiendo a quién proporciona el buzón o cuenta de correo:

- **Correo profesional:** Facilitado por las empresas y organizaciones a las personas que se relacionan con ellas. Se subdivide a su vez en:
  - **Correos impersonales:** Representan a la organización o a su estructura funcional: prensa, ventas, redacción, administración, clientes, soporte, webmaster… Son del tipo: informacion@almacenes.com
  - **Correos individuales**: Identifican a quién lo utiliza por su nombre, apellidos, nombre.apellidos… Son del tipo: luis.perez@almacenes.com
- **Correo personal:** Contratado por una persona a título individual.

3.2. En función de la forma de pago

Otra clasificación puede tener como origen el pago o no de este servicio por la persona que lo utiliza. En este caso los tipos de correo que encontramos son los siguientes:

- **Correos gratuitos:** No tienen ningún coste para quien los utiliza. En general suelen tener una carga publicitaria importante, visible desde el programa o aplicación que nos permite su uso. También es posible que la publicidad se sitúe en los propios mensajes que enviamos.

- **Correos asociados a un servicio:** Facilitados a los usuarios de un producto o servicio (acceso a Internet, clientes de un banco, consumidores de un hiper, socios de un club…).

- **Correos de pago:** Contratados directamente por el usuario. Pueden ser una opción dentro de otro servicio pagado por el usuario, o bien pueden adquirirse individualmente.

3.3. En función de cómo se usa

Una cuenta de e-mail podemos utilizarla para fines:

- **Personales**

- **Profesionales**

- **Administrativos**

- **Específicos** (utilizamos el buzón para un solo fin: Suscribirnos a una lista, comprar en un sitio web, acceder a una determinada página web...)

Muchas veces estos usos se entremezclan y nos encontramos con personas que utilizan una misma cuenta para dos o más fines, debido a la complejidad que significa mantener diferentes identidades, con claves de acceso separadas.

En general, **cada vez está más extendido el uso de cuentas gratuitas de uso específico** cuando el sitio, lista o servicio al que se va a suscribir el usuario no le inspira la suficiente confianza.

Las posibilidades de uso del correo son tan amplias como las del teléfono, el correo tradicional o el fax.

3.4. En función de cómo se accede a él

Existen dos formas de acceder al correo electrónico:

Correo POP:

En este caso el usuario **se conecta desde un dispositivo** (su ordenador personal, por ejemplo) **al servidor que gestiona su buzón, para descargarse el correo recibido y/o enviar el saliente**. El servidor hace las veces de almacén intermedio en el que se conserva el correo que va recibiendo el usuario hasta que éste lo descarga. Una vez descargado, los mensajes se suelen borrar. Algunos dispositivos, como las aplicaciones en movilidad, permiten leer el correo sin que éste se borre.

Para su correcto funcionamiento, **el correo POP necesita disponer de un programa en el ordenador/dispositivo del usuario.** Los programas más conocidos son Outlook, Eudora, Lotus… Asimismo requiere que el ordenador/dispositivo del usuario esté conectado a Internet o a una red corporativa.

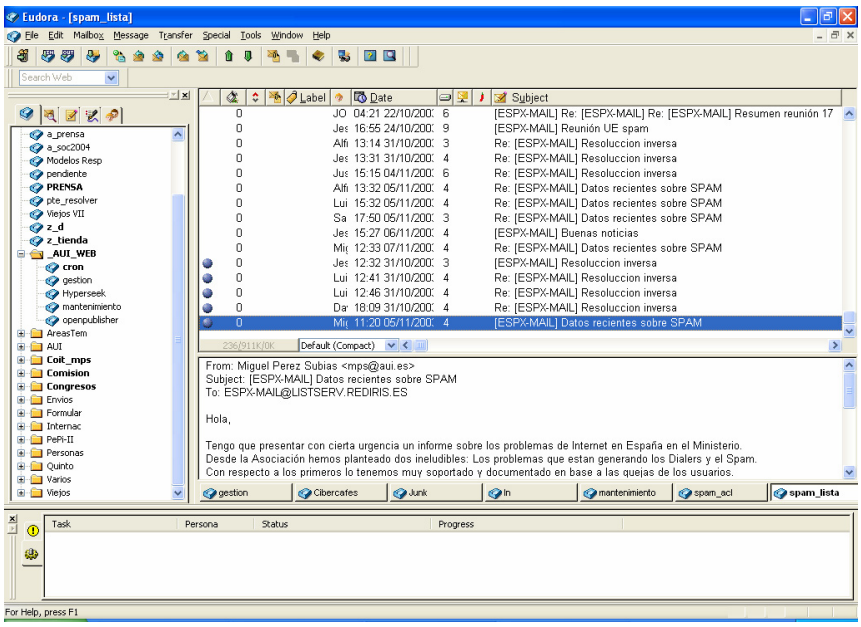

Figura 2

Correo web o WebMail:

En este caso, **el usuario se conecta directamente a través de su navegador web al servidor**. Éste le permite, desde una interfaz en el propio navegador, gestionar todo su correo (leer, escribir, descargar…). La información en este caso se queda en el servidor.

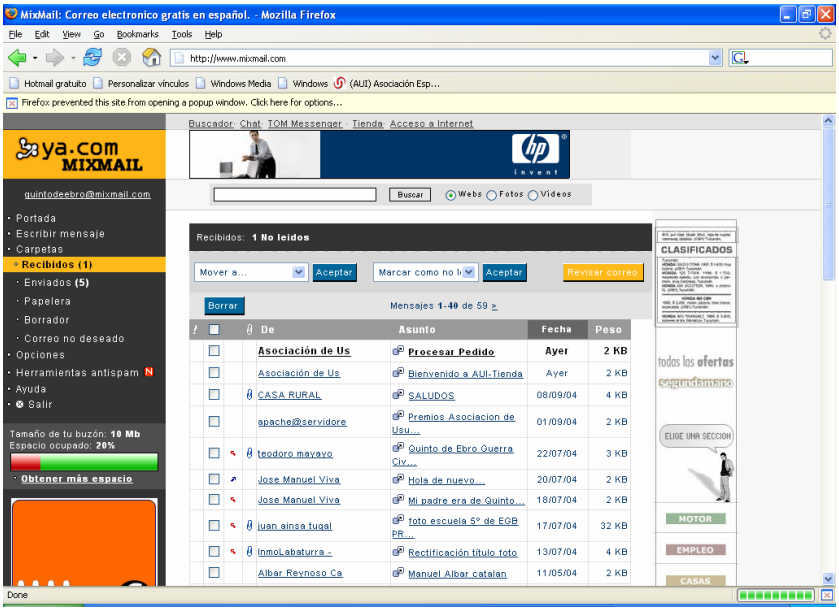

Figura 3

Cada vez hay más **servicios mixtos** que permiten al usuario decidir cómo utilizar su correo. Así por ejemplo, si está en movimiento recurrirá a las soluciones webmail por su comodidad y accesibilidad. En la oficina, en cambio, resultará más confortable utilizar el correo pop

El **control de acceso al buzón** suele estar basado en una identificación del usuario (en general es el propio e-mail o lo que hay a la derecha de la @, dependiendo de los programas) y una clave de acceso o password. Son muchos los programas que permiten cambiar la clave si somos capaces de responder a una pregunta cuya respuesta hemos grabado previamente.

Los servidores **pueden y deben aplicar políticas de uso** que garanticen y comprometan un correcto uso de este servicio.

CAPÍTULO 4. FUNCIONAMIENTO DEL CORREO ELECTRÓNICO

El correo electrónico es una herramienta cotidiana que forma parte de la rutina diaria, personal y profesional, de millones de personas. Sin embargo, pocas veces sus usuarios se detienen a pensar cómo funciona técnicamente y qué arquitectura lo soporta. Dedicaremos el próximo capítulo al análisis de su funcionamiento.

4.1. Un poco de historia

Comenzaremos este capítulo rememorando la aparición del correo electrónico. El programa SNDMSG (Send Message) es el precursor del SMTP, empleado en el año 1971 por Ray Tomlinson (junto con su propio proyecto CYPNET), para la creación de una aplicación que permitiera el envío del correo electrónico dentro de la red ARPANET. Un año más tarde, el programa utilizado en Arpanet para el envío de ficheros (FTP), fue ampliado con el comando MAIL y MLFL.

Hasta el año 1980 el correo era enviado por medio de FTP. Fue en aquel año cuando nació el primer protocolo estándar de correo electrónico, MTP (Mail Transfer Protocol), descrito en el documento RFC 772. MTP sufrió varias modificaciones (RFC 780, 788) y en el año 1982, en la RFC 821, Jonathan B. Postel describió el Simple Mail Transfer Protocol.

Desgraciadamente, el SMTP en su forma básica no cumplió todas las esperanzas. De ahí que surgieran muchos documentos que describían la extensión del protocolo. Entre los más importantes podemos destacar:

- **RFC 1123:** Exigencias para los servidores de Internet (también abarca SMTP).
- **RFC 1425:** Introducción del estándar de las extensiones del protocolo SMTP – ESMTP.
- **RFC 2505:** Conjunto de sugerencias sobre protección antiSpam de los servidores.
- **RFC 2554:** Autorización de las conexiones – introducción del comando AUTH.

El actual estándar SMTP fue descrito en el año 2001 en RFC 2821.

4.2. Estructura de una dirección de correo

Una dirección de correo se compone de dos partes:

- **Identificador del usuario o del buzón del usuario:** Utilizado para depositar el correo que llega a un dominio determinado en su buzón correspondiente. Es la parte anterior al símbolo @.
- **Identificador del dominio al que pertenece el correo electrónico**: Utilizado para encaminar el correo a su destino, mediante una consulta MX al DNS. Parte posterior al símbolo @.

Una dirección cualquiera de correo electrónico queda entonces determinada de la siguiente forma: **Usuario@dominio**

4.3. Estructura de un mensaje de correo

Básicamente un mensaje de correo está dividido en tres partes (según la RFC 2822):

- **Cuerpo del mensaje:** Contenido en sí del correo. En él se encuentra la información útil que se intercambian el remitente y el destinatario.
- **Encabezados del mensaje:** Información que se encuentra precediendo al cuerpo del mensaje. Enuncia los datos del remitente, los lugares por donde ha ido pasando el correo, los programas utilizados para su envío...
- **Envoltura del mensaje:** Equivale al "sobre" del mensaje. En ella se encuentra la información del destinatario, que será utilizada por las máquinas para hacer llegar el correo a su destino.

En el Anexo 1 de este documento, dentro del resumen de la normativa RFC 2822, se puede encontrar un análisis más detallado de cada una de las partes del correo electrónico. Se especifica detalladamente los principales encabezados del mensaje, su funcionalidad y cómo se generan.

4.4. Arquitectura del correo electrónico

En el funcionamiento del servicio de correo electrónico intervienen tres componentes:

1. Agentes de usuario (UA)

- Clientes

2. Agentes de transferencia de mensajes (MTA)

- Servidores

3. Almacenes de mensajes (MS)

- Buzones

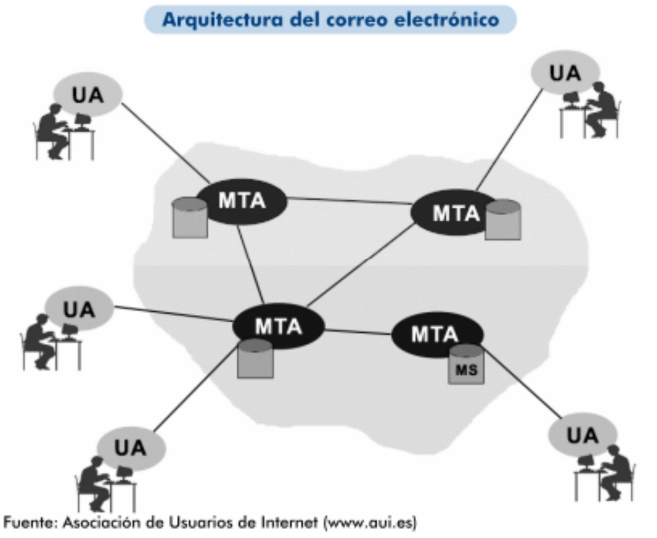

Figura 4

Agentes de usuario

¿Qué son?

Los agentes de usuario son los **clientes o lectores de correo instalados en los ordenadores personales**. Estas aplicaciones permiten gestionar el correo electrónico de una forma sencilla, proporcionando los servicios para componer o editar mensajes. Pueden estar dotados de una interfaz gráfica (Eudora, Outlook, Pegasus...) o de texto (pine).

Funciones:

La principal función de estos programas es la de **interaccionar con los MTA (Agentes de Transferencia de Mensajes)**, entregándoles los mensajes que el usuario desea enviar para que éstos sean remitidos a su correspondiente dirección de destino. También se encargan de **aceptar el correo que llega al usuario.**

Tipos de programas utilizados por los usuarios:

Existen gran cantidad de programas para enviar y recibir correo electrónico. Algunos de los más conocidos y utilizados son: **Outlook, Eudora, Pegasus, Netescape Messenger...** Todos ellos permiten configurar las direcciones de los servidores SMTP para el envío de correo, y de los POP3 para la recogida de los mensajes. A su vez, también llevan incorporado un cliente IMAP que posibilita gestionar directamente los mensajes del buzón sin tener que descargárselos en el PC local.

Webmail:

Como se avanzó en el capítulo anterior, el webmail **no requiere ninguna configuración especial ni tener instalados programas adicionales**. Accede al correo a través del navegador http, siempre que el proveedor de correo ofrezca este servicio.

Agentes de transferencia de mensajes

¿Qué son?

Los agentes de transferencia de mensajes, MTA (Message Transfer Agents), son los **servidores de correo**.

Funciones:

Tienen dos funciones principales:

1. Encaminar los mensajes hacia su destino final
2. Mantener los buzones de usuarios

Para encaminar los mensajes hacia los servidores destinatarios y comunicarse entre ellos, utilizan el **protocolo SMTP**. Cuando el correo llega a su destino, el servidor de correo almacena este mensaje en el buzón que tiene el usuario, que se encuentra físicamente localizado en la máquina que hace las funciones de MTA.

Para poder leer el correo existen tres protocolos posibles:

- El **POP3 y el IMAP,** si se tienen los programas apropiados
- El **http,** si el proveedor ofrece webmail

También se encargan de gestionar las colas de salida.

Tipos de programas utilizados por los servidores:

Hay una gran variedad de programas que permiten montar un servicio de correo. Los más extendidos en Internet son los basados en **UNIX**. La mayoría de ellos son de libre distribución (Sendmail, Postfix, Qmail, Exim...) También los hay basados en **Microsoft Windows** (NTMail, Exchange y otros).

Almacenes de mensajes

Los almacenes de mensajes, MS (Message Store), son los **buzones donde se almacenan los correos cuando llegan a su destino**. Mediante los protocolos POP3 o IMAP el agente de usuario (programa de correo) interacciona con el servidor de correo para acceder a su buzón correspondiente.

Como se ha comentado anteriormente, también existe la opción de leer los mensajes utilizando el navegador de Internet, siempre que el proveedor de correo ofrezca webmail, sin utilizar una agente de usuario específico.

4.5. Correo saliente: Envío de correos

En los próximos apartados se explica el funcionamiento del correo saliente y los protocolos que intervienen en el proceso: Cómo se van rellenando cada una de las cabeceras y la forma de interpretarlas. Finalmente se presentan varios ejemplos prácticos.

¿Cómo funciona?

En el envío de correo electrónico intervienen principalmente tres protocolos: El SMTP, otro que especifica el formato de los mensajes, y el MIME, descritos en las RFC 2821, RFC 2822 y RFC 2045 respectivamente.

El primer paso para enviar un mensaje es **comunicarse con el servidor de correo**, siguiendo los pasos indicados por el protocolo SMTP, en la RFC 2821 (ver Anexo 1). El protocolo contempla un **proceso de identificación** a través de los comandos HELO o EHLO. Este proceso no es realizado correctamente por la mayoría de los servidores, lo que ha provocado que en muchos casos no se llegara finalmente a realizar esta identificación. Esto está cambiando debido a la profusión del Spam. En cualquier caso, lo que sí que queda reflejado es la IP del host origen en el servidor. La dirección de correo que especifica el remitente tampoco es verificada. La dirección destino, especificada en el comando RCPT TO:, ha de ser correcta.

Existen algunos servidores que ya realizan ciertas comprobaciones para verificar la identidad de los clientes que utilizan sus servidores SMTP. Esto será estudiado con mayor detalle en el capítulo 8.

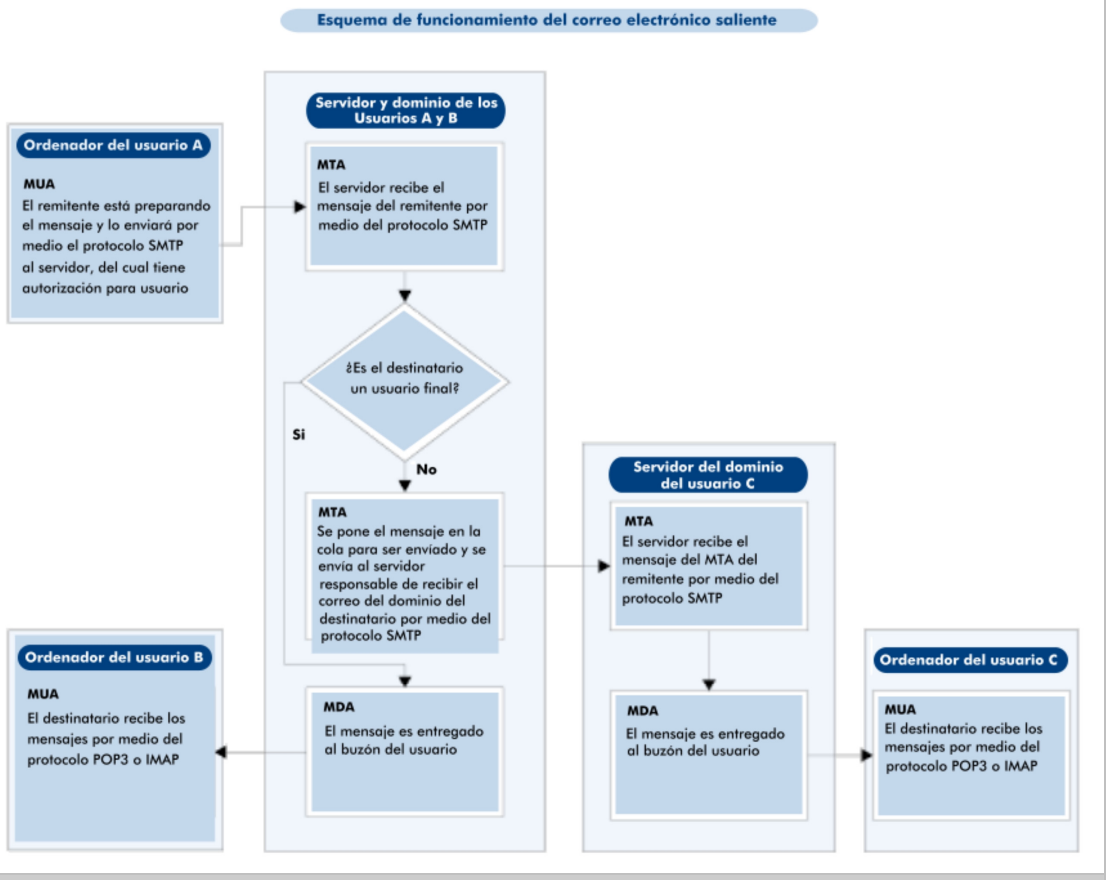

Figura 5

Una vez establecida la comunicación, que es equivalente a crear la envoltura del mensaje, sólo queda **crear los encabezados y el cuerpo del mensaje**. Esto es llevado a cabo por el agente usuario (programa de correo) que se esté utilizando. Éste se encarga de poner las cabeceras correspondientes establecidas por la RFC 2822, haciendo coincidir, si no se especifica otra cosa, los campos Form y To con los especificados en MAIL FROM: y en RCPT TO: respectivamente. Por otro lado, **le da el formato correspondiente al texto del mensaje y al contenido del mismo (archivos adjuntos…),** siguiendo el estándar MIME descrito en la RFC 2045.

Una vez que el mensaje es entregado al servidor SMTP, éste **pondrá una cabecera Message-ID y otra Received al principio del mismo**, y se lo entregará a otro servidor de correo, utilizando para esta comunicación el protocolo SMTP.

El segundo servidor SMTP comprueba la dirección de correo que se ha pasado en el RCPT TO: para **redireccionar ese mensaje a su destino** (no modifica las cabeceras del cuerpo del mensaje, Form, To**…**), **y añade una cabecera Received** encima de la que puso el anterior. Estos pasos se repetirán tantas veces como sea necesario hasta que el correo llegue a su destino.

4.6 Interpretación de las cabeceras de los mensajes

A continuación se muestra la cabecera estándar, visible cuando se abre un mensaje de correo electrónico, y la cabecera de forma extendida:

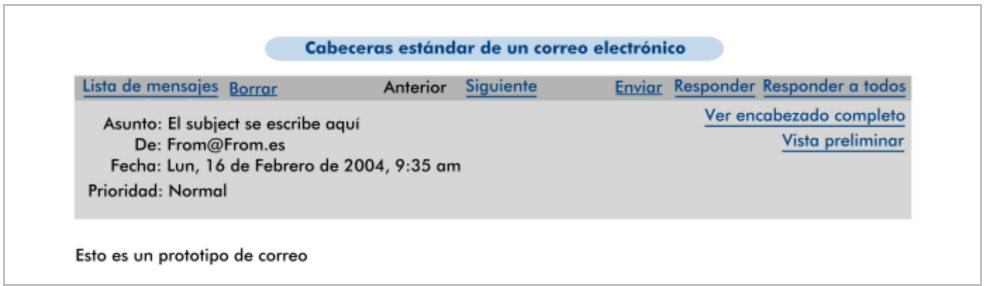

Figura 6

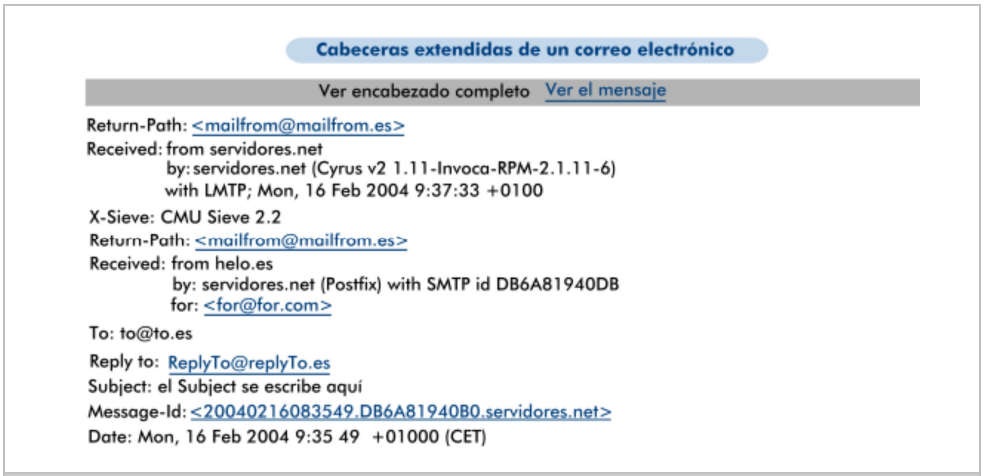

Figura 7

En la figura 6 se pueden observar las cabeceras principales de un correo electrónico (definidas en la RFC 2822). Los datos mostrados se corresponden con un correo real. El campo **De**, From@From.es, es el que hace referencia a la cabecera From. El campo **Para**, To@To.es, se corresponde con la cabecera To.

Si nos fijamos en la Figura 7 (la misma cabecera presentada en la Figura 6 pero extendida) se pueden ver todos los demás campos que se han especifican en el resumen de la RFC 2822 (ver Anexo 1). En el campo de **Return-Path** aparece la dirección del remitente que se especificó en la transacción SMTP con el comando MAIL FROM: (mailfrom@mailfrom.es), que no tiene que coincidir obligatoriamente con el contenido de la cabecera From (from@from.es). Se puede ver que este campo tampoco tiene que ser el mismo que se especifica en **Reply-To** (ReplyTo@ReplyTo.es).

Los campos que realmente nos dan información sobre la procedencia del mensaje son los etiquetados como **Received**. En el correo presentado en la Figura 7 se observa que hay dos cabeceras con este nombre, lo cual indica que el mensaje ha pasado por dos servidores de correo, uno en el de salida y otro el de entrada.

La primera de las cabeceras Received corresponde al servidor de destino. La segunda cabecera es la más importante, y corresponde, en este caso, con la del servidor origen. La información proporcionada en estas líneas es sumamente útil, ya que la dirección IP que aparece al final de la primera línea es la del host origen. El nombre helo.es es como dice llamarse ese host. La dirección de correo que aparece en la tercera línea encerrada entre los signos "< >" precedida de la palabra from es la dirección real a la que va dirigida el mensaje (en teoría debería aparecer en la cabecera To del mensaje).

La forma de visualizar las cabeceras de un mensaje de correo electrónico depende del gestor de correo que se utilice pero todos lo permiten. Así, por ejemplo, si se usa Outlook Express, se puede lograr señalando el mensaje y pulsando "Control-F3".

Ejemplo de envío de un correo

En la Figura 8 se muestra un ejemplo de utilización del protocolo SMTP en el envío de un correo electrónico. Concretamente la secuencia de comandos que se puede observar corresponde al correo que aparece en las Figuras 6 y 7. Éste no es el proceso que tiene que hacer un usuario para enviar su correo, sino que son los pasos que realiza el programa de correo que utiliza. Dependiendo de la configuración de éste, los campos se rellenarán con un valor u otro.

Secuencia de comandos SMTP para el envío de un correo

```
220 .servidoresdns.net ESMTP Postfix
helo helo.es
502 Error: command not implemented
helo helo.es
250 .servidoresdns.net
mail from:mailfrom@mailfrom.es
250 Ok
rcpt to:@pepi-ii.com
250 Ok
data
354 End data with <CR><LF>.<CR><LF>
From:From@From.es
To:To@To.es
Reply-To:ReplyTo@ReplyTo.es
Subject:El Subject se escribe aqui

Esto es un prototipo de correo
.
250 Ok: queued as DB6A8194ODB
```

Figura 8

4.7. Correo entrante: recepción de correo

A continuación se describen las opciones existentes para acceder al correo recibido.

¿Cómo funciona?

Existen dos protocolos para tener acceso al correo recibido: Protocolo POP3 y Protocolo IMAP.

El protocolo **POP3** es el más sencillo. Sus siglas hacen referencia a Post Office Protocol (protocolo de correo de oficina) y su funcionalidad es la de descargar los mensajes del buzón del usuario, residentes en el servidor de correo. Con este protocolo sólo se pueden leer los mensajes recibidos en el ordenador desde el cual se han recogido.

El protocolo **IMAP** (Internet Message Access Protocol), sirve para gestionar el correo recibido, sin necesidad de descargarlo al ordenador desde el que se accede para poder leerlo. Este protocolo ofrece la posibilidad de gestionar el correo dentro del propio servidor. Con una serie de instrucciones se pueden crear diferentes carpetas para almacenar los mensajes, moverlos entre carpetas, leerlos, ver las cabeceras, marcar aquellos que están leídos... Es posible realizar exactamente las mismas tareas que permite desarrollar un servicio de webmail.

Estos dos protocolos **requieren autenticación por parte del usuario para permitirle acceder a su buzón de correo**, por lo que son relativamente seguros. Existen otras dos versiones extendidas de los protocolos, denominadas **POP3S (POP3 Seguro)** e **IMAPS (IMAP Seguro)**, que utilizan encriptación de los datos intercambiados con el servidor para que un posible programa que capturara tráfico de la red no interceptara la contraseña y el login del usuario, o el contenido del mensaje.

Ejemplo de recepción de correo

A continuación se presentan dos ejemplos ficticios de utilización de los protocolos POP3 e IMAP. Se trata de los **pasos que seguirían los programas de correo utilizados por el usuario para recoger y leer los mensajes**.

Las líneas que comienzan con **C:** son los comandos que introduce el programa de correo y las que comienzan con **S:** son las respuestas del servidor. Se puede apreciar que en ambos ejemplos **se requiere introducir un login y una contraseña** (*líneas en negrita*) para tener acceso al contenido del buzón.

El significado de los comandos utilizados puede consultarse en los resúmenes de protocolo POP3 e IMAP (RFC 1939 y RFC 2060) que se encuentran en los Anexos 3 y 4, respectivamente.

Utilización de POP3:

C: telnet servidorPOP3 110
S: +OK POP3 server ready
C: user miusuario
S: +OK Name is valid mailbox
C: pass mipasword
S: +OK Maildrop locked and ready
C: list
S: 1 1755
S: 2 2362
S: 3 8483
C: retr 1
S: (blah blah ...
S: .....
S: .....blah)
S:.
C: dele 1
C: retr 2
S: (blah blah ...
S: .....
S: .....blah)
S:.
C: dele 2
C: retr 3
S: (blah blah ...
S: .....
S: .....blah)
S: .
C: dele3
C: quit
S: +OK POP3 server signing off

Utilización de IMAP:

C: telnet servidorIMAP 143

S: * OK IMAP server ready

C: 001 LOGIN miusuario mipassword

S: 001 OK User loged in

C: 001 LIST “” *

S: * LIST (\Noinferiors) “/” “INBOX”

S: * LIST (\HasNoChildren) “/” “Enviados”

S: * LIST (\HasNochildren) “/” “Pendientes”

S: 001 OK Completed

C: SELECT “INBOX”

S: * FLAGS (\Answered \Flagged \Draft \Deleted \Seen)

S: * OK [PERMANENTFLAGS (\Answered \Flagged \Draft \Deleted \Seen *)]

S: * 106 EXISTS

S: * 0 RECENT

S: * OK [UIDVALIDITY 1075711479]

S: * OK [UIDNEXT 123]

S: 001 OK [READ-WRITE] Completed

C: FETCH 1 (BODY[TEXT])

S: (blah blah ...

S: .....

S: .....blah)

S: 001 OK Completed

C: 001 LOGOUT

CAPÍTULO 5. SPAM, LA AMENAZA A LA SUPERVIVENCIA DEL CORREO ELECTRÓNICO

En los capítulos precedentes se ha presentado el correo electrónico como uno de los principales recursos de la Sociedad de la Información. Sus ventajas son múltiples y su coste escaso, de esta combinación surge seguro su enorme popularidad. Sin embargo su utilidad se está viendo hoy en día amenazada por el envío indiscriminado de correos basura, el temido Spam. Algunas fuentes apuntan incluso a que el crecimiento del correo electrónico se ha estancado, disminuyendo, debido a esta causa.

La importancia de este fenómeno lleva a dedicar los próximos capítulos a su estudio. En este primero se conocerá en detalle al "enemigo": En qué consiste, cuál es su origen y cómo se propaga.

5.1. Introducción al Spam

Tal y como hemos venido comentando a lo largo de esta publicación, no hay lugar a dudas de que, junto con los virus, **el Spam es en la actualidad uno de los principales problemas de Internet**.

Un porcentaje cada vez más alto de todos los mensajes de correo electrónico que se envían y reciben es Spam. A fecha de febrero de 2004 el **62%**[1] de los mensajes fueron identificados como anuncios de Viagra, páginas pornográficas o programas informáticos con el precio muy rebajado ("piratas").

Esta tendencia, que los expertos predicen que aumentará espectacularmente durante 2.005, puede hacer que en un futuro próximo **el número de usuarios del correo electrónico**, tal y como hoy en día se concibe, **decrezca en lugar de aumentar, llegándose incluso a inutilizar este servicio.** Si a todo esto añadimos la actitud agresiva con la que actúan últimamente los Spammers, que recurren a virus para convertir las propias máquinas de los usuarios en emisoras de Spam, y atacan a los proyectos que luchan contra él, tenemos ante nosotros un problema de gran envergadura y de difícil solución, que merece la pena analizar en profundidad.

[1] Estudio de la compañía Brightmail

Un estudio llevado a cabo por la Trans Atlantic Consumer Dialogue (TACD, que se autodefine como un foro de 65 entidades europeas y norteamericanas de defensa del consumidor) revelaba que el número de usuarios que realiza compras on line ha decrecido por miedo al Spam, tendencia que puede agudizarse en un futuro. A los internautas les resulta cada vez más "*peligroso*" dar su dirección de correo electrónico para registrarse en un sitio web o para hacer una compra on line, sea en el sitio que sea.

Estos resultados ponen de manifiesto que **el Spam está provocando un freno de la confianza de los internautas y consumidores on line en el comercio electrónico en particular, y en Internet en general**.

El Spam representa un abuso por una parte en los receptores de los mensajes, que se ven afectados desde el punto de vista de costes económicos, al tener que hacer frente al gasto (en tiempo y dinero de la recepción de estos mensajes) lo quieran o no, así como de costes sociales. Las implicaciones en el ámbito social se derivan de la molestia y ofensa asociada a determinados contenidos y a la inhibición del derecho a publicar la propia dirección en medios como listas de noticias o páginas web (por miedo a que sea capturada). Podemos concluir, que **el Spam viola los derechos de los receptores por múltiples razones, entre ellas la intrusión y la violación de la intimidad.**

Por otra parte, **el Spam también representa un problema para los PSIs que se ven abocados a grandes gastos** por el consumo extra de recursos informáticos, el ancho de banda requerido para el procesamiento y entrega de miles de mensajes, y sobre todo, por el tiempo adicional del personal dedicado a solucionar estos problemas en situaciones de saturación. Deben hacer frente a la mayor parte del coste por una publicidad que sólo les revierte inconvenientes a ellos y a sus usuarios.

Definición de Spam

Denominaremos Spam o correo electrónico basura a:

- Las **comunicaciones comerciales no solicitadas realizadas a través de correo electrónico u otros medios electrónicos equivalentes**.
- También consideramos Spam al **envío masivo de mensajes no solicitados, sean o no comerciales**, que inundan Internet con muchas copias del mismo mensaje.

Es decir, **consideramos Spam a las comunicaciones no solicitadas, sean de forma masiva o no, y a las comunicaciones masivas no solicitadas, sean o no de naturaleza comercial.**

Las diferentes definiciones de Spam que se dan por parte de los distintos organismos no siempre coinciden. A veces el Spam no se ve únicamente como un fenómeno comercial, puesto que hay que tener en cuenta que otros abusos del correo electrónico son similares, y hasta en muchos casos se habla de Spam cuando se quiere referir a toda forma de correo no solicitado. En otras ocasiones no se considera Spam si el mensaje no ha sido enviado de forma masiva.

Si acudimos por ejemplo a la definición que se dio en el 105 Congreso de los Estados Unidos, se consideran mensajes electrónicos comerciales a aquellos que contienen anuncios para la venta de productos o servicios, un número de teléfono a través del cual se puede comunicar el usuario con la persona responsable de un anuncio, o promueven el uso de listas de Internet que contienen dichos anuncios. En esta definición se contempla cualquier uso comercial, no aludiendo a si el mensaje se distribuye de forma masiva o no.

Abusos del correo electrónico:

Vamos a detenernos en este apartado al estudio de otros abusos del correo electrónico que no consideraremos Spam. Es técnicamente incorrecto otorgarles esta denominación porque puede haber casos en los que actividades llevadas a cabo por los Spammers no puedan encuadrarse en ellos y viceversa. Expliquemos pues, cuales son estos abusos:

- **Difusión de contenido inadecuado**, es decir, contenido ilegal por su complicidad con hechos delictivos: Apología del terrorismo, programas "piratas", pornografía infantil, amenazas, estafas, esquemas de enriquecimiento piramidal, virus o códigos maliciosos, etc. La temática del Spam abarca en la mayoría de las ocasiones casi todos los ejemplos comentados de contenido inadecuado.

- **Difusión a través de canales no autorizados**, es decir, usando estafetas ajenas para enviar correo propio. Aunque el mensaje sea legítimo, se están utilizando recursos ajenos sin consentimiento. Los Spammers a menudo utilizan máquinas ajenas para hacer sus envíos.

- **Difusión masiva no autorizada** (Unsolicited Bulk Email). Es el uso de máquinas propias o ajenas para enviar de forma masiva cualquier tipo de correo no solicitado. Se trata de cualquier grupo de mensajes no solicitados, cuyo contenido es sustancialmente idéntico (muchos proveedores de servicio especifican un umbral para denominar envío masivo de 25 o más direcciones de destino en un periodo de 24 horas). Se considera un abuso por varios motivos, principalmente porque el emisor de los mensajes descarga en los transmisores y receptores el coste de sus operaciones, tanto si están de acuerdo con ello, como si no. El Spam puede ser un caso particular de la difusión masiva no autorizada.

- **Comunicaciones comerciales no solicitadas**, (Unsolicitated Commercial Email). No implican que los envíos se realicen de forma masiva, pues el simple envío de un mensaje ya constituye una violación, y de hecho es ilegal en muchos países como España.

- **Ataques con objeto de imposibilitar o dificultar el servicio.** Están dirigidos a un usuario o al propio sistema de correo. En ambos casos el ataque consiste en el envío de un número alto de mensajes por segundo o cualquier variante, que tenga el objetivo final de paralizar el servicio por saturación de las líneas del CPU del servidor, o del espacio en disco del servidor o del usuario. En inglés estos ataques se conocen como "mail bombing", y son un caso particular de DoS (Denial of Service, denegación del servicio). El Spam también puede ocasionar casos de denegación de servicio por saturación y sobrecarga de los recursos de los proveedores de servicio, sin embargo su finalidad última no es imposibilitar o dificultar el servicio.

Los comienzos del Spam y el origen del término

El primer e-mail comercial no solicitado fue enviado de forma masiva a todos los usuarios de Arpanet en mayo de 1978 por Gary Thuerk, responsable de ventas de la empresa Digital Equipment Corp (DEC). Thuerk pensó que los usuarios de Arpanet podrían estar interesados en conocer que DEC (empresa de informática) había integrado el protocolo que soportaba Arpanet directamente en un nuevo DEC-20, con su sistema operativo TOPS-20.

Como estudiamos en el capítulo 4, **el protocolo SMTP se creó en 1981 de forma insegura** para ser usado por científicos, sin pensar en ningún uso comercial. En esta época ya existían listas de distribución (como LISTSERV-1984) usadas para distribuir información de uno a muchos. La explosión de Internet en 1994 a nivel social y comercial, hizo que se descubrieran los agujeros de SMTP y cómo éste podía ser utilizado para distribuir mensajes, con cualquier tipo de información comercial, a miles de buzones con un coste bajo.

La **generalización del uso del Spam empezó en 1995-1996**. Entonces cualquier máquina con un servidor de correo podía ser usada por los Spammers para distribuir su información. El gran problema eran los ataques que sufría el puerto SMTP (25) para distribuir Spam. En dicha época el servidor de correo más extendido era Sendmail, el cual solucionó las deficiencias de SMTP con sus reglas de configuración. En esos años el Spam que se recibía en los buzones era de dimensiones muy inferiores a las actuales.

Hoy en día estos problemas de configuración no están erradicados en el 100% de las máquinas de Internet, por lo que siguen existiendo servidores open-relay (máquinas open-relay son servidores de correo electrónico mal configurados), que permiten encaminar correo desde cualquier dirección IP. Esto da pié a un uso indebido de recursos de la empresa por parte de personas ajena a la misma. Estas estafetas son las preferidas por los Spammers para inyectar mensajes de Spam.

Posible origen del término Spam:

Spam es una palabra inglesa cuyo origen está en una empresa charcutera norteamericana (Hormel Foods), que en 1937 lanzó una carne en lata originalmente llamada Hormel's Spiced Ham. El gran éxito de este producto lo convirtió con el tiempo en una marca genérica, es decir, que se acabó llamando al citado producto con el nombre de la compañía (igual que en España, por ejemplo, a Colgate, con su dentífrico). Esto ocasionó que los fabricantes cambiaran el nombre para reducirlo a cuatro letras: SPAM. El SPAM fue un producto muy conocido, que alimentó a los soldados rusos y británicos en la II Guerra Mundial y que fue comercializado en todo el mundo en 1957, haciéndose aún más popular en los años 60.

La asociación de SPAM con el correo electrónico no solicitado, tiene dos versiones:

1. A raíz de una secuencia de la serie de humor por excelencia en el Reino Unido, "Monty Python", en la que se hacía una burla sobre la carne en lata. Su divertidísima costumbre de gritar la palabra SPAM en diversos tonos y volúmenes se trasladó metafóricamente al correo electrónico no solicitado. En los episodios de Monty Python, los gritos de la palabra Spam perturbaban las conversaciones normales, igual que el correo electrónico no solicitado perturba las comunicaciones vía e-mail.
2. La otra versión es que la asociación de SPAM con el correo electrónico no solicitado proviene de un laboratorio informático de la Universidad de California del Sur. Ésta lo bautizó así porque presenta similitudes en sentido figurado con la carne enlatada con dicho nombre: Aparece en cualquier lugar y nadie la pide en ningún caso, nadie se la come (es lo primero que se echa a un lado cuando se toman entremeses); y a veces tiene algo de sabor, como ese 0,0001% del correo electrónico no deseado que resulta útil a alguien.

La primera constancia de uso de este término se remonta a 1994, cuando dos abogados (Canter y Stegel)[2] enviaron un mensaje anunciando sus servicios a todas las listas de distribución de USENET, y los usuarios les llamaron Spam. De cualquier manera, Spam es una palabra comúnmente aceptada para designar al correo electrónico no deseado.

[2] Datos obtenidos de "Spam E-mail and Its Impact on IT Spending and Productivity" (diciembre de 2.003), Spira, J. B., realizado por Basex Inc., www.basex.com

Efectos del Spam: ¿Por qué es perjudicial?

El gran volumen de mensajes:

La facilidad y bajo coste del envío de miles de mensajes en periodos cortos de tiempo, ha provocado una gran proliferación de esta práctica, que representa hoy en día más de la mitad del tráfico total que circula en Internet. Esta gigantesca cantidad de mensajes provoca en muchos casos la imposibilidad o dificultad del servicio del correo electrónico y la reducción de su efectividad:

- El Spam consume recursos de la estafeta de correo electrónico, ralentizando el procesamiento del correo normal.
- Afecta al ancho de banda, congestionando las infraestructuras de comunicaciones.
- Ocasiona la inundación de los buzones de los usuarios, haciendo que se rebase la capacidad máxima de los mismos y, por tanto, provocando la pérdida de correo deseado y útil.
- Induce al receptor a una pérdida de confianza en el correo electrónico, por la naturaleza molesta y ofensiva de muchos mensajes.

El robo de recursos a los operadores:

Los Spammers utilizan diversas técnicas para conseguir enviar miles de mensajes de correo electrónico, de tal forma que el gasto ocasionado y la responsabilidad recaigan sobre otras personas. Nos referimos a los operadores de encaminamiento, que son los encargados del transporte del mensaje de correo entre emisor y receptor, y al operador de destino, que es responsable de mantener el control de los buzones de los receptores.

A continuación, explicamos las técnicas más usadas por los Spammers para hacer que los costes de sus envíos masivos recaigan sobre otras personas, y por qué representan un robo de recursos:

- La mayor parte del Spam se envía a través de sistemas intermediarios inocentes, sin ninguna relación con el Spammer. Se utilizan servidores de terceros sin que éstos sean conscientes, aprovechando la peculiaridad que presenta la mayor parte de los sistemas de correo de Internet de transportar y entregar mensajes a cualquier usuario, no sólo a los propios. Esta característica hace que las redes y los dispositivos de almacenamiento de estos intermediarios se saturen de Spam con e-mails que no se deberían entregar. Además provocan las quejas de los receptores, que a menudo suponen que su proveedor de correo está aliado con el Spammer, porque le entregó el mensaje.

- Otra técnica usada por los Spammers, que también representa un robo de recursos, es la de conseguir una cuenta de acceso a Internet gratuita y hacer los envíos masivos desde ésta. Si el PSI no detecta antes al Spammer y le cancela la cuenta, éste envía decenas de miles de mensajes y después la abandona, dejando todas las responsabilidades al PSI.

- También es una práctica frecuente utilizar como remitente una cuenta existente o una dirección falsificada de un usuario, empresa u organización. Sobre éste recaen las consecuencias del envío masivo de correo electrónico: Desbordamiento de su buzón con miles de e-mails devueltos de las direcciones que no existían, gran cantidad de usuarios que responden quejándose, etc. Se trata de un ataque muy dañino, que acarrea en muchas ocasiones tener que cambiar las cuentas afectadas.

Todo esto ha traído graves consecuencias a los operadores. La primera un gran aumento en los costes, ocasionado por la necesidad de disponer de mayor cantidad de recursos. También por tener que contar con mano de obra adicional para solucionar los desastres acarreados por el Spammer, y para vigilar las actividades que se llevan a cabo desde las cuentas de los usuarios, con el fin de impedir los abusos. Por otra parte, si el Spammer usa la segunda o tercera opción enunciada, es muy probable que el operador sea incluido en listas negras. Esto ocasiona además de los daños en imagen y los derivados de las denuncias de los afectados, que sus clientes inocentes sufran las consecuencias, dejando de recibir correo electrónico durante algunos días.

El coste social y monetario que recae en el receptor:

En efecto, si suponemos que un usuario típico dedica unos 10 segundos en identificar y descartar un mensaje, basta multiplicar este tiempo y el coste del mismo por los millones de mensajes Spam que diariamente se transmiten en la red, para hacernos una idea de su repercusión. El tiempo de conexión que dedican diariamente los clientes de un gran proveedor a descartar los envíos no solicitados y el precio que esto supone es enorme. Esto lo pagamos todos los usuarios de Internet traducido en un mayor coste de las telecomunicaciones y los servicios. En cambio, el Spammer puede realizar millones de envíos con inversiones bajísimas.

En conclusión, por una parte alguien nos hace pagar por algo que no queremos hacer ni recibir, y por otra, ninguna publicidad resulta tan barata para el anunciante y tan cara para el receptor. Para entender esto proponemos una analogía de publicidad fuera del ámbito de Internet: Realizar llamadas telefónicas para promocionar un producto o servicio a cobro revertido. Todos podemos hacernos una idea de cuánto abuso representa.

Se trata principalmente de la promoción de productos o servicios fraudulentos:

El Spam anuncia en la mayoría de las ocasiones productos y servicios que no interesan lo más mínimo al destinatario o que son engañosos y fraudulentos (métodos para curas milagrosas, componentes de ordenador "piratas", montajes para enriquecerse rápidamente, pornografía…).

Según un análisis de la Comisión Federal del Comercio de Estados Unidos[3], de una muestra al azar de 1.000 mensajes Spam escogidos entre 11 millones, **el 66% fue considerado fraudulento**. De los mensajes que ofrecían oportunidades de negocio o inversiones tales como trabajo desde casa, **fue considerado fraudulento el 96%.**

Casi todos son productos inútiles que no merecen la pena o que son ilegales, ya sea por su naturaleza, o porque es ilegal promocionarlos en medios comunes en los que hay que pagar un precio por el coste del anuncio, pues están sujetos a una legislación.

Es ilegal:

Tanto el método usado para recopilar las direcciones de correo electrónico víctimas, como el propio hecho del envío masivo de mensajes, son combatidos por la mayoría de países y colectivos que trabajan en la red. Estudiaremos en detalle estas leyes, especialmente las españolas, en el capítulo 9.

Aparece también en los grupos de noticias y listas de distribución:

Los mensajes que se difunden a través de los grupos de noticias y listas de distribución con contenido comercial y ajeno a la temática del grupo en el que aparecen, también son Spam. Algunos intentan quitar importancia al asunto diciendo que no son Spam sino mensajes off topic, es decir, que no son ilegales sino simplemente no se corresponden con el tema del grupo de distribución al que han sido enviados por algún error. Pero la diferencia entre un mensaje off topic y un mensaje Spam es clara: El Spam además de off topic, es comercial. Del mismo modo que los mensajes Spam que llegan al buzón personal de correo electrónico del usuario, hacen gastar tiempo y atención.

---

[3] Datos obtenidos del artículo "Dos tercios del Spam que recibimos son fraudulentos", www.iblnews.com . Eileen Harrington, director asociado de la FTC.

Estos mensajes por tanto son Spam y representan una lacra para estos sistemas porque aunque son no requeridos por el grupo de noticias, el usuario debe descargarlos. La única alternativa sería conectarse, bajar primero las cabeceras, limpiar los mensajes que sean Spam y después volverse a conectar para bajarse los mensajes seleccionados, pero acarrea más coste en tiempo y dinero que resignarse a descargarse todos los mensajes.

Por otro lado, consumen recursos de los servidores, lo que repercute en demoras en los tiempos de conexión, y en general, en una pérdida de eficacia y utilidad de las propias listas y grupos de noticias, además de los trastornos económicos.

Ejemplos de estafas, prácticas fraudulentas y engañosas que realizan los Spammers

Las estafas, fraudes y engaños que llevan a cabo los Spammers pueden localizarse **en la cabecera o en el cuerpo del mensaje**.

En la cabecera:

Según las conclusiones de un estudio realizado por la Comisión Federal del Comercio de Estados Unidos (FTC)[4], **el 33% del Spam analizado contiene información falsa en el campo "From:" ("De:") y el 22% de los mensajes contienen información falsa en el campo "Subject:" ("Asunto:").** La mayoría de ellos sugieren una relación con el receptor del mensaje, para aportar credibilidad.

En el cuerpo del mensaje:

El Spam es un canal ideal para llegar a un público desprotegido, niños, personas mayores o cualquier usuario confiado, al que es más fácil timar. A continuación se han recopilado **algunos de los engaños más comunes que se llevan a cabo en el contenido del mensaje** (según la FTC contienen signos de falsedad en el 40% de los casos):

- **Cartas en cadena y hoaxes:** Las cartas en cadena que incluyen dinero, artículos valiosos y prometen grandes beneficios son una estafa. Así, los usuarios que empiezan una de estas cadenas o contribuyen a propagarla enviándola a alguien, están contribuyendo a ese engaño. Los hoaxes también son un tipo de fraude, que persigue ante todo conseguir direcciones de correo electrónico para enviar Spam.

[4] "False Claims in Spam, a report by the FTC's Division of Marketing Practices", abril de 2003. Federal Trade Commission.

- **Trabajos desde casa:** Los mensajes con ofertas para trabajar desde casa, a menudo son un fraude e incumplen sus promesas. Al final el usuario trabaja muchas horas, asume costes de papel, fotocopias, y cualquier otro material necesario para el trabajo sin recibir nada a cambio o, simplemente, el beneficio recibido no compensa los costes. En otras ocasiones, las compañías que encargan estos trabajos solicitan que se abone una cantidad para recibir las instrucciones o los programas tutoriales que nunca llegarán, y de aquí sacan su beneficio.
- **Métodos para perder peso:** Nos referimos a programas y productos que promueven la pérdida de peso de manera rápida y sin esfuerzo. Todos los testimonios y garantías que se dan en el mensaje no tienen ningún valor, por lo que nunca se debe hacer caso de lo que digan.
- **Créditos o préstamos**: Se debe ser cauto con los e-mails que ofrezcan servicios financieros por entidades no conocidas, pues prometen facilidad para concederlos sin consultar la situación financiera en la que nos hallamos. Puede ser una manera encubierta de conseguir el número de cuenta, por ejemplo, y estafar al usuario.
- **Contenidos para adultos**: Los mensajes que ofrecen contenidos para gratuitos adultos, pueden hacer que se instale un programa que desconecte la conexión a Internet y la redireccione a algún número de tarificación adicional, o con prefijo internacional, con precio mucho más alto. Parte del beneficio de la llamada llega directamente al estafador.
- **Basados en la realización de llamadas**: Estos anuncios ofrecen falsas participaciones en concursos, superofertas o servicios que requieren de una llamada, o del envío de un fax, a un número de tarificación adicional (803, 806 y 807) o con prefijo internacional.
- **Promoción de la técnica de Spam**: Utilizar el propio recurso del Spam para convencer a empresas de que éste es una receta mágica y barata para hacer crecer y dar a conocer su negocio.

Una empresa fraudulenta de marketing promete a un cliente que enviará mensajes a clientes potenciales que han solicitado recibir información sobre nuevos productos y servicios. Sin embargo, lo que la empresa que contrata los servicios del Spammer a menudo consigue es crearse enemigos que nunca comprarán nada tras haber recibido estos mensajes no solicitados, e incluso perderá algunos de sus clientes tradicionales.

Para intentar que los receptores de un mensaje no consideren éste como Spam y conseguir que lo lean con cierta confianza en su veracidad, los Spammers pueden recurrir a crear falsos sitios web antiSpam, o a falsificar los mensajes electrónicos para que parezcan procedentes de organizaciones que luchan contra el Spam. Además, normalmente incluyen algún recurso en el que el usuario puede pedir que su dirección no vuelva a ser utilizada para enviar Spam. Sin embargo, casi nunca es cierto. En otras ocasiones facilitan un número de teléfono de otro continente al que se debe llamar. El precio de la llamada desanima a los usuarios.

En definitiva, el Spam representa un canal barato para incurrir en todo tipo de timos, estafas y prácticas fraudulentas e ilegales, que aunque podrían castigarse mediante el código penal o por la ley de publicidad engañosa, a menudo son difícilmente perseguibles. Además, estos mensajes pueden incluir algún dispositivo de rastreo (como el web bug), con lo que al abrir el correo automáticamente se está informando al Spammer de que la dirección del receptor está activa, y con ello nos predisponemos a recibir todo tipo de publicidad.

5.2. Origen de las direcciones víctimas de Spam

El primer paso que debe llevar a cabo el Spammer para realizar su actividad es obtener direcciones de correo electrónico de forma masiva. En este apartado expondremos las tácticas utilizadas para lograrlo.

Métodos de captura de direcciones

Las principales técnicas usadas para la obtención de direcciones son la **compra de bases de datos selectivas** (con direcciones de correo electrónico clasificadas por temáticas de interés), o la **elaboración propia** mediante la obtención de las direcciones en listas opt-in, páginas web, servidores de correo electrónico, búsquedas selectivas en Internet, virus y códigos maliciosos... Los Spammers también recopilan direcciones a través de grupos de noticias, listas o foros de discusión, y mensajes encadenados (hoaxes), utilizando normalmente búsquedas selectivas, de forma que los envíos se remiten al grupo de usuarios que lo forman. Explicamos a continuación estas técnicas:

- **A partir de listas opt-in**: Se trata de listas de usuarios que han dado su consentimiento expreso para recibir información publicitaria a cambio de información de interés. Son servicios a los que cualquiera se puede suscribir de forma voluntaria.

- **En sitios web**: Responsables de sitios web sin escrúpulos recogen direcciones de los usuarios que pasan por su portal sin su consentimiento, mediante mecanismos como web bugs, adware, etc. También recogen las direcciones de las listas de miembros de chats.

- **A través de servidores de correo-e**: Los Spammers son capaces de extraer direcciones de correo, simulando una transacción SMTP y preguntando si un usuario es o no correcto. Hacen comprobaciones automáticas de nombres de usuario con software combinador, que selecciona nombres posibles para un determinado proveedor de correo, esperando encontrar direcciones válidas entre un conjunto de direcciones de destino aleatoriamente creadas.

- **Mediante búsquedas selectivas en Internet**: Determinado software especializado es capaz de hacer barridos en Internet o en determinadas zonas para localizar miles de direcciones de correo electrónico.

- **Mediante virus y códigos maliciosos**: Se trata de virus que se propagan por correo electrónico capturando datos de las libretas de direcciones. Contaminan los mensajes y se envían a sí mismos a las direcciones recopiladas para infectar a más usuarios. Posteriormente, se envían a determinadas direcciones para el procesamiento y almacenamiento del material recogido. Este es el caso del virus Sobig.

- **A través de grupos de noticias, listas de distribución, foros de discusión y chats**: Se remite el Spam a todas las direcciones incluidas en las listas. En este caso el Spammer se suscribe al grupo, foro o lista, o bien utiliza la identidad de alguien que ya está suscrito al mismo. Otra opción es que el Spammer consiga las direcciones de los miembros del grupo a través de software rastreador.

- **Mediante la utilización de hoaxes**: Este método tiene especial relevancia por ser los propios usuarios, en su desconocimiento, los que facilitan al Spammer su dirección. Consideramos el tema de especial interés, por lo que le dedicaremos un próximo apartado.

Las direcciones de correo electrónico que se obtienen mediante los métodos expuestos, se almacenan y clasifican en **bases de datos selectivas** con el fin de venderlas o usarlas posteriormente para realizar Spam.

Conviene destacar que la mayor parte de los métodos utilizados en la obtención de direcciones de correo, sin el consentimiento expreso del usuario, pueden ser ilegales, ya que la dirección de correo electrónico está considerada en la mayoría de los supuestos como un dato personal por la LOPD (Ley de Protección de Datos de Carácter Personal), con los efectos que ello conlleva en España. Esta ley prohíbe la compra-venta de direcciones de correo a no ser que se tenga el consentimiento expreso del usuario.

Por ello, el único método legal en España para obtener direcciones de correo electrónico es la elaboración de listas opt-in. Sin embargo, en los formularios dedicados al efecto en muchas ocasiones aparece una casilla que dice "*No deseo recibir ofertas*", que el usuario debería marcar para "*en teoría*", no dar el consentimiento para recibir comunicaciones comerciales que no sean la que está solicitando. Pero a menudo, el responsable de la gestión de la lista, vende todas las direcciones recogidas, las de los que sí dieron su consentimiento y las que no. Evidentemente la mayor parte de las listas opt-in son legales pero hay buena parte de engaño e incumplimiento de lo que se asegura en las advertencias de privacidad.

En contraposición, la legislación de otros países no protege los datos personales de esta manera. En Estados Unidos, por ejemplo, es prácticamente inexistente. De ahí que los Spammers tengan casi vía libre en este sentido.

Conclusiones interesantes tras el análisis de dos estudios

Proponemos a continuación la lectura de las conclusiones de dos investigaciones realizadas en la UE y Estados Unidos en torno a las fuentes de las que los Spammers se abastecen de direcciones de correo electrónico:

- Los métodos más usados por los Spammers son programas de rastreo que buscan direcciones de e-mail en áreas públicas de Internet (páginas web, grupos de noticias, listas de distribución, foros de discusión y chats).
- Los sitios más castigados según la FTC fueron los chats. Un dato curioso es que una dirección tecleada en un chat recibía Spam nueve minutos después de ser utilizada por primera vez. Según el estudio de la UE, las direcciones que recibieron más mensajes no deseados eran las que se habían dejado en sitios web de gran afluencia de público.
- El 86% de las direcciones facilitadas en páginas web recibieron Spam. No importaba en qué parte del sitio web se encontraran siempre que contuvieran el símbolo "@". Las direcciones que se habían ocultado de alguna manera (por ejemplo, no conteniendo este símbolo), no recibieron Spam.
- El 86% de las direcciones proporcionadas en grupos de noticias, listas de distribución o foros de discusión recibieron Spam según la FTC. Sin embargo, según el estudio de la UE, estas direcciones reciben algo menos Spam que las anteriores. Un dato interesante es que las direcciones eran tomadas de las cabeceras de los mensajes de la lista de distribución, en lugar del cuerpo del mensaje.
- Ambos estudios coinciden en que a mayor afluencia de público a un sitio web o servicio, más Spam reciben las direcciones dejadas en él.

Los investigadores encontraron que las direcciones que se incluyeron en otras áreas de Internet, recibieron menos Spam: La mitad de las direcciones fijadas en páginas web personales se mantuvieron libres de Spam, al igual que el 91% de las direcciones incluidas en directorios de e-mail.

Las direcciones que se incluyeron en los perfiles de usuario de mensajería instantánea, los nombres de dominio registrados en las bases de datos whois, los servicios de búsqueda de empleo y búsqueda de pareja on line, no recibieron ningún Spam durante las seis semanas de la investigación de la FTC.

En el estudio de la UE, un dominio fue utilizado por un Spammer para encontrar direcciones válidas de forma aleatoria, mediante el método "**a través de servidores de correo electrónico**", que hemos comentado en este mismo apartado. El servidor atacado, recibió en total **8.506 mensajes**, tales como a@nombre de dominio, aa@nombre de dominio, aaa@..., b@..., c@..., ac@..., aac@..., aaac@..., d@..., ad@..., aad@..., aaad@..., etc.

En casi todos los casos, los investigadores encontraron que el Spam recibido no estaba relacionado con la dirección usada, es decir, que **el usuario está expuesto a mensajes Spam (incluyendo mensajes desagradables) independientemente de su perfil**. Esto se puso de manifiesto especialmente en algunas direcciones de e-mail dadas de alta en listas de distribución para niños. Éstos recibieron una cantidad grande de Spam que promovía sitios web para adultos, esquemas para trabajar desde casa, e igualan a las otras direcciones, en mensajes publicitarios relacionados con las drogas.

Un método que conlleva además otros graves daños: El hoax

Los hoaxes son **mensajes de correo electrónico engañosos, distribuidos en cadena por los propios usuarios**. Son mensajes no solicitados que por lo general no tienen carácter comercial, pero que llenan el buzón incomodando. En inglés se denominan también junk mail o garbage mail.

Los hoaxes se caracterizan por ser enviados desde direcciones no anónimas, por personas que siguen una determinada cadena. Algunos tienen textos alarmantes sobre catástrofes, virus informáticos, noticias que hacen mención a la pérdida del trabajo o incluso a la muerte. Todos ellos proclaman que aquello puede suceder si no se reenvía el mensaje a todos los contactos de la libreta de direcciones. También hay hoaxes que tientan con la posibilidad de hacerte millonario con sólo reenviar el mensaje, o que apelan a la sensibilidad invocando supuestos niños enfermos. Se basan pues, en el temor o superstición de la gente con el único fin de engañar e intentar recopilar direcciones de correo electrónico para realizar Spam.

Características y categorías de hoaxes:

Los hoaxes tienen, en la gran mayoría de los casos, un objetivo común: Conseguir direcciones de correo electrónico y congestionar los servidores. En otras ocasiones, su objetivo es alimentar el ego del autor, realizar estafas o difamar a personas.

Todos ellos presentan ciertas **características** que nos permiten reconocerlos: No tienen firma (aunque algunos incluyen falsas firmas), invocan los nombres de grandes compañías, y todos piden ser reenviados a los contactos de la lista del usuario. Generalmente amenazan al receptor del mensaje con grandes desgracias si el mensaje no se reenvía. Nunca remiten a ningún sitio web donde comprobar la información.

Por otra parte, el **tema** al que hacen mención puede ser englobado en alguna de las siguientes categorías[5]:

- Falsas alertas de virus.
- Mensajes de temática religiosa.
- Cadenas de solidaridad. Por un lado juegan con la sensibilidad del receptor ("*no pierdes nada reenviando este e-mail y un pequeño niño puede salvar su vida*"). Por otro lado, perjudican a todas las cadenas que pudieran ser creadas por gente que realmente lo necesita.
- Cadenas de la suerte. Son el equivalente de las viejas cadenas que recibíamos por correo postal ("*envíe esta carta a cinco personas. José Pérez no las envió y a la semana murió aplastado por un camión. Nilda Gutiérrez las envió y a los dos días ganó la lotería*").
- Leyendas urbanas. Son esas historias que circulan de boca en boca (y en los últimos años a través del correo electrónico) y que mucha gente da por descontado que son ciertas.
- Métodos para hacerse millonario, que son el equivalente por correo electrónico, de las clásicas pirámides para hacer dinero.
- Regalos de grandes compañías. Por ejemplo, circulaba un mensaje en el se decía que Microsoft y AOL pagarían una cantidad "x" por cada e-mail que se enviara. ¿Cómo pueden saber estas compañías que yo estoy enviando un mensaje para poder pagarme? Por otro lado, con que unos cuantos miles de personas manden algunos cientos de mensajes se arruinarían.
- Mensajes tomando el pelo a la gente que envía hoaxes.
- Mensajes verdaderos o que están basados en algún hecho real, pero que por diversas causas no deben ser reenviados en cadena.

Hay otros mensajes que no nacen como hoaxes pero pueden **transformarse** en ellos:

- Poemas y mensajes de amor y esperanza (éstos suelen presentarse en un archivo con formato PowerPoint).
- Mensajes para unirse a programas de afiliados.
- Chistes y fotos que circulan en cadena.

[5] Según la información obtenida en www.rompecadenas.com.ar . En esta página se pueden encontrar los textos de más de 80 hoaxes y más detalles de este tipo de práctica.

Consecuencias que conlleva su distribución y reenvío:

Se podría pensar que las consecuencias del envío de unos cuantos mensajes falsos o mensajes broma son mínimas, o que no pueden llegar a ser dañinos. Pero los hoaxes pueden ser peligrosos por varias razones: Alimentan las bases de datos de los Spammers, llenan de publicidad y correo electrónico no deseado los buzones de los usuarios, congestionan los servidores, y hacen perder tiempo y dinero al receptor. También ocasionan falta de credibilidad a cadenas creadas por gente que realmente lo necesita.

Por otra parte, determinados hoaxes pueden perjudicar a los usuarios de otras maneras.

Los hoaxes Sulfnbk o Jdbgmgr eran falsas alertas que hicieron que muchísima gente borrara archivos fundamentales en el funcionamiento de Windows creyendo que se trataba de virus.

Muchos hoaxes funcionan en base al miedo que generan y pueden provocarnos pánico, terror, asco, etc.

La cantidad de hoaxes creados con relación a los atentados en Estados Unidos generó un miedo adicional en mucha gente.

Por otro lado, son especialmente dañinos los mensajes que involucran a personas o empresas reales, ya que es muy fácil utilizar este medio para difamar o calumniar.

Un ejemplo es el hoax que vinculaba al grupo musical "La oreja de Van Gogh" con la banda terrorista ETA.

Finalmente, un fenómeno que está apareciendo con mucha frecuencia, es que se toma algún hoax existente y se le insertan todos los datos de alguna persona real (nombre, cargo, lugar de trabajo, teléfono, mail), generalmente profesionales, para darle mayor seriedad al mensaje. No hace falta decir las molestias que esta situación puede causarle a esta persona que aparece avalando supuestamente determinada información (cientos de e-mails, llamadas telefónicas, denuncias, etc.). Esta maniobra es una de las más bajas que puedan realizarse: Utilizar el nombre de una persona inocente y ajena para difamar a otra. Una vez más, la gente sin escrúpulos se vale de los sentimientos de las personas para hacer daño y recolectar direcciones de e-mail.

Los hoaxes provocan mucho perjuicio a los internautas: Recolectan las direcciones de mail, vulnerando la privacidad de los usuarios, y violan la intimidad y el nombre de quienes son víctimas de estas maniobras.

Cómo actuar frente a los hoaxes:

En primer lugar, **no conviene reenviar nunca estos mensajes**.

Si se desea reenviar el mensaje a alguien, se debe evitar que circulen todas las direcciones que venían en él. Al reenviar un mensaje con la opción "Reenviar mensaje" o "Forward" del programa de correo, automáticamente se incorporan al cuerpo y cabecera del mensaje todas las direcciones incluidas en los campos "Para" y "CC". Para conseguir que estas direcciones no aparezcan en el mensaje que vamos a enviar, se puede proceder seleccionando la parte del mensaje que se desea reenviar evitando las direcciones, y copiarlo y pegarlo en un mensaje nuevo. También, utilizando el campo "CCO" o "BCC", pues todas las direcciones que se incluyen en estos campos no serán vistas por las personas que reciben el mensaje.

Hay muchos motivos diferentes por los que no se deben reenviar estos mensajes. Por un lado, para evitar contribuir a la saturación de los buzones y servidores de correo electrónico. Por otro, que todos podemos llegar a ser víctimas de estos delincuentes. Imaginemos que el día de mañana vemos nuestro nombre difamado en cientos o miles de e-mails. Hay que pensarse varias veces antes de reenviar una cadena que involucra a personas con nombre y apellido, pues se estará siendo cómplice involuntario de la difamación.

Actualmente no hay una legislación clara frente a estos mensajes de corte no comercial, puesto que se consideran "inofensivos". Sin embargo, en este apartado hemos dejado claro que deberían estar normalizados al igual que se intenta con los mensajes Spam. El buzón de correo electrónico puede considerarse como parte de nuestra intimidad, es por ello que un envío no autorizado ni solicitado resulta perjudicial por sí mismo, y por lo tanto atentatorio contra el usuario, que accede a Internet para otras finalidades.

Por eso, y puesto que hoy en día no existe otra forma de combatir esta práctica, es conveniente **concienciar a los usuarios para que no sean cómplices y no reenvíen estos mensajes**.

5.3. La distribución del Spam

Estudiaremos en este apartado la cadena de distribución del Spam, es decir, los diferentes elementos que son necesarios para permitir el envío masivo de un mensaje. Prestaremos especial atención a los "Open Relays", servidores abiertos que dirigen y propagan estos mensajes por la Red.

La cadena de distribución del Spam y sus principales elementos

Las personas/entidades implicadas en la distribución del Spam son, según Grey, M. C.[6], los siguientes:

- **Proveedores del software**: Desarrollan aplicaciones que hacen extremadamente fácil efectuar envíos masivos y buscar direcciones de correo electrónico válidas (asociando combinaciones de letras a nombres de dominio, efectuando potentes búsquedas selectivas en Internet, etc.).
- **Cosechadores de direcciones**: Utilizan el software anteriormente descrito para buscar direcciones de correo electrónico válidas.
- **Spammers**: Envían los mensajes de forma masiva, utilizando el software apropiado y las bases de datos con las direcciones de destino.
- **Compañías clientes**: Empresas que deciden que las promociones de sus productos y servicios deben llegar a cualquiera, en cualquier lugar, independientemente del medio utilizado. Recurren a este método, contratando los servicios de los Spammers, o realizando el Spam ellas mismas.
- **Compañías, organizaciones y gobiernos que luchan contra el Spam:** Se encuentran en el lado opuesto, intentando contribuir a romper esta cadena.

Todos estos componentes representan una cadena extendida, si bien por la sencillez que implica, en muchas ocasiones todos o varios de sus eslabones son la misma persona o entidad. Dicho lo anterior, podemos analizar cuáles son los principales elementos necesarios para la distribución de Spam:

- El **software** necesario: Consistiría, por un lado, en buscadores configurados específicamente para encontrar direcciones en Internet. Por otro, en un programa sencillo que reproduzca un diálogo SMTP, colocando los campos de remite y destino que convengan y falsificando algunas de las cabeceras de tránsito de los mensajes. Para realizar envíos masivos de Spam basta con conocer el protocolo SMTP.
- Una **base de datos** con direcciones de correo a las que distribuirá el mensaje de Spam, que se puede comprar o confeccionar.

---

[6] Grey, M. C. es directora de investigación de Gartner Research. Sus declaraciones han sido extraídas del artículo "The Great Spam Supply Chain" (15 de marzo de 2003), www.cio.com/archive/031503/tl_email.html

- **Una máquina (estafeta) con la que establecer el diálogo SMTP**: En este caso puede ser una máquina local con un paquete de servidor de correo electrónico, o una máquina remota mal configurada a la que se accede por el puerto 25 (SMTP). En otras ocasiones los Spammers utilizan métodos de hacking para convertir cualquier servidor en un open relay.

El problema e implicaciones de los servidores abiertos

Los servidores de correo electrónico abiertos o estafetas abiertas (open relays) son servidores mal configurados, que permiten a cualquier otra máquina del mundo dirigir mensajes a través de ellos. Esto permite un uso indebido de recursos de la empresa por parte de personas ajenas a la misma.

Estas estafetas son las preferidas por los Spammers para inyectar mensajes Spam, puesto que de esta forma usan recursos ajenos, cuyos costes no corren de su cuenta. Usando software automatizado, los Spammers exploran Internet en busca de servidores con estas características. Cuando descubren alguno, encaminan a través de él sus envíos masivos, que son procesados en mayor volumen y menor tiempo de lo que podrían con sus propias computadoras individuales. Este uso indebido, crea problemas a los internautas del mundo entero, a la organización responsable de estas máquinas y a la ejecución de la ley.

Para entender cómo un mensaje ajeno puede ser retransmitido por el servidor de correo electrónico de una organización, es necesario tener presente cómo funciona el servicio de correo electrónico. Cuando alguien de la organización envía un mensaje a un servidor externo, el software del servidor debe comprobar que dicho servidor destino es seguro (si esta definido como tal en sus registros internos). Si es así, enviará el mensaje. Cuando el servidor recibe un mensaje externo, el software deberá confirmar si el receptor del mensaje es un usuario autorizado (perteneciente a la organización), y en ese caso, aceptará la transacción y entregará el mensaje. Si el servidor no es seguro y permanece "abierto", remitirá mensajes a los destinatarios que no son usuarios de la organización y estará configurado de manera que acepta y encamina mensajes a nombre de cualquier usuario de cualquier lugar, incluyendo terceros sin relación. Así, un servidor abierto permite que cualquier remitente, encamine mensajes a través del servidor de la compañía.

Los **problemas** que esta mala configuración de los servidores de correo electrónico pueden causar a la organización responsable son:

- Los recursos e infraestructuras de comunicaciones pueden ser objeto de hurto y uso fraudulento, pues se está dejando una puerta abierta al uso por terceros desconocidos de los servicios informáticos de la organización.

- Los mensajes Spam recibidos por terceros pueden parecer provenir del sistema que contiene el servidor abierto. En efecto, el uso de estafetas abiertas permite a los Spammers encubrir sus identidades, porque parece que el Spam viene realmente de ellas. Si los servidores de una organización en concreto son usados de este modo, el tráfico podría colapsar el sistema. La red de la organización podría verse inundada por los mensajes Spam que intenta enviar, por quejas de las personas que los reciben, y con el Spam devuelto de las direcciones que se incluyeron en el envío, pero no existían.

  La reparación de esta sobrecarga, podría ser costosa y repercutir en una gran cantidad de tiempo fuera de servicio. Pero aún más costosa podría ser la pérdida potencial de confianza de los que piensen que es dicha organización la que ha enviado el Spam.

- El proveedor de servicios de Internet puede cortarle el servicio al detectar esta práctica.

- Un mayor tráfico, puede provocar que los costes administrativos se incrementen.

Pero esto no es todo, los Spammers también **pueden usar servidores proxy abiertos (mal configurados) de la organización**. Ello puede permitir situaciones tales como que terceras personas se introduzcan en el sitio web de la organización, y se conecten a máquinas de Internet desde el interior.

Un Spammer puede usar un proxy abierto para conectarse al servidor de correo electrónico de la organización, cargar el envío masivo de Spam, y luego desconectarse, todo ello de forma anónima y sin posibilidad de rastreo.

Figura 9

La Comisión Federal del Comercio de Estados Unidos (FTC) asegura que ha detectado al menos **1.000 estafetas que podrían estar potencialmente abiertas**, de las cuales el 90 por ciento se encuentran en 16 países: Estados Unidos, China, Corea, Japón, Italia, Polonia, Brasil, Alemania, Taiwán, México, Gran Bretaña, Chile, Francia, Argentina, India, España, y Canadá. Estos países se reflejan en el mapa anterior.

El porqué existen tantos servidores mal configurados, se debe principalmente a que en los primeros tiempos de Internet, muchos se mantenían en este estado para permitir que los e-mails viajasen entre diversas redes. Esto ayudó a crecer a Internet. Como herencia de esta época algunos servidores poseen por defecto esta configuración abierta.

5.4. Análisis de las cabeceras de los mensajes

Los Spammers intentan ocultar su identidad **falsificando las cabeceras de los mensajes de correo electrónico**. En este apartado veremos cómo encontrar la verdadera identidad del emisor del Spam a través de ellas, las herramientas disponibles para localizar las direcciones de Internet de origen y los datos del proveedor de Internet de origen, en los casos en los que sea posible.

Según un estudio realizado por la Comisión Federal del Comercio de Estados Unidos[7], de una muestra al azar de 1.000 mensajes Spam, de entre más de 11 millones, el 44% usó direcciones de retorno falsas para ocultar la identidad del remitente o un "asunto" engañoso.

Recomendamos en primer lugar, repasar el apartado 4.6. de esta publicación "Interpretación de las cabeceras de los mensajes".

Cómo averiguar la identidad de un Spammer

Para intentar averiguar la identidad de un Spammer nos interesa estudiar el campo "**Received:"** de la cabecera del mensaje. Cada estafeta por la que pasa el mensaje añade una información en la parte de arriba de este campo, de tal manera que:

- El primer campo "Received:" ha sido añadido por la última estafeta por donde pasó el mensaje.

[7] Información obtenida del artículo "Dos tercios del Spam que recibimos son fraudulentos", www.iblnews.com , y del propio estudio: "False Claims in Spam, a report by the FTC's Division of Marketing Practices", abril de 2003. Federal Trade Commission.

- El último campo "Received:" debería indicar la primera estafeta que recibió el mensaje (suponiendo que no se han usado técnicas de enmascaramiento, es decir, que no se ha falsificado parte de la cabecera o que el servidor de origen incluye información en este campo[8]).

Así, el esquema del campo "Received:" para una secuencia de estafetas A->B->C->D es:

```
Received: from <estafeta_que_manda(C)> by
<estafeta_que_recibe(D)><datos>.

Received: from <estafeta_que_manda(B)> by
<estafeta_que_recibe(C)><datos>.

Received: from <estafeta_que_manda(A)> by
<estafeta_que_recibe(B)><datos>.
```

Es decir, **se lee de abajo a arriba y de izquierda a derecha para recomponer la secuencia**. Los servidores B y C son estafetas intermedias entre las de origen y destino (A y D respectivamente).

Reproducimos a continuación el campo "Received:" del ejemplo anterior para clarificar que significa cada componente:

```
Received: from tsmtp3.ldap.isp ([10.20.4.23]) by mb30.terra.es (terra.es)
with ESMTP id HPHCHU00.JC5 for <jmmpos@terra.es>;

        Sat, 6 Dec 2003 16:32:18 +0100

Received: from relay.mixmail.com ([62.151.8.30]) by tsmtp3.ldap.isp
(terra.es) with ESMTP id HPHCHS00.RVX for <jmmpos@terra.es>;

        Sat, 6 Dec 2003 16:32:16 +0100

Received: from [172.30.8.15] (helo=web01)by relay.mixmail.com with
smtp id 1ASePn-0007dj-00 for jmmpos@terra.es;

        Sat, 06 Dec 2003 16:32:15 +0100
```

Esta cabecera es de un mensaje legítimo (y por tanto con su cabecera no falsificada), enviado desde martammr@mixmail.com a jmmpos@terra.es, que indica que el mensaje original fue mandado desde una máquina cuya dirección IP es [172.30.8.15] (que pertenece a Mixmail), que ha pasado por dos servidores intermedios, "relay.mixmail.com", con dirección [62.151.8.30], "tsmtp3.ldap.isp" (Terra.es), con dirección [10.20.4.23], y que fue entregado a "mb30.terra.es" (Terra.es).

[8] Existen todavía servidores de una versión antigua de SendMail, que no registran esta información, por lo que si el Spammer usa este tipo de servidor, no podremos rastrear su mensaje. Sin embargo, afortunadamente no es el caso más habitual.

A continuación vamos a ver dos mensajes de correo, que provienen de Spammers, cuya cabecera ha sido falsificada. **Un indicio de que el mensaje o su cabecera ha sido falsificados, es que se rompe la secuencia de estafetas del campo "Received:".** Los datos que aparezcan tras este punto de ruptura pueden ser falsos.

Mensaje 1: La siguiente cabecera es de un mensaje Spam dirigido a la dirección de correo tresmr@hotmail.com.

X-Message-Info: ASZdpiY8olkOLMeOyu9AxQlar2pq6Aw6/Muu/W3TUsQ=

Received: from mc7-f26.hotmail.com ([65.54.253.33])

by mc7-s11.hotmail.com with Microsoft SMTPSVC(5.0.2195.6713);

Fri, 5 Dec 2003 12:25:50 -0800

Received: from ôÉàæÄãÄÜ×öÐ©Ê²Ã´£ ([80.139.98.148])

by mc7-f26.hotmail.com with Microsoft SMTPSVC(5.0.2195.6713);

Fri, 5 Dec 2003 12:25:49 -0800

To: <Oraqgcvpobr6Wt2LH791@yahoo.com>

From: "Liz" <tomblikecontributoryboatyard@tombstonecontrite.net>

Subject: -=SIZE=- it D0es matter

Date: Fri, 05 Dec 2003 15:26:05 -0500

MIME-Version: 1.0

Content-Type: text/html; charset="iso-8859-1"

Content-Transfer-Encoding: quoted-printable

Return-Path: tomblikecontributoryboatyard@tombstonecontrite.net

Message-ID: <MC7-F26rx5zAa6l3zZx0000835b@mc7-f26.hotmail.com>

X-OriginalArrivalTime: 05 Dec 2003 20:25:50.0320 (UTC)

FILETIME=[F932EF00:01C3BB6D]

Observamos inicialmente que algunos campos de la cabecera contienen ristras de caracteres extraños. Así, el campo "To:" (dirección de destino) no contiene la verdadera dirección de destino (que es tresmr@hotmail.com), sino una dirección extraña (Oraqgcvpobr6Wt2LH791@yahoo.com). El campo "From:" y el nombre de la máquina de origen (en el campo "Received:") también da la impresión de que se han falsificado.

Mensaje 2: Veamos un segundo mensaje Spam, que también iba dirigido a tresmr@hotmail.com:

```
X-Message-Info: 8Q6ATcAEb5e7zPw0COqY18Hn5ysiSxR1Ta5EkS16Z2g=
Received: from mc8-f8.hotmail.com ([65.54.253.144])
by mc8-s13.hotmail.com with Microsoft SMTPSVC(5.0.2195.6713);
Wed, 3 Dec 2003 15:24:55 -0800
Received: from Zcotierwymtn3F ([80.139.48.158])
by mc8-f8.hotmail.com with Microsoft SMTPSVC(5.0.2195.6713);
Wed, 3 Dec 2003 15:24:36 -0800
To: <faarabnqh6LR3Dr575@hotmail.com>
From: "Tammy Wolf" <nowherescrimmage.org>
Subject: View it before its gone
Date: Wed, 03 Dec 2003 18:24:48 -0500
MIME-Version: 1.0
Content-Type: text/html; charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable
Return-Path: nowherescrimmage.org@mail.hotmail.com
Message-ID: <MC8-F89wmfKGezPLC6M0001d6b2@mc8-f8.hotmail.com>
X-OriginalArrivalTime: 03 Dec 2003 23:24:37.0334 (UTC)
FILETIME=[9E2BDF60:01C3B9F4]
```

En este segundo mensaje tampoco coincide el contenido del campo "To:" con la dirección de destino. Sin embargo observamos que el nombre de la máquina origen en el campo "Received:" (Zcotierwymtn3F), sí podría corresponderse con una máquina real.

En ambos mensajes, a pesar de la falsificación de la cabecera, vemos que ésta nos da información de los servidores por donde ha transitado el mensaje antes de llegar al buzón de destino y la verdadera dirección IP del servidor de origen, que sirve para localizar el sitio desde el que el Spammer está haciendo sus envíos masivos. Esta dirección IP se encuentra al principio del último campo "Received:", la cual en el primer mensaje es [80.139.98.148], y en el segundo, [80.139.48.158].

Herramientas para localizar a los responsables del servidor origen del Spam

Dada la dirección IP de origen de los mensajes, disponemos de diversos recursos para tratar de combatir el Spam:

Efectuar una queja al encargado de la gestión del sitio web con esa dirección:

Normalmente, debería ser postmaster@[80.139.98.148] ó abuse@[80.139.98.148], en el caso del primer mensaje analizado en la sección anterior (aunque en muchos casos estas direcciones no se utilizan o directamente no se leen por ser blanco de los Spammers).

Localizar qué sitio web es el que tiene asignada dicha dirección, y con ello, los datos del responsable:

Existen varias vías para obtener el nombre de dominio de una dirección IP:

- **Hacer una consulta a un servidor DNS**: Esta consulta se puede efectuar mediante herramientas al efecto, dependiendo del sistema operativo que se use. Si no se dispone de ninguna, se puede acudir a páginas que facilitan estos accesos, como www.dnsstuff.com

En la página www.dnsstuff.com, se ofrecen herramientas con las que consultar todas las bases de datos necesarias de forma transparente. Asimismo disponen de aplicaciones útiles para rastrear una dirección IP o un nombre de dominio, o saber si la dirección IP está incluida en una de las 300 listas negras de Spammers a las que puede acceder la página en cuestión.

- **Utilizar las bases de datos whois de dominios de Internet**:
  - InterNIC (www.internic.net/cgi-bin/whois), para dominios .edu, .com, .org, y .net
  - RIPE NCC (www.ripe.net/db/whois.html), para dominios europeos
  - ES-NIC (https://www.nic.es/esnic/servlet/WhoisControllerHTML), sólo para dominios .es.

Una dirección IP, como hemos dicho, caracteriza unívocamente una máquina en Internet. Pero ésta puede ser estática (como en el caso de servidores o de conexiones mediante ADSL) o dinámica dentro de un rango asignado por un servidor. En el **caso de que la dirección sea dinámica**, también nos hará falta saber la **fecha y hora** en que se envió dicho mensaje. Esto viene reflejado en el campo "Date:".

Para los mensajes Spam analizados anteriormente, cuyas direcciones origen hemos descubierto que eran [80.139.98.148] y [80.139.48.158], tras realizar una consulta a las bases de datos whois, obtenemos que ambas pertenecen a la misma organización cuyos datos son los siguientes[9]:

```
% This is the RIPE Whois server.
% The objects are in RPSL format.
%
% Rights restricted by copyright.
% See http://www.ripe.net/ripencc/pub-services/db/copyright.html

inetnum:      80.128.0.0 - 80.146.159.255
netname:      DTAG-DIAL16
descr:        Deutsche Telekom AG
country:      DE
admin-c:      DTIP
tech-c:       DTST
status:       ASSIGNED PA
remarks:
**************************************************
remarks: *ABUSE CONTACT: abuse@t-ipnet.de
remarks:* IN CASE OF HACK ATTACKS, ILLEGAL ACTIVITY,
      *       VIOLATION,       SCANS,       PROBES,       SPAM,       ETC.
**************************************************
mnt-by:       DTAG-NIC
changed:      ripe.dtip@telekom.de 20010807
changed:      ripe.dtip@telekom.de 20030211
source:       RIPE

route:        80.128.0.0/11
descr:        Deutsche Telekom AG, Internet service provider
origin:       AS3320
mnt-by:       DTAG-RR
```

[9] (C) Copyright 2000-2003 Computerized Horizons, obtenido de www.dnsstuff.com

changed:	bp@nic.dtag.de 20010807
source:	RIPE
person:	DTAG Global IP-Addressing
address:	Deutsche Telekom AG
address:	D-90492 Nuernberg
address:	Germany
phone:	+49 180 5334332
fax-no:	+49 180 5334252
e-mail:	ripe.dtip@telekom.de
nic-hdl:	DTIP
mnt-by:	DTAG-NIC
changed:	ripe.dtip@telekom.de 20031013
source:	RIPE
person:	Security Team
address:	Deutsche Telekom AG
address:	Germany
phone:	+49 180 5334332
fax-no:	+49 180 5334252
e-mail:	abuse@t-ipnet.de
nic-hdl:	DTST
mnt-by:	DTAG-NIC
changed:	abuse@t-ipnet.de 20030210
source:	RIPE

Entre toda esta información, nos interesa conocer la base de datos que contenía esta dirección, que era RIPE; la dirección de correo electrónico a quien podemos enviar nuestra queja, que es abuse@t-ipnet.de ; y los datos de la organización: una descripción de su nombre y actividad ("Deutsche Telekom AG, Internet service provider"), el país de origen (Germany) y un número de teléfono y fax de contacto.

CAPÍTULO 6. MEDIDAS CONTRA EL SPAM

El usuario no se encuentra "indefenso" ante el Spam, existen diferentes medidas que puede adoptar para evitarlo o, al menos, disminuir el número de mensajes de estas características que recibe. Algunas de estas medidas son de carácter preventivo, ya que se adoptan para evitar recibir correo basura. Otras tienen un carácter más activo, en el sentido de que "luchan" contra el Spam dirigido al usuario: Bien evitando que éste llegue a su servidor de correo o bien filtrándolo una vez recibido, para eludir su lectura.

6.1. Medidas preventivas

Comenzaremos este apartado proponiendo una serie de consejos a distintos agentes que, de alguna manera, participan o son víctimas de actividades relacionadas con el Spam. Estos consejos pueden ayudar a los usuarios a recibir menos Spam y a que éste les resulte menos perjudicial. También se aportan consejos a los administradores de correo electrónico para que, por un lado, informen a los usuarios sobre el tema y, por otro, controlen sus sistemas y políticas institucionales, evitando que los recursos que gestionan sean mal utilizados por sus propios clientes o por Spammers ajenos al servicio.

Proseguiremos este apartado con un breve análisis sobre la situación legislativa con relación al Spam en la Unión Europea y en Estados Unidos (análisis en el que profundizaremos durante el capítulo 9). La legislación también puede considerarse una medida preventiva contra el Spam, pues lo que persigue en último término es la imposición de multas y penas para disuadir a los Spammers de que lleven a cabo sus actividades.

Si estas medidas de prevención contra el Spam fueran ampliamente adoptadas, podrían contribuir, si no a una erradicación del problema, sí a una disminución de la cantidad de Spam que circula.

Consejos a los usuarios. Pautas para minimizar la cantidad de Spam recibido

Estas pautas nos pueden ayudar a minimizar la cantidad de Spam recibido, así como a adquirir unas "*buenas costumbres*" en relación con la seguridad de nuestros datos:

1. **No hacer pública nuestra dirección de correo electrónico, siempre que sea posible, en páginas web, listas de distribución, chats, etc.:** Si no hay más remedio que suministrar la dirección, pueden tenerse en cuenta algunos consejos:
   - Aportar una dirección de correo temporal gratuita, distinta de la que se usa normalmente, con el fin de que nos sea fácil prescindir de ella en el caso en que ya no nos interese.

- Omitir el carácter "@". Los métodos de rastreo de direcciones de los Spammers se basan a menudo en la búsqueda de este carácter (incluido en todas las direcciones de e-mail). Si lo omitimos y sustituimos por "ARROBA", o incluimos "QUITALASMAYUSCULAS" después de "@", reduciremos drásticamente las posibilidades de que nuestra dirección sea captada por los Spammers.

Vemos un ejemplo con la dirección de correo tresmr@hotmail.com. Siguiendo este procedimiento, la haríamos pública como:

tresmrARROBAhotmail.com

tresmr@QUITALASMAYÚSCULAShotmail.com

Los resultados de un reciente estudio[10] indican que si la dirección se oculta de alguna manera, aunque sea de forma sencilla tal y como acabamos de enunciar, las posibilidades de recibir Spam por la captura de la dirección mediante programas rastreadores (que es la principal fuente de los Spammers), es prácticamente nula.

2. **Leer y comprender la política de privacidad de los sitios web donde se suministre la dirección de correo electrónico**: La información es en muchas ocasiones la mejor arma de los consumidores electrónicos. En España la LOPD no permite la utilización de datos personales (la dirección electrónica puede ser calificada como tal), ni su uso por terceros sin previa autorización, por ello, los sitios web que pretendan hacer uso de la dirección de e-mail facilitada por los usuarios, deben advertirlo al menos en su política de privacidad.

   En caso de que no existan otras advertencias, se debe poner atención en comprender la política de privacidad, pues muchos sitios se basan en redactarlas muy extensas para que los usuarios no se molesten en leerlas. En cualquier caso, si ésta no aparece, permite a la compañía vender la dirección de correo electrónico, cederla a terceros, realizar algún uso sospechoso… En este caso es mejor no facilitarla, o al menos valorar si nos interesa hacerlo pese a todo. Los formularios online deben incluir una casilla en la que el usuario puede señalar si desea o no recibir comunicaciones comerciales.

3. **Usar más de una dirección de correo electrónico dependiendo del uso que se vaya a hacer de ella**: Una para los mensajes personales, otra para asuntos profesionales, otra para proporcionarla en chats u otros sitios web con fines de ocio, por ejemplo.

---

[10] "Why Am I Getting All This Spam? Unsolicited Commercial E-mail Research" (www.cdt.org/speech/Spam/030319Spamreport.shtml), realizado por Center for Democracy & Technology de la UE, en marzo de 2003. Las direcciones estudiadas que fueron ocultadas de alguna manera no recibieron ningún Spam, frente a los más de 8.000 que recibieron otras direcciones sometidas al estudio.

4. **Elección de la dirección de correo electrónico**: La dirección marta@dominio.com, por ejemplo, es posible que reciba más Spam que otra como m_x5_r1@dominio.com. Usando un nombre poco común como dirección es más difícil que reciba Spam. Recordemos que utilizar direcciones de destino aleatorias suele ser uno de los métodos utilizados por los Spammers. Recurren a combinadores que seleccionan nombres posibles y palabras de diccionario, para un determinado proveedor de correo, esperando encontrar direcciones válidas.
5. **Usar las opciones de filtrado del gestor de correo:** Todos los gestores de correo actuales incluyen algún tipo de herramienta para filtrar mensajes y bloquear direcciones concretas, de tal forma que no se reciban mensajes de ellas.

Consejos a los creadores de contenidos, foros, listas y páginas web

La mayor parte de los sitios web en Internet combaten el Spam adoptando sus propias medidas de protección y vigilancia. No obstante, es conveniente seguir unos consejos básicos para proteger las direcciones propias del responsable de la página web, de los internautas que la visiten y de los clientes:

1. En general, **no se deben publicar direcciones de correo en las páginas, a no ser que sea estrictamente necesario**: Si se publican direcciones se deben tomar algunas medidas de precaución para que éstas no sean rastreadas por los Spammers. Se puede recurrir a sencillas técnicas que hacen invisibles las direcciones a los programas de rastreo.

Estas técnicas se basan en que estos programas funcionan haciendo búsquedas selectivas de las "arrobas" (tal y como ya hemos enunciado) o el "mailto" que aparecen en las direcciones. Una manera sencilla de "*esquivar*" el rastreo puede ser publicar las direcciones en formato gráfico, sin el enlace al e-mail.

También se puede implementar una función en Javascript, tal que dado únicamente el nombre del buzón, le añada la arroba y el nombre de dominio para completar la dirección de correo. De esta forma en la página sólo aparece el nombre del buzón, por lo que no puede ser tomada automáticamente.

Otra forma podría ser incluir la dirección ASCII codificada en decimal, o sustituir la arroba por otro texto, como hemos comentado en el apartado anterior de consejos a los usuarios.

2. En el caso de **gestionar listas de distribución**, se debe disponer de las medidas mínimas para proteger el servicio:
   - No se deben permitir altas sin que se validen a través de la dirección de correo electrónico suscrito, para evitar altas no deseadas a terceros. Es una buena práctica incluir en los mensajes siempre un enlace que permita darse de baja de ella de forma sencilla, con el fin de controlar la disponibilidad de la relación de los suscriptores.
   - Si la lista posee contenidos accesibles, es conveniente no publicar los e-mails de los participantes en los mensajes o advertir de los riesgos que conlleva la participación.
   - Es muy positivo que antes de publicar los mensajes, éstos pasen por algún sistema de moderación o validación, para evitar mensajes comerciales o mensajes off-topic.
   - No permitir listas públicas de envío.
   - Controlar y limitar el número máximo de copias o envíos simultáneos que pueden realizar los que utilizan los servicios, con el fin de evitar envíos masivos desde la lista.

A continuación incluimos una serie de consejos que se han de tener en cuenta si el sitio web que se gestiona obtiene la dirección de correo de sus usuarios (con el fin de enviarles información promocional). Se ha de ser muy cuidadoso para que el sitio web goce de confianza y no sea calificado como Spammer, con las consecuencias que ello traería al respecto.

Aspectos a tener en cuenta al solicitar o recoger datos de los usuarios:

Cuando un usuario se suscribe a una página web porque le interesan servicios que en ella se ofrecen o información sobre sus productos, es interesante que se le informe de la finalidad y las condiciones en las que serán tratados sus datos en el mismo formulario de suscripción. El objetivo es que el usuario dé su consentimiento con la mayor información posible al respecto.

Para que no se vea sorprendido es conveniente también incluir información adicional sobre la periodicidad aproximada de los comunicados o boletines que se le van a enviar, quién es el responsable de los datos que suministra, así como si éstos se cederán a terceros. También debemos asegurarnos que el consentimiento sea explícito, para evitar usuarios que acepten sin leer las advertencias.

Estas prácticas son positivas para ambas partes ya que, por un lado, **se está actuando de forma ética, honesta y legal de acuerdo con las leyes de protección al consumidor y de protección de datos, y por otro, los usuarios se sentirán seguros y tendrán confianza, repercutiendo esto en una mayor fidelidad de los suscriptores y mayor eficacia de las comunicaciones** que sean enviadas.

Validación de los datos:

Una práctica que también reporta beneficios a ambas partes es comprobar los datos de los usuarios tan a fondo como sea posible, con el fin de no utilizar datos incorrectos, mejorando con ello la calidad de los boletines enviados y sus contenidos.

En especial es importante chequear la dirección de correo que se recibe a través de cualquier medio anónimo, como puede ser un formulario en una página web. Es positivo analizar los datos (nombres y direcciones sobre todo) y preguntarse cuántos de ellos son realmente válidos. Aunque la ventaja del correo electrónico es que los costes de los envíos son muy inferiores a los envíos postales, existe la falsa creencia de que tiene menos importancia el envío masivo sin la validación de los datos.

Para conseguir saber si los datos son válidos, se puede enviar un mensaje de validación con un enlace para completar el proceso de alta. De esta manera se garantizará su autenticidad, eliminando las posibles direcciones erróneas. Desde el punto de vista de combatir el Spam se conseguirá hacer del boletín una herramienta útil y segura que otorgará calidad al servicio.

Uno de los inconvenientes del proceso de validación es que sólo un 30% de los clientes potenciales completa el proceso de alta. Aunque este dato pudiera desanimarnos de utilizar un sistema de validación, conviene pensar que es más positivo disponer de una lista de clientes más pequeña, pero con el 100% de los datos correctos, que de una lista mayor con un 30% de clientes con sus datos erróneos.

De esta forma, enviando boletines sólo a clientes potenciales cuyos datos y consentimiento sean cien por cien veraces, se conseguirán más clientes reales, sin ningún riesgo de perder la conexión del proveedor de servicios por ser calificado de Spam o ser incluido en una lista negra, con las molestias que ello conllevaría.

Adquisición de listas de direcciones de terceros:

La venta de datos sin el consentimiento expreso del usuario al que pertenecen está prohibida en España por la LOPD. Se debe por tanto ser reacio a la compra de direcciones, pues en la mayoría de las ocasiones éstas no han sido tomadas con el consentimiento de los usuarios o sus datos son erróneos. En el caso de compra, se deben solicitar los formularios de autorización de los usuarios, así como su política de privacidad.

La consecuencia de enviar e-mails de promoción a usuarios obtenidos de una lista comprada, que no haya sido correctamente confeccionada en el sentido que venimos aconsejando, será enviar información a receptores que no leerán los contenidos de los mensajes, o simplemente no los recibirán porque su dirección no es correcta. Sin contar con las quejas de los usuarios que no solicitaron esos envíos, por la invasión de su intimidad.

Consejos a los PSI y a los administradores de servidores de correo electrónico

Los proveedores de servicio y los administradores de servidores de correo electrónico, deben comprometerse a favorecer la confianza de los usuarios en Internet, e intentar evitar el abuso de terceros de los recursos de que disponen, por el beneficio de ambas partes, usuarios y compañía. Para ello la entidad debe tener en cuenta una serie de **recomendaciones** que se detallan a continuación:

1. **Se debe disponer de una política institucional para el uso correcto de los recursos de la red (dominio y rango de direcciones IP asignadas) que delimite sus responsabilidades**: La institución debe responsabilizarse del servicio de correo electrónico que se ofrezca a instituciones autorizadas (dominios residentes, fundaciones, organismos independientes, etc.), a las que se deberá explicar y deberán aceptar las condiciones de uso.
2. **Se deben tomar las medidas mínimas de seguridad para evitar abusos de los recursos de la compañía**: La institución tiene que garantizar que todos los servidores de correo electrónico de su red están adecuadamente configurados y cumplen con unas determinadas pautas que garantizan la seguridad.
3. **En caso de que la institución cuente con foros o listas de distribución, debe disponer de unas medidas mínimas para proteger el servicio:** Éstas se han comentado en el epígrafe anterior.
4. **En el caso de recabar datos de carácter personal o direcciones de correo electrónico, se debe proporcionar mecanismos para que el usuario pueda ejercer sus derechos de rectificación y cancelación de los mismos (según lo especificado en la LOPD), así como informar de la forma de llevarlo a cabo:** Hay que tener en cuenta que la institución es responsable de las consecuencias que impliquen el almacenamiento y manipulación automática de datos de direcciones de correo electrónico por parte de los usuarios de su red. Los consejos sobre este tema también han sido abordados en el epígrafe anterior.
5. **Se deben atender las quejas y comunicaciones de los usuarios:** Es necesario garantizar que se gestionan las incidencias que llegan a la dirección abuse@dominiodelaempresa.es, o a los buzones o formularios que la empresa disponga para este fin, actuando de la manera que corresponda según el caso.

   La institución debe dar a conocer la existencia de dichas direcciones, e indicar el tipo de información que es necesario enviar para poder tomar acciones, documentándola en su caso. Es necesario contestar a las quejas y denuncias que lleguen a dicho buzón, sean locales o externas. Así, cuando se ha demostrado un incidente de abuso interno, la institución se debe comprometer a tomar las medidas oportunas contra el involucrado de acuerdo con la política de uso correcto de la red de dicha institución y la legislación vigente.

6. **La institución debe garantizar que los actuales y futuros usuarios, con dirección de correo electrónico de dominio interno, son informados de manera clara, comprensible y de fácil localización** sobre los siguientes aspectos:

   - Identificación de la empresa o proveedor. Según lo dispuesto en la LSSI sobre los prestadores de servicios de la Sociedad de la Información, se deben incluir todos los datos de la compañía.

   - Dirección de correo electrónico o postal donde los usuarios puedan hacer saber al administrador o responsable, incidentes o quejas. También los datos que se deben adjuntar para que puedan ser debidamente atendidos.

   - Implicaciones del uso del correo electrónico con direcciones del dominio de la institución.

   - Política de uso correcto de los recursos y servicios de la empresa, que ésta adquiere con los usuarios y que desea hacer pública, así como las acciones que se llevarán a cabo en caso de incumplimiento.

   - Política de seguridad y privacidad, en la que la compañía deberá explicar el tratamiento y uso que hace de los datos que obtiene (direcciones IP, cookies, direcciones de correo y otros datos).

   - Conceptos básicos y efectos de los abusos del correo electrónico, así como enlaces a las instituciones que la compañía crea oportuno para generar confianza en los usuarios, como por ejemplo, a la agencia de protección de datos, cuerpos de seguridad u organizaciones de consumidores.

El proveedor de servicio y los administradores de servidores de correo electrónico, pueden intentar prevenir el Spam desde tres distintos frentes, que ya han sido mencionados en las recomendaciones anteriores, pero que a continuación pasamos a comentar en mayor profundidad.

Correcta definición de una política institucional para el uso del servicio de correo electrónico:

La política institucional es un **documento público, fácilmente accesible desde las páginas web de la organización, avalado por un responsable de máximo nivel**. En él la organización afirma que los usuarios disponen de información sobre los abusos del correo electrónico que pueden llevarse a cabo, sus implicaciones y problemática; Asimismo se garantiza que este servicio es utilizado de acuerdo con unas mínimas normas éticas, y en general, se asegura un correcto servicio. Con esta política se persigue que la organización sea calificada como "fiable", en este sentido, de cara al exterior.

Los **objetivos** de la política institucional deberían estar ligados a un documento de "términos y condiciones de uso", el cual no tendría objetivos jurídicos sino sólo un compromiso formal, público y activo para luchar y perseguir, dentro de sus posibilidades, cualquier abuso local y externo referido al problema del Spam. Además, debe apuntar cuáles serán las posibles medidas técnicas contra usuarios que hayan cometido cualquier infracción relacionada con los abusos que estamos tratando.

La redacción de estos documentos es de gran importancia, sin embargo, según un estudio realizado por la compañía Sybari[11] , sólo una tercera parte de las compañías europeas dice tener redactado un documento interno de definición de Spam. De éstas, sólo la mitad lo ha puesto en práctica dándolo a conocer a sus trabajadores y departamentos. En el otro extremo, el 28 % ni siquiera tiene prevista su emisión.

La organización RedIris propone un ejemplo de documento tipo para la "política institucional" de una organización de su comunidad y otro "documento de términos y condiciones de uso del correo electrónico" (www.rediris.es/mail/abuso). Con las correcciones pertinentes, estos documentos podrían ser de aplicación para cualquier institución:

Política institucional acerca del problema del ACE (Abusos del Correo Electrónico):

Nuestra organización reconoce los principios de libertad de expresión y privacidad de información como partes implicadas en el servicio de correo electrónico. Nuestra organización ofrece unos niveles de privacidad similares a los que se ofrecen en el correo postal tradicional y en las conversaciones telefónicas.

Nuestra institución anima al uso del correo electrónico y respeta la privacidad de los usuarios. Nunca de forma rutinaria se realizarán monitorizaciones o inspecciones de los buzones sin el consentimiento del propietario del buzón asignado por los responsables de nuestra organización. Sin embargo podrá denegarse el acceso a los servicios de correo electrónico locales e inspeccionar, monitorizar y cancelar un buzón privado:

- Cuando haya requerimientos legales.

[11] Estudio realizado por la compañía Sybari a más de un centenar de compañías de dieciséis países (entre los que figura España). Sus conclusiones han sido obtenidas del artículo "Las empresas creen que las leyes contra el Spam son insuficientes" (12 de noviembre de 2003), www.vunet.com

- Cuando haya sospechas fundadas de violación de la política interna de la institución, como comercio electrónico, falsificación de direcciones etc. Evitando caer en rumores, chismorreos u otras evidencias no fundadas y previo consentimiento del máximo responsable del servicio.
- Cuando por circunstancias de emergencia, donde no actuar pudiera repercutir gravemente en el servicio general a la comunidad.

Disposiciones generales:

1. Nuestra institución es responsable de cualquier nombre de dominio, DNS de tercer nivel, bajo el dominio "org.es".
2. Dentro de los servicios de comunicaciones que nuestra institución provee, se ofrece un buzón de correo electrónico y una o varias máquinas para el encaminamiento y recogida de correo a/desde Internet a todo nuestro personal que lo requiera. Teniendo registro de las personas que los están utilizando bajo las direcciones electrónicas de las que somos responsables.
3. Como gestores del servicio de correo electrónico dentro de nuestra institución, nos reservamos el derecho de tomar las medidas sancionadoras oportunas contra los usuarios internos y externos que realicen cualquiera de los abusos incluidos en el Anexo 1.
4. Disponemos de suficiente información acerca de:

- Las diversas actividades que trascienden los objetivos habituales del uso del servicio de correo electrónico que presta nuestra Institución (Anexo 1).
- Los perjuicios directos o indirectos que este problema ocasiona a nuestros propios usuarios, rendimientos de máquinas, líneas de comunicaciones, etc., reflejados en el Anexo 2.

Objetivos:

Este documento ha sido escrito con los siguientes objetivos en mente:

1. Proteger la reputación y buen nombre de nuestra institución en la Red (Internet).
2. Garantizar la seguridad, rendimientos y privacidad de los sistemas de nuestra organización y de los demás.
3. Evitar situaciones que puedan causar a nuestra organización algún tipo de responsabilidad civil o penal.
4. Preservar la privacidad y seguridad de nuestros usuarios.
5. Proteger la labor realizada por las personas que trabajan en nuestros servicios de comunicaciones frente a ciertos actos indeseables.

Ámbito de aplicación:

1. Todas las máquinas de nuestra institución capaces de encaminar correo electrónico (estafetas).
2. Todas las piezas de mensajes (texto, cabeceras y trazas) residentes en ordenadores propiedad de nuestra institución.
3. Todos los usuarios responsables de buzones asignados por los responsables de nuestra organización.
4. Todos los servicios internos que utilizan el correo electrónico, como por ejemplo los servidores de listas de distribución y respondedores automáticos.

Esta política sólo se aplica al correo electrónico en formato electrónico y no es aplicable a correo electrónico en formato papel.

Compromisos:

1. Emplear los recursos técnicos y humanos a nuestro alcance para intentar evitar cualquiera de los tipos de abusos reflejados en el Anexo 2.
2. Poner a disposición pública y fácilmente accesible de nuestros usuarios, propietarios de buzones institucionales, de la siguiente información:

- "Términos y condiciones de uso del servicio de correo electrónico" (se adjunta a continuación).
- "Abuso del correo electrónico y sus implicaciones".

3. Poner a disposición de los usuarios del servicio de correo electrónico de la institución los procedimientos adecuados para que puedan actuar contra los abusos externos del correo que sufrirán en sus propios buzones (correo basura o Spamming).
4. Intentar mantener nuestros servidores de correo institucionales con las últimas mejoras técnicas (actualizaciones, parches, filtros, etc.) para defenderlos de los ataques definidos en el Anexo 1.
5. Proteger los datos personales de nuestros usuarios: nombre, apellidos y dirección de correo electrónico de acuerdo a la legislación española reflejada en la LORTAD (Ley Orgánica de Tratamiento de Datos - Ley Orgánica 5/1992 del 29 octubre) .
6. Intentar impedir y perseguir a usuarios internos que realicen cualquiera de las actividades definidas en el Anexo 1.
7. Coordinarnos con el equipo gestor del Programa RedIRIS para colaborar en la creación de un frente común frente a este tipo de actividades definidas en el Anexo 1. Esto incluye la colaboración al nivel necesario para la persecución de estas actividades.
8. Dedicar un buzón (abuse@organizacion.es) donde puedan ser enviados y atendidos los incidentes.

Aprobado por el Director de la organización

Documento tipo para la política institucional, en relación con el problema del abuso del correo electrónico de una organización:

En apoyo de los objetivos fundamentales de nuestra institución: enseñanza e investigación y respetando los principios de libertad de expresión y privacidad de información, se ofrece una serie de recursos de red, comunicaciones y de información a nuestra comunidad. El acceso a estos recursos es un privilegio que está condicionado a la aceptación de la Política de Utilización de estos recursos. Se debe reconocer que la calidad de estos servicios depende en gran medida de la responsabilidad individual de los usuarios.

En caso de no entender completamente alguno de estos apartados póngase en contacto con el responsable del servicio en le teléfono 9xxx o el buzón postmaster@org.es. Las condiciones que se exponen pueden ser actualizadas para acoplarse a nuevas situaciones.

1. Los usuarios son completamente responsables de todas las actividades realizadas con sus cuentas de acceso y su buzón asociado en nuestra organización.

2. Es una falta grave facilitar y/o ofrecer nuestra cuenta y buzón a personas no autorizadas.

3. Los usuarios deben ser conscientes de la diferencia de utilizar direcciones de correo electrónico suministradas por nuestra institución, o privadas ofrecidas por cualquier proveedor Internet. El campo remite de las cabeceras de correo indica el origen al que pertenece el emisor de un mensaje, por lo que hay que tener en cuenta las repercusiones. Resumiendo, para temas privados deben ser usados los buzones del proveedor Internet, pero nunca desde las instalaciones de nuestra organización y para temas profesionales serán usadas las direcciones de nuestra organización.

4. Correo personal. Los servicios de correo electrónico suministrados por nuestra organización pueden ser usados de forma incidental para temas personales excepto si:

- interfieren con el rendimiento del propio servicio,
- interfieren en las labores propias de los gestores del servicio,
- suponen un alto coste para nuestra organización.

Los mensajes de tipo personal están sujetos a los términos y condiciones de este documento.

5. Debe de ser consciente de los términos, prohibiciones y perjuicios englobados en el documento "Abusos del Correo Electrónico".

6. Está prohibida la utilización en nuestras instalaciones de buzones de correo electrónico de otros proveedores Internet:

- Es ilegal utilizar como encaminador de correo otras máquinas que no sean las puestas a disposición por nuestra organización.
- Es incorrecto enviar mensajes con direcciones no asignadas por los responsables de nuestra institución y en general es ilegal manipular las cabeceras de correo electrónico saliente.

7. El correo electrónico es una herramienta para el intercambio de información entre personas no es un herramienta de difusión de información. Para ello existen otros canales más adecuados y efectivos, para lo que debe de ponerse en contacto con los responsables del servicio.

8. La violación de la seguridad de los sistemas y/o red pueden incurrir en responsabilidades civiles y criminales. Nuestra organización colaborará al máximo de sus posibilidades para investigar este tipo de actos, incluyendo la cooperación con la Justicia.

9. No es correcto enviar correo a personas que no desean recibirlo. Si le solicitan detener ésta práctica deberá de hacerlo. Si nuestra organización recibe quejas, denuncias o reclamaciones por estas prácticas se tomarán las medidas sancionadoras adecuadas.

10. Está completamente prohibido realizar cualquiera de los tipos de abusos definidos en el documento "Abusos del Correo Electrónico". Además de las siguientes actividades:

- Utilizar el correo electrónico para cualquier propósito comercial o financiero.
- No se debe participar en la propagación de cartas encadenadas o participar en esquemas piramidales o temas similares.
- Distribuir de forma masiva grandes cantidades de mensajes con contenidos inapropiados para nuestra organización.
- Está prohibido falsificar las cabeceras de correo electrónico.
- Las cuentas de nuestra organización no deben ser usadas para recoger correo de buzones de otro proveedor de Internet.

11. Estará penalizado con la cancelación del buzón, el envío a foros de discusión (listas de distribución y/o newsgroups) de mensajes que comprometan la reputación de nuestra organización o violen cualquiera de leyes españolas

Aprobado por el Director de la organización

Configuración adecuada de los servidores de correo:

La correcta configuración de los servidores de correo electrónico, ayudará a proteger el sistema de usos indebidos.

Una forma de comprobar si una organización tiene los servidores de correo electrónico mal configurados es dirigirse a www.mail-abuse.org/tsi En este site se puede encontrar abundante documentación sobre los pasos a seguir, dependiendo del sistema operativo y del software que se tenga instalado.

El servidor principal de correo electrónico de una organización debe ser el **centro desde el que se coordine la seguridad de todo el servicio en la organización**. Los requisitos recomendables a tener en cuenta para configurarlo, desde el punto de vista de la seguridad, se detallan a continuación:

1. Definir el espacio de direcciones de correo lógicas de las que es responsable el servidor, sin omitir los dominios virtuales.
2. Definir claramente las direcciones IP de las redes a las que se da servicio de correo electrónico, y que deberán ser las únicas que tengan permiso para utilizar el servidor principal en el encaminamiento de e-mails. A cualquier otra se le debe denegar el servicio de la transacción SMTP.
3. Utilizar procedimientos de autenticación SMTP AUTH de forma que sólo se permite el uso del servidor si:

   a) El emisor del mensaje es un usuario local que se ha autentificado correctamente, o

   b) El emisor es un usuario externo y el destinatario un usuario local.

   Además, se debería evitar que un usuario autentificado pudiese utilizar cualquier dirección de e-mail y sólo permitirle utilizar la/s dirección/es de correo asociadas a su nombre de usuario y contraseña (esta recomendación substituiría totalmente las recomendaciones 2 y 3).
4. Comprobar la identificación HELO/EHLO del cliente SMTP. Se debe tener en cuenta que esta recomendación, junto con la comprobación de la resolución inversa, conllevan problemas ya que hay muchos servidores con estos fallos de configuración.
5. No aceptar e-mails desde o destinadas a direcciones externas al dominio de la organización. Este principio junto con el anterior, debe denegar el encaminamiento de mensajes de correo electrónico desde cualquier dirección IP exterior, destinada a cualquier dirección IP exterior, independientemente de cual sea la dirección de origen que aparezca en el campo "mail from:". De esta forma nos aseguramos que los servidores no estén abiertos.

6. Comprobar las resoluciones DNS para rechazar conexiones SMTP de servidores que no dispongan de resolución inversa, y para rechazar mensajes en los que durante la sesión SMTP aparezca un valor de "mail from:" con un dominio incorrecto.

7. Implementación de listas de acceso de direcciones de dominios, usuarios y/o direcciones que se les deniega el acceso, por no tener protegido su servidor de correo, por ser máquinas de proveedores de servicio que dan soporte a Spammers, o por ser máquinas que hacen Spam; así como disponer de herramientas para filtrar estas direcciones.

8. Limitar el número de mensajes que un usuario puede enviar por minuto y comprobar periódicamente el número total de mensajes que se envían desde cada uno, para evitar que un Spammer se aloje entre nuestros usuarios.

9. Configurar los servidores para que proporcionen códigos de error normalizados y almacenar la identidad de las máquinas (dirección IP), e información correcta y suficiente donde se reflejen las trazas de todas las transacciones SMTP, así como la fecha correcta de los envíos. Se debe conservar durante un tiempo razonable estos ficheros y revisarlos y actualizados de forma periódica. Con estas medidas se podrán depurar y mejorar los errores que se presenten, garantizando que los e-mails generados dentro de la red pueden ser identificados y seguidos hasta su origen, así como identificar prácticas fraudulentas.

De este modo no se debe permitir el encaminamiento desde o a servidores terceros que no pertenezcan a la organización. Con ello se habrá solucionado este problema y no se estará siendo cómplice de Spammers.

Estas recomendaciones se completan/amplian en el apartado 12.1, del capítulo 12 de esta publicación.

Legislación

La legislación es una de las posibles medidas preventivas de lucha contra el Spam, puesto que lo que se persigue en último fin con su creación y aplicación, es intimidar con sanciones las actividades del Spam para evitar que se produzcan, en la medida de lo posible.

En el capítulo 9 de esta publicación estudiaremos con detalle las leyes que regulan el funcionamiento del correo electrónico y, en concreto, aquéllas que tratan de impedir la práctica del Spam. Por ello ahora nos limitamos a realizar un resumen de las mismas.

Situación en la Unión Europea:

La UE aprobó la **Directiva 2002/58/CE** ("Directiva sobre la intimidad y las comunicaciones electrónicas") que prohíbe el envío de comunicaciones comerciales no solicitadas a personas físicas en toda la Unión Europea. La normativa se basa en las siguientes reglas fundamentales:

- El principio de consentimiento previo (opt-in)
- Todos los mensajes deben mencionar una dirección de respuesta válida donde el abonado pueda oponerse al envío de mensajes posteriores.
- Todos los mensajes enviados a direcciones conseguidas sin conocimiento de los destinatarios son considerados ilegales y cada estado miembro puede imponer multas por ello. La única excepción que se tiene en cuenta es el caso del marco limitado de las relaciones entre clientes y empresas.

Esta directiva europea debía ser transpuesta a la legislación nacional de cada estado con fecha máxima de octubre de 2003, sin embargo Bruselas se ha visto obligada a abrir procedimientos de infracción contra países como Francia, Bélgica, Holanda, Luxemburgo, Portugal, Finlandia, Suecia y Alemania por no haber cumplido los plazos previstos para introducir a escala nacional esta normativa.

De esta forma, a fecha de enero de 2004, los países que han adoptado una legislación que prohíbe el Spam mediante un régimen opt-in son Dinamarca, España, Grecia, Italia, Finlandia, Alemania, Bélgica, Austria y el Reino Unido; de los cuales Finlandia, Alemania y Bélgica todavía no han adoptado la totalidad de competencias de la mencionada directiva.

La ley contra el Spam del Reino Unido, que entró en vigor el 11 de diciembre de 2003 ha levantado gran controversia, puesto que ha incluido la posibilidad de poder extraditar a los Spammers que envíen mensajes a usuarios del Reino Unido desde otros países, para poder ser juzgados allí. Asimismo ha sido criticada porque impone una pena máxima de 5.000 libras esterlinas (9.255 dólares). Los expertos señalan que no es disuasoria, puesto que algunos de ellos obtienen de 20.000 a 30.000 libras (de 37.020 a 56.030 dólares) por semana por realizar los envíos masivos. En Estados Unidos, por ejemplo, se ha indemnizado a compañías como American Online, con casi siete millones de dólares por daños en un caso de Spam.

Situación en España:

La legislación española contempla, regula y penaliza las actividades de Spam en el contexto de la **LSSI (Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico)**, en el Título III, de "comunicaciones comerciales por vía electrónica".

Tras su entrada en vigor se prohibía totalmente el envío de Spam en España. Sin embargo, y posteriormente a esta legislación, se han introducido unos cambios en la **Ley General de Telecomunicaciones** (LGT, aprobados a 16 de diciembre de 2003) que afectan a la LSSI.

Así, por ejemplo, en la disposición primera, modificación del artículo 21, permite la utilización del correo electrónico para remitir mensajes a aquellas personas o empresas con las que se haya mantenido una relación contractual sin necesidad de una autorización previa por parte de éstas. Textualmente dice: "*Lo dispuesto en el apartado anterior (referente a la prohibición de envíos comerciales) no será de aplicación cuando exista una relación contractual previa*".

Según fuentes del Ministerio esta "redefinición" del concepto de Spam tuvo lugar por la necesidad de adaptarse a la normativa europea en este sentido (Directiva 2002/58/CE), que autoriza las comunicaciones con el cliente siempre que éste haya mantenido una relación con la firma y no haya manifestado expresamente su oposición a recibir este tipo de mensajes. Esta nueva formulación satisface también a las peticiones que desde distintas asociaciones empresariales vinculadas al comercio electrónico se realizaron en tal sentido. Éstas se encontraban con la imposibilidad legal de informar a sus clientes de las promociones y ofertas por correo electrónico, mientras desde fuera de nuestro país, se les bombardea con todo tipo de proposiciones.

Sin embargo, esta nueva situación hace que **un tipo de Spam sea legal en España**, no conservándose en sentido estricto la opción del usuario de no recibir ningún tipo de mensaje no solicitado sin consentimiento explícito previo. Usuarios, asociaciones de empresas de marketing interactivo y organismos de lucha contra el Spam comparten la opinión de prohibir todo tipo de Spam.

Para evaluar adecuadamente la situación, pensemos en las bases de datos de las grandes empresas con las que cualquier ciudadano contrata los suministros básicos: Telefónica, Fecsa-Endesa, Iberdrola, Gas Natural, Bancos y Cajas de Ahorros, etc. En la actual situación legislativa, dichas empresas quedan legitimadas para inundar el buzón de correo electrónico del usuario, ofreciéndole productos o servicios de su propia empresa que sean similares a los inicialmente contratados. Y del mismo modo, y en virtud del principio de igualdad, cualquier otra empresa, sea multinacional o pyme.

Dado el carácter internacional del Spam, **la legislación nacional no resulta muy efectiva para evitar el problema dentro de España**. Conectarse a Internet rompe toda forma de fronteras: Es posible delimitar puntos de origen pero no puntos de encuentro o puntos de paso de la información.

Una persona en Hong-Kong usando una cuenta de correo web de un proveedor de servicios en Argentina, puede enviar un mensaje Spam a usuarios en "n" países (de manera simultánea), entre ellos a uno que tiene su cuenta en un servidor español.

En un caso cómo éste, aunque la víctima del Spam sea española, no se puede acudir a la LSSI, ni a las directivas europeas. Por ello, la legislación nacional es necesaria, pero no demasiado útil para prevenir o combatir el Spam, ya que sólo puede regular las emisiones de Spam con origen en máquinas ubicadas en territorio nacional.

Es de destacar que, aunque la legislación española prohíbe el Spam en casi todas sus formas, a fecha de marzo de 2003 España estaba entre los 10 primeros países productores de Spam. Este dato nos obliga a reflexionar sobre la eficacia de la situación legislativa actual.

Opinión de las empresas acerca de la legislación:

Recogemos en este epígrafe la opinión de varias empresas, elaborada a partir de dos estudios[12].

A finales de 2002 (tras la aprobación de la LSSI sin ninguna modificación), se observa que en España la mayoría de las empresas consultadas consideran aceptable la legislación que afecta a sus comunicaciones interactivas (un 49%). Este dato muestra una falta de opinión crítica al respecto causada por el desconocimiento general acerca del tema, aspecto que se pone aún más de manifiesto dado que casi un tercio de las empresas consultadas (31%) no sabe o no contesta ante esta pregunta.

---

[12] "IV Estudio sobre el Marketing y la Publicidad en Medios Interactivos 2002", realizado por AGEMDI-fecemd", (Asociación de Agencias de Marketing Directo e Interactivo-Federación Española de Comercio Electrónico y Marketing Directo). Estudio realizado a 258 empresas españolas anunciantes/usuarias de publicidad con más de 11 empleados, independientemente de su sector de actividad de forma aleatoria, que dirigen sus productos y servicios al consumidor final. Estudio realizado por la compañía Sybari a más de un centenar de compañías de dieciséis países (entre los que figura España) y cuyas conclusiones han sido obtenidas del artículo "Las empresas creen que las leyes contra el Spam son insuficientes" (12 de noviembre de 2003), www.vunet.com

Algo parecido ocurre respecto a la pregunta de *"¿han disminuido sus acciones de marketing on line a causa de la ley?".* La ley no ha afectado a casi ninguna empresa y un 30,6% de las empresas tampoco sabe o no contesta a esta pregunta. Podemos apreciar cómo el desconocimiento de la nueva legislación de Internet es algo llamativo y preocupante.

Estas cifras ponen de manifiesto que la entrada en vigor de esta ley no ha redundado en importantes trabas a las empresas que llevan a cabo publicidad on line.

Si nos situamos en 2003, la mitad de las empresas europeas considera que la legislación sobre las comunicaciones electrónicas no afectará en absoluto a la recepción masiva de e-mails comerciales no solicitados vía Internet. El estudio revela que apenas una de cada veinte empresas cree que la acción de los reguladores pondrá fin al Spam, mientras que una de cada cinco augura una reducción de esta práctica. En la misma línea, casi la mitad de las compañías encuestadas, desconfían completamente de que sus gobiernos vayan a implantar una legislación contra el Spam eficaz, considerando el porcentaje restante que tan sólo tendrá una eficacia limitada.

Estos datos ponen de manifiesto que **las empresas no creen que la legislación de sus países vaya a ser una herramienta eficaz de lucha contra el Spam**, ya sea porque su naturaleza no sea la adecuada, o porque una legislación no es la solución al problema.

Situación legislativa en Estados Unidos:

Hasta finales de 2003 la situación legislativa en torno al Spam en Estados Unidos era un tanto caótica. Cada estado era libre de adoptar sus propias medidas o de no hacer nada al respecto. La solución a este caos fue aprobar la ley federal "Controling the Assault of Non-Soclicited Pornography and Marketing Act. of 2003" (**CAN-SPAM**).

Ésta crea a partir del 1 de enero de 2004 una situación uniforme para el marketing por e-mail y propone penas para un conjunto de actividades relacionadas con el Spam, como el robo o la obtención de direcciones electrónicas de sitios web. Ésta es la primera iniciativa de reglamentación de contenidos en Internet en Estados Unidos desde sus inicios en los años 90 y ha sido aprobada tras conocer los resultados del estudio realizado por la FTC (Federal Trade Commission), en el que se advertía de que la mayoría de los mensajes eran fraudulentos y de la existencia de abundantes mensajes con material pornográfico.

El objetivo principal de esta ley, no es propiamente combatir el Spam, sino **erradicar los mensajes pornográficos y fraudulentos**. Por tanto, en lo esencial, la ley legaliza el Spam: Permite a cualquier sujeto o empresa enviar publicidad masiva, hasta que el propio usuario solicite ser dado de baja en la lista. Este principio de **"solicitud activa de baja en la lista" (opt-out)** se contrapone totalmente al principio de "solicitud activa de alta en la lista" (opt-in), aprobado anteriormente en algunos estados como California. El problema para California, al igual que para otros estados que ya habían dictado leyes contra el Spam, es que éstas han quedado sin efecto tras la entrada en vigor de la CAN-SPAM, debido a que ésta se trata de una ley federal.

Podemos apuntar una serie de reflexiones en torno a esta ley:

- No prohíbe la recogida de direcciones sin el consentimiento del usuario, sino solamente su recopilación mediante el uso de programas especiales o el envío masivo de mensajes a servidores intentando "*adivinar*" direcciones válidas. De esta forma la reflexión es inmediata: ¿Cómo van a saber las autoridades si se ha conseguido una dirección de forma lícita o ilegal?

- Se permite el envío de Spam mediante opt-out, lo que en la práctica permite a los Spammers continuar haciendo lo mismo que hasta ahora. En efecto, muchas veces cuando nos damos de baja de una lista de Spam, al día siguiente empezamos a recibir mensajes de varias más. Esto es así porque muchos Spammers dan nuestra dirección de baja de forma efectiva, pero la revenden inmediatamente a otras empresas o a sus propias filiales, que a partir de entonces empiezan a usarla con la misma filosofía. En la práctica, esta ley podría venir a legalizar esta situación.

- Presupone que un usuario quiere recibir publicidad mientras no indique lo contrario, lo que choca frontalmente con lo que solicitan la mayoría de agentes en la lucha contra el Spam: Que solamente reciban publicidad aquellos internautas que lo consientan.

Al margen de la discusión de por qué tiene un usuario que borrarse de una lista en la que nunca dio su consentimiento para que le incluyeran, está el hecho de la **tremenda generación de mensajes que conlleva la aceptación de las comunicaciones comerciales mediante opt-out**. El método de envío de mensajes de listas de e-mails obtenidas a través de opt-out es insostenible, puesto que el número de e-mails que se generarían como consecuencia de ello colapsaría el sistema de correo electrónico, si sólo un porcentaje pequeño de empresas en Internet decidieran emplear este método de promoción. Veámoslo con un ejemplo numérico.

Si sólo *"una décima parte del 1%"* de los usuarios de Internet decidieran hacer envíos masivos de e-mails a una velocidad moderada con un acceso vía módem y un PC, enviarían un promedio de 100.000 mensajes al día. Entonces todos los usuarios del mundo recibirían 100 mensajes Spam al día.

Si el 1% de los usuarios hiciera ese número de envíos masivos, todos los usuarios recibirían 1000 Spam al día.

Por ello, no puede ser razonable permitir el uso del método opt-out para las comunicaciones comerciales por e-mail, ya que sería como pedir a la gente que enviara 100 mensajes cada día para darse de baja de una lista. Todo ello generaría un volumen de correo que no sería sostenible por las redes.

Conclusiones:

En muchas ocasiones, la mentalidad de los gobiernos en materia de Sociedad de la Información no siempre es la adecuada para combatir problemas tan importantes como el Spam.

En la **Unión Europea** se insta a todos los países que la componen a prohibir toda forma de comunicación comercial no solicitada y a la forma de envío basado en opt-in. Sin embargo se deja un agujero a través del cual **cualquier empresa puede enviar las comunicaciones vía correo electrónico siempre que el receptor haya sido cliente suyo**. Ello puede redundar en que el usuario se vea saturado de mensajes de compañías de las que es cliente.

Al menos la situación anterior acota el Spam de alguna manera. Sin embargo, la legislación aprobada en **Estados Unidos**, en nuestra opinión, lejos de intentar solucionar el problema, lo legaliza. Así, **legitima el envío de comunicaciones comerciales bajo una serie de supuestos bastante amplia, basada en opt-out**. Se presupone que todos los usuarios desean recibir comunicaciones comerciales o Spam de cualquier tema, salvo pornografía. Esta situación es bastante preocupante dado que un gran porcentaje del Spam que circula por Internet proviene de Estados Unidos.

Por otra parte, e independientemente de cómo esté redactada una ley contra el Spam, tendrá valor únicamente para emisores y receptores que se encuentren en el país de aplicación. Por tanto, se trata de una medida para combatir el Spam que es necesaria pero de efectividad bastante limitada.

Aunque se presuponga que la legislación de un país en materia de Spam esté bien redactada, los Spammers siempre podrían buscar otros países sin una legislación adecuada desde los que bombardear a los usuarios. Resultaría, en consecuencia, más efectiva, la posibilidad de **extraditar a los Spammers a los países hacia los que dirigen sus envíos,** juzgándolos allí, tal y como se contempla en la ley contra el Spam del Reino Unido.

En cualquier caso, aún cumpliéndose que la legislación fuera realmente eficiente, ésta calificaría al Spam como una práctica ilegal, pero no sería un instrumento para acabar realmente con ella.

6.2. Medidas de lucha contra el Spam

Una vez que el Spam se recibe en un equipo:

- Hay que intentar localizar la fuente originaria,
- Enviar una comunicación al responsable del primer servidor desde donde se realizó el envío,
- Filtrarlo de una forma segura para separarlo de los mensajes útiles y, finalmente,
- Denunciar al emisor de éste en aquellos organismos que investigan o persiguen a los Spammers

Tenemos al alcance de nuestra mano una serie de herramientas tecnológicas para evitar el Spam que podemos clasificar en dos categorías:

- Aquéllas que se puede aplicar **antes de recibir los mensajes en el servidor destino**: Recurren a un filtrado basado en el análisis de las transacciones SMTP.
- Aquéllas que **filtran los mensajes una vez hayan sido recibidos**. Este proceso de filtrado se puede realizar tanto desde la máquina del usuario, como a nivel del servidor del proveedor de servicio.

Medidas para combatir el Spam impidiendo su recepción

Las medidas adoptadas para que el mensaje que se detecta como Spam no llegue a recibirse en el servidor de correo electrónico, implican que **la transacción SMTP entre el servidor origen y el destino no finaliza con éxito, y por tanto el mensaje es rechazado.** Estas medidas intentan evitar tanto la entrada de Spam en el dominio, como presionar al origen para que no vuelva a intentarlo, ya que éste recibe todos los mensajes de error que se generan al fallar cada una de las transacciones SMTP necesarias para entregar un mensaje.

La decisión de rechazar un mensaje se toma en función del perfil del servidor que pretende enviar el mensaje, o de las características que presenta la cabecera de los mensajes enviados durante el diálogo SMTP.

Estas medidas son más comprometidas en la lucha contra el problema del Spam. Sin embargo también pueden ser más injustas, puesto que catalogan a un servidor sin dar oportunidad a analizar si su mensaje es Spam o no.

Para adoptar este tipo de medidas **es necesaria la configuración del servidor de correo electrónico,** y por tanto éste debe de ser lo suficientemente flexible como para permitirlo.

Los dos servidores de correo más utilizados son Sendmail y el comercializado por Microsoft, que no permiten mucha flexibilidad en su configuración. Como solución podemos optar por servidores más flexibles como **Postfix y Exim**.

Otra alternativa es utilizar un **servidor SMTP proxy flexible frente al servidor de correo electrónico** para permitir este tipo de configuraciones. De esta forma si se quieren implementar en el servidor determinadas medidas de filtrado de mensajes, y éste no lo permite, mediante un servidor proxy podríamos conseguirlo sin necesidad de cambiar el servidor de correo.

A continuación se detalla el empleo de listas negras y otros métodos basados en la configuración del servidor de correo electrónico, con el propósito de luchar contra el Spam antes de su recepción.

Métodos basados en listas negras:

La experiencia demuestra que estas listas bloquean entre el 1% y el 3% del Spam.

A partir de mediados de los años 90, cuando el Spam empezó a despertar, el método más habitual de distribuirlo era usando estafetas ajenas open-relay. Esto no sólo consumía los recursos de la máquina (disco, CPU y líneas de comunicaciones), sino que evitaba cualquier posible medida legal del país de origen. Muchos servidores empezaron a actualizar su configuración para evitar el uso de sus recursos de forma ilegal.

Simultáneamente, la excesiva cantidad de máquinas open-relay provocó la aparición de múltiples iniciativas con diferentes técnicas para **generar listas o bases de datos que contuvieran un registro con los servidores abiertos que existían.** Estar incluido en esa lista implicaba ser poco fiable, porque con mucha probabilidad enviarían Spam.

La gran labor de las listas negras fue **obligar a los servidores de correo a actualizarse**. Además, **dieron a conocer el gran problema del Spam**, constituyéndose como el único mecanismo disponible para combatirlo.

En un primer momento estas bases de datos sólo eran accesibles en local, por lo que cada institución debía tener la suya y no existía coordinación entre ellas. En 1997 la iniciativa MAPS/RBL ideó un **mecanismo de acceso remoto**, en concreto vía DNS (Domain Name System), sistema utilizado actualmente. Se trata de un mecanismo que permite a los servidores de correo electrónico preguntar a dichas bases de datos si la dirección IP (servidor de correo) que se que va a conectar a mi máquina para comenzar una transacción SMTP, está o no incluida. En caso de estarlo la conexión se cierra, y en caso contrario, se continúa con la transacción. Evidentemente estas listas negras disponían de herramientas para comprobar periódicamente si las máquinas seguían siendo open-relay o habían corregido el problema.

A partir de este momento, empezaron a aparecer y venderse numerosas iniciativas de listas negras con diferentes criterios. Hoy en día las listas negras con estafetas open-relays no son las únicas, también existen otras que siguen criterios diferentes como cumplir estrictamente algunos RFCs, listas manuales mantenidas con coordinación internacional, etc. Estas iniciativas obtienen la información de diversas fuentes, entre ellas de las denuncias que introducen los usuarios y de mecanismos vía web, para comprobar si una máquina está o no mal configurada. Incluso hay algunas que escanean los puertos SMTP de toda la red en busca de máquinas que puedan ser incluidas en alguna lista.

A continuación se presenta una tabla con las **listas negras más conocidas actualmente**. En ella se incluye una columna denominada "*Zona DNS*", en la que se especifica el DNS que utiliza cada una de ellas. En efecto, las direcciones IP contenidas en las listas se reflejan en una zona inversa del DNS de la organización que lleva la iniciativa, que es consultada en tiempo real por los servidores de correo electrónico que las utilizan en cada transacción SMTP.

Nombre	Zona DNS	Descripción
MAPS/RBL/DUL/RSS (www.mail-abuse.org)	blackholes.mail-abuse.org dialups.mail-abuse.org relays.mail-abuse.org rbl-plus.mail-abuse.org	Almacena *open-relays*, rangos de marcado telefónico. Fueron los primeros y una de las mejores iniciativas. En 2000 empezó a comercializarse (MAPS RBL+).
ORDB (www.ordb.org)	relays.ordb.org	Sólo almacena *open-relays*. Actualmente es una de las más sólidas.
ORBZ	orbz.gst-group.co.uk	Una de las más agresivas. Nació en 1998 y murió en 2001 por problemas jurídicos. Una de las históricas.
FIVETEN (www.five-ten-sg.com/blackhole.php)	blackholes.five-ten-sg.com	Almacena diversas fuentes de Spam: Direcciones de grupos de noticias, organizaciones con formularios inseguros, etc.
SPAMHAUS (SBL) (www.Spamhaus.org/sbl)	Spamhaus.relays.osirusoft.com	Lista manual de bloques de IPs de distribuidores masivos de Spam y/o empresas colaboradoras con el Spam.
DSBL (www.dsbl.org)	list.dsbl.org multihop.dsbl.org	Desde abril de 2002. Almacena *open-relays* que ellos mismos comprueban.

RFC-Ignorant (www.RFC-Ignorans.org)	dsn.rfc-ignorant.org	Detecta servidores que incumplen RFCs básicos del correo-e: RFC 2821, 1123, 2142, 954. Se haya en continuo crecimiento.
OSIRUS (www.relays.osirusoft.com)	Relays.osirusoft.com	Almacenan direcciones IP con diferentes criterios: *open-relays*, usuarios y empresas que colaboran con el Spam, servidores de listas que no solicitan confirmación, etc. Actualmente también funciona como agregador de varias listas negras.
Spamcop (www.Spamcop.net)	Bl.Spamcop.net	Una de las mejores. Almacena de forma temporal servidores que simplemente han distribuido Spam.
Spamhaus (www.sbl.Spamhaus.org)	sbl.Spamhaus.org	Almacena *open-relays*, Spammers, etc. Dispone de una amplia red de zonas DNS repartida por Europa y USA.

Tabla 1: Relación simplificada de algunas de las iniciativas de listas negras. Fuente: www.rediris.com

Aclaraciones:

- **RFC 1123:** Indica que cualquier servidor de correo debe disponer de una dirección de correo tipo <postmaster@...>. *"SMTP servers MUST NOT send notification messages about problems transporting notification messages. One way to prevent loops in error reporting is to specify a null reverse-path MAIL FROM:<>".*

- **RFC 1123:** Se refiere a MTAs mal configurados que no soportan *"Mail From:<>"*, porque lo usan falsamente como medida anti-Spam (como por ejemplo Terra). *"The syntax shown in RFC-821 for the MAIL FROM: command omits the case of an empty path: "MAIL FROM: <>" (see RFC-821 Page 15). An empty reverse path MUST be supported".*

- **RFC 2142:** Indica que cualquier servidor de correo debe disponer de una dirección de correo tipo <abuse@..>

- **RFC954:** Básicamente se refiere a direcciones IP que no disponen de datos correctos o desactualizados en las bases de datos *whois*.

Cada lista dispone de su propia **política de criterios** y contempla unos motivos por los que se ingresa o sale de ella. Uno de los aspectos más importantes de una lista negra es la disponibilidad y accesibilidad de un buen soporte rápido de zonas de DNS a ser posible con posibilidad de acceso desde varias partes de mundo. Un acceso lento o una caída de estas zonas supondría un cuello de botella en la entrada de mensajes en los servidores que las utilizan.

El uso de listas negras como medida para combatir el Spam tiene dos **efectos**:

- Por un lado, llevan a cabo un filtrado que aunque no muy efectivo, elimina y reduce el impacto del Spam. Se trata de un filtrado que sólo tiene en cuenta la dirección IP del servidor del que proviene el mensaje, y desprecia otras características que podrían ser mucho mejores indicadores de si se trata de un Spam, como sería el cuerpo y cabecera del mensaje. Por ello **deben usarse como complemento de otras técnicas.**

- Por otro lado, el efecto más beneficioso es que avisan a proveedores y administradores responsables de servidores usados para enviar Spam. Con ello ayudan a mejorar sus configuraciones y a eliminar a los clientes indeseables que realizan envíos masivos. Además, ejercen una medida de presión para evitar que este tipo de práctica pudiera serles rentable.

Sin embargo las listas negras tienen un importante **punto negativo** que se deriva de su propia definición y que hace que mucha gente esté en contra de su uso. **Todos los mensajes procedentes de un servidor que esté incluido en la lista negra, serán rechazados**. Esto conlleva que podrían ser rechazados e-mails correctos procedentes de un servidor de correo electrónico, sin posibilidad de rescatarlos. Además invita a que una organización pueda ser víctima de un Spammer sin saberlo y por ello ser incluida en distintas listas negras. Esto le conllevaría una serie de problemas importantes a la hora de utilizar el correo electrónico, aunque fuera con fines lícitos. De esta forma se estaría castigando a inocentes y dejando impune a los verdaderos culpables.

Por este motivo **es importante elegir cuidadosamente las listas que se vayan a usar**, ya que hay algunas que bloquean rangos completos de direcciones IP simplemente porque un Spammer utilizó una conexión temporal desde este ISP en algún momento.

Desde nuestro punto de vista, y tras estudiar las características de cada una de las listas citadas en la tabla, el uso de **ordb.org** sería positivo para eliminar correo procedente de servidores mal administrados (open-relay), y de esta forma se evitaría denegar el envío a servidores que podrían no ser utilizados por Spammers.

Métodos basados en el análisis del diálogo SMTP:

En esta ocasión, **el servidor comprueba la naturaleza de la cabecera del mensaje que se envía durante el diálogo SMTP**. En función de las diferentes características que presenta, puede calificarlo como Spam y con ello no permitir que la transacción acabe satisfactoriamente.

A continuación analizaremos las **comprobaciones** que más comúnmente realizan los servidores:

- **8 caracteres no ASCII en la línea del asunto**: Actualmente alrededor del 30% del Spam se origina en China, Taiwán u otros países asiáticos. Si se está seguro de que no se van a recibir mensajes en idiomas orientales entonces se pueden rechazar mensajes de correo que tengan 8 caracteres no ASCII en el asunto. Este método es bastante bueno y elimina entre 20-30% de los mensajes Spam que podrían llegar. Esta medida está hoy en día implementada en la mayoría de los servidores, por lo que no es muy común encontrarse con Spam que provenga de estos países.
- **Listas con direcciones en el campo "From:" ("De:") de Spammers conocidos:** Esto era efectivo en 1997, pero hoy en día no funcionaría, pues los Spammers usan direcciones falsas o de usuarios inocentes.
- **Emisores de dominio desconocido**: Algunos Spammers usan direcciones que no existen en el campo "From:". Se puede conocer a priori la parte del nombre de dominio e investigar si existe a través de un servidor DNS. Esto rechaza aproximadamente entre el 10 y el 15% del Spam. Esta medida es adecuada porque el usuario normalmente no querría recibir esta clase de mensajes, ya que no podría responderlos aún si no fueran Spam.
- **Callback**: Establece una conexión con el servidor del dominio y simula la entrega de un mensaje a esa dirección.
- Comprobar la **existencia de la dirección usada en la orden MAIL FROM.**
- **Dirección IP que no tiene registro en el DNS**: Se comprueba que la dirección desde la cual se recibe el mensaje pueda ser convertida en un nombre de dominio. Esta medida rechaza bastantes mensajes, sin embargo no es una buena opción porque no comprueba si el administrador del sistema del servidor de correo es bueno, sino si tiene un buen proveedor de red vertical. Los proveedores de servicio compran las direcciones IP de sus servidores de red vertical y éstos, compran a su vez en servidores de red vertical mayores. Esta cadena normalmente involucra a varios proveedores verticales, por lo que todos tienen que configurar su DNS correctamente para que la cadena de comprobaciones funcione. Si algún intermediario en el proceso comete un error o no quiere configurarlo, entonces no funciona. Podemos concluir que esta medida no aporta mucho con respecto al carácter del servidor de correo individual que se encuentra al final de la cadena, sino más bien del proceso anterior de configuración de direcciones.
- **Requerir comando "HELO":** Cuando dos servidores de correo se comunican entre sí vía SMTP, establecen un diálogo en el que primero envían el comando "HELO", que contiene entre otros datos, el nombre del servidor. Algunos programas de software de Spam no lo hacen. Filtrar los mensajes que provengan de transacciones de este tipo, rechaza entre 1-5% del Spam.

- **Requerir comando "HELO" y rechazar servidores desconocidos**: Tomar el nombre que se obtiene en el comando "HELO" y comprobar en el DNS si es un servidor correctamente registrado. Esto funciona en base a que generalmente un Spammer que usa una conexión telefónica temporal, no configurará un registro DNS válido para ello. Con esta comprobación se bloquea entre el 70 y el 80% del Spam, pero también puede rechazar muchos mensajes legítimos que provienen de sitios con múltiples servidores de correo, en donde un administrador del sistema olvidó teclear los nombres de todos los servidores en el DNS.

Todas estas medidas contribuyen a rechazar un tanto por ciento del Spam que llega al servidor, sin embargo conllevan que un gran porcentaje de mensajes válidos sean también rechazados, por provenir de un servidor en el que no se han configurado correctamente alguna de las características que se han comentado.

Su principal ventaja es que no representa un alto consumo de capacidad de proceso en el servidor. Además, aunque se rechacen mensajes válidos, el emisor recibirá un aviso en el que se le advierte que su mensaje no ha sido entregado, por lo que podrá tomar medidas al respecto.

Medidas posteriores a la recepción del mensaje. Filtrado basado en contenidos

Al hablar de medidas posteriores a la recepción del mensaje, nos referimos con ello a las que se toman después de que el Spam haya llegado a los servidores o a los buzones. Implican, por tanto, que la transacción SMTP entre el servidor origen y el destino ha concluido con éxito: El mensaje ha sido depositado en la estafeta local.

Funcionan según la siguiente filosofía: **Si se detecta algún patrón de texto que aparezca a menudo en el Spam, pero no en mensajes legítimos, entonces la siguiente vez que se encuentre sería razonable asumir que ese mensaje, probablemente, es Spam.**

Este tipo de filtrado se puede realizar tanto desde la máquina del usuario, como a nivel del servidor de correo electrónico. Desde este punto de vista, **clasificamos las medidas de filtrado de contenidos** en dos grupos:

- **Filtros de contenido instalados en el cliente de correo electrónico o usuario final**: Analizan cadenas de datos que puedan encajar con el contenido de la cabecera o del cuerpo del mensaje tras la recepción de éste en el buzón del usuario. Como resultado de este análisis se decide si el mensaje es Spam o no.

  Con los mensajes calificados como Spam se puede proceder de diversas formas: Borrarlos directamente o trasladarlos a una carpeta para que el usuario pueda examinarla en busca de algún mensaje válido. Gracias al filtro, el correo no deseado no se ve y por tanto no molesta. Además, permite trasladar al destinatario la decisión de configurar sus propios filtros y decidir, por tanto, los mensajes que quiere ver y los que no.

Sin embargo, esta técnica no soluciona la recepción del Spam vía protocolos POP o IMAP, con los problemas de consumo de recursos que conlleva, ya que lo que realmente hace es ocultar al usuario lo que ya ha llegado a su buzón.

- **Filtros de contenido instalados en el servidor de correo electrónico**: En este caso, el análisis que determina si el mensaje es Spam se realiza en el servidor. En él también se toma la decisión de la conservación de los mensajes interceptados en directorios de cuarentena para su posterior revisión, o su borrado. Por tanto, en este caso quien decide los mensajes que son calificados como Spam es el responsable del servidor. Los filtros en los servidores solucionan los mismos problemas que los ubicados en la máquina de cliente, pero además evitan que el Spam llegue al buzón de los usuarios con el correspondiente ahorro de recursos que esto conlleva.

  Sin embargo, tienen el inconveniente de dejar en manos de los responsables del servicio la creación de las bases de datos de patrones de palabras utilizadas para filtrar el Spam. De esta forma el usuario no puede, en forma alguna, controlar los mensajes que se están filtrando. Para evitar que mensajes válidos no sean entregados es habitual enviar un mensaje al receptor del e-mail Spam interceptado, avisándole de lo ocurrido. En él se adjuntan algunos datos del mensaje original, dándole la posibilidad de reclamar en el caso de que lo considerara como válido en un periodo de tiempo de algunos días.

  Esta medida es positiva porque de esta forma no se eliminan mensajes válidos sin consultar al destinatario, y además el usuario no ve el mensaje (sólo los campos "From:", "To:",...). El administrador se asegura de que el usuario no abrirá ningún mensaje Spam.

  Por otro lado, mengua en gran parte la ventaja del ahorro de recursos que el filtrado en el servidor proporciona, ya que deben enviarse los mensajes de aviso. La elección de cómo llevarlo a cabo dependerá del caso concreto ante el que nos hallemos.

Es importante destacar que el filtrado basado en contenidos (ya sea en el servidor o en el usuario), **no soluciona los efectos del Spam en el ancho de banda de las líneas de la empresa, ni en los recursos del servidor**, que por el contrario los debe aumentar para poder soportar el consumo que implican los filtros.

Otro punto negativo de estas técnicas es que el servidor de correo que no entrega los mensajes, **no advierte de ninguna manera al emisor**. Esto significa que un servidor legítimo no recibirá ningún informe de aviso de que su correo se ha rechazado. El mensaje simplemente desaparecerá.

A continuación vamos a exponer las características y modo de funcionamiento concreto de los filtros de contenidos usados actualmente. Para ello realizamos una nueva clasificación, basada en el algoritmo de filtrado utilizado. En concreto, valoraremos si éste recurre a reglas estáticas, definidas por el administrador, o se basa en métodos estadísticos. Así, distinguiremos **filtros estáticos y filtros bayesianos o adaptativos.**

Filtros estáticos basados en reglas:

Se trata de filtros que escanean el contenido de los mensajes en busca de patrones de palabras o grupos de ellas que indiquen si se trata de un mensaje Spam o no. Los hemos denominado estáticos porque **funcionan comparando los nuevos mensajes con patrones fijos almacenados en una base de datos**. El administrador debe introducir y actualizar dichos patrones. Éstos se obtienen de varias maneras:

- A través del análisis de mensajes Spam, creando una base de datos con los patrones más usuales del Spam recibido, mediante herramientas disponibles al efecto.

- Si se prefiere externalizar esta tarea, existen proveedores o empresas que se dedican a interceptar Spam, procesarlo para extraer los patrones más comunes, y generar bases de datos que luego serán descargadas por las empresas clientes para configurar sus filtros, en los servidores o en los usuarios finales.

- También han surgido iniciativas sin ánimo de lucro, en las que los usuarios envían el Spam que reciben, ofreciéndose como servicio el analizarlo y la tramitación de las denuncias pertinentes. Además el Spam es reutilizado para la obtención de los patrones que sirven para detectarlo.

Este tipo de filtros de contenidos, instalados en los servidores, son una buena solución corporativa contra el Spam. Sin embargo la gestión de la base de datos de los patrones usados es compleja, pues depende del idioma y del tipo de Spam que se reciba, además de requerir su actualización permanente.

Están apareciendo **productos de empresas antivirus** como TrendMicro (Emanager), McAfee (SpamKiller), etc., que, acompañando a los productos para evitar los virus, también intentan combatir el Spam.

Si lo pensamos, la filosofía de estos filtros es similar a la de los antivirus. Al tiempo que escanean los mensajes en busca de patrones de virus, también escanean en busca de patrones de contenidos de Spam.

Estas empresas, igual que mantienen y actualizan continuamente sus ficheros de virus, lo están haciendo también con patrones de contenidos de Spam.

Filtros bayesianos:

Los filtros convencionales basados en reglas fijas se han demostrado poco eficaces para frenar el Spam, ya que los Spammers cambian constantemente sus técnicas y los formatos de sus mensajes para saltarse las barreras que les imponen los servidores. Quienes envían mensajes no solicitados, intentan hacerlos cada vez más parecidos a mensajes legítimos, para no ser eliminados antes de llegar a la bandeja de entrada del usuario.

De modo que los filtros que utilizan como reglas de filtrado la dirección del remitente, su dominio o alguna palabra del asunto o del cuerpo del mensaje, además de ser muy engorrosos y exigir un trabajo constante de actualización, resultan bastante ineficaces.

Una técnica que mejora considerablemente los resultados en la lucha contra el Spam es el uso de filtros bayesianos o adaptativos. Éstos **pueden ser entrenados por el usuario para que se adapten a los mensajes que él mismo recibe**. Uno de los autores que primero planteó esta idea fue Paul Graham. En su ensayo "A plan for Spam" propone aplicar a los filtros antiSpam el Teorema de Bayes de probabilidades combinadas.

Definición del algoritmo utilizado en la implementación de un filtro basado en las teorías bayesianas:

El filtrado bayesiano se basa en el principio de que la mayoría de los sucesos están condicionados y que la probabilidad de que ocurra un suceso en el futuro puede ser deducido de las apariciones previas de ese suceso. Esta técnica se puede utilizar para clasificar Spam. Si algún patrón de texto aparece a menudo en Spam, pero no en mensajes legítimos, entonces la siguiente vez que se encuentre el mismo patrón de texto en un nuevo mensaje, sería razonable asumir que este e-mail probablemente es Spam.

Antes de que el correo pueda filtrarse utilizando este método, se necesita generar un antecedente de cada patrón o conjunto de ellos, asignándole un valor de probabilidad de que sea Spam. Esta probabilidad se basa en cálculos que tienen en cuenta cuán a menudo aparece el patrón en el Spam frente al correo legítimo, mediante el análisis de los mensajes salientes de los usuarios y del Spam conocidos. Las palabras y patrones que se analizan se toman tanto del contenido del cuerpo, como de la cabecera.

Teniendo en cuenta lo anterior, el filtro estadístico más simple funciona del siguiente modo: Los usuarios desechan todos los mensajes Spam en una carpeta separada de los mensajes válidos. En intervalos de tiempo, el programa de filtrado revisa todos los mensajes del usuario, y para cada palabra o muestra, calcula el cociente de las que pertenecen a un mensaje Spam entre las totales analizadas. Por ejemplo, si una palabra aparece en 200 mensajes Spam de 1000 analizados y en 3 mensajes válidos de 500 analizados, la probabilidad de que esa palabra pertenezca a un mensaje Spam es de:

$$P_i = (200/1000) / (3/500 + 200/1000) = 0{,}971.$$

Cada vez que llega un nuevo mensaje, se descompone en palabras, se calculan sus probabilidades de ser Spam y se toman las m palabras con mayores probabilidades, es decir, más cercanas a 0 ó a 1 indistintamente (cuyas probabilidades son P_1,..., P_m). De esta manera, la probabilidad de que el mensaje que ha llegado sea Spam es:

$$P = (P_1*P_2*...*P_m) / ((P_1*P_2*...*P_m) + (1-P_1)*(1-P_2)* ... * (1-P_m))$$

Normalmente para discernir si el mensaje es Spam o no, se usa un umbral, es decir, si P (probabilidad de que el mensaje sea Spam) es mayor que el umbral, el mensaje se califica como Spam; si P es menor o igual, se califica como mensaje válido. Este umbral suele fijarse alrededor de 0,9, pero este número no es muy relevante porque en la mayor parte de las ocasiones, las probabilidades quedan cercanas a 0 ó a 1. En el cálculo de P, los filtros bayesianos usan como máximo m = 20 palabras. Si se consideraran más palabras, porque se pensara que algunas de ellas con altas probabilidades de ser Spam se utilizan también en mensajes legítimos, se comenzarían a incluir patrones que únicamente aumentan el nivel de ruido, elevando el número de mensajes que el filtro considera como Spam, cuando no lo son.

Este es el caso de algoritmo más sencillo. En la actualidad se usan probabilidades modificadas a partir del Teorema de Bayes para conseguir mejores características de filtrado.

Es importante observar que este análisis se realiza sobre el correo del usuario o la empresa que lo instala en concreto, y por lo tanto es "hecho a medida". Podemos concluir que la belleza de la filtración bayesiana proviene de que **se puede adaptar a cada usuario individual**, simplemente aprovechando la información obtenida al clasificar cada e-mail recibido.

Una institución financiera podría utilizar una determinada palabra relacionada con el dinero más veces que un usuario genérico, por lo que obtendría muchos falsos positivos si utilizara una base de datos de reglas antiSpam general. El filtro bayesiano, por otro lado, toma nota del correo saliente válido de la empresa (y reconoce estas palabras relacionadas con el dinero como frecuentemente utilizadas en mensajes legítimos), y por lo tanto, tiene mucho mejor ratio de detección de Spam y mucho menor ratio de falsos positivos.

Una vez el usuario ha clasificado algunos mensajes, el filtro comenzará a hacer esta diferenciación por sí mismo, y generalmente, con un nivel muy alto de la exactitud. Si el filtro incurre en una equivocación, el usuario re-clasifica el mensaje, y el filtro aprende de sus errores. Por ello, los filtros bayesianos aumentan su exactitud con tiempo. No se requiere ningún mantenimiento complicado una vez el filtro está instalado, por lo que puede ser fácilmente utilizado por cualquier usuario.

De la explicación anterior se deduce que el filtro bayesiano no es estático, pues se actualiza constantemente en base a los nuevos mensajes Spam y válidos, aumentando su rendimiento a lo largo del tiempo y adaptándose a los cambios en las tácticas de Spam y a los cambios de la clase de mensajes escritos por los usuarios.

Funcionamiento del filtro bayesiano en entornos reales

En un entorno de funcionamiento real, podemos medir la calidad del filtro mediante dos indicadores:

- El porcentaje de mensajes no Spam calificados como Spam erróneamente ("tasa de falsos positivos").
- El porcentaje de mensajes Spam filtrados correctamente ("precisión").

Para este segundo indicador, también puede utilizarse el parámetro "tasa de errores", es decir, el porcentaje de mensajes Spam no detectados, que es equivalente al anterior ("precisión" = 1 – "tasa de errores").

El parámetro más importante desde el punto de vista del usuario real es el porcentaje de falsos positivos. En efecto, si un mensaje Spam evade el filtro es fácil hacer click en el botón de borrar. Sin embargo, si se marca con etiqueta de Spam a un mensaje normal, el usuario no lo verá y éste quedará perdido. Una solución a este problema es comprobar cada cierto tiempo la carpeta a donde se destina el Spam. El inconveniente es que esto resulta aburrido y una pérdida de tiempo si se reciben muchos mensajes Spam, además de desperdiciar parte de los beneficios que aporta el filtrado.

Conseguir una precisión cercana al 100% o un número de falsos positivos cercano a 0, es en la práctica más difícil de lo que podría parecer en un principio. Idealmente se podría conseguir el 0% de errores si marcamos todo como Spam (umbral ≈ 0), salvo que de esta forma tendríamos que muchos mensajes buenos son marcados como Spam. Por otra parte podríamos conseguir el 0% de falsos positivos si no marcamos ningún mensaje como Spam (umbral ≈ 1), sin embargo estaríamos dejando entrar muchos mensajes Spam.

Por tanto, para conseguir un filtro de alta calidad, y dado que nunca se podrá alcanzar la posición ideal de ambos (ver el gráfico siguiente), hay que intentar conseguir bajas tasas de ambos parámetros llegando a un compromiso, según los valores que nos interesen.

Figura 10

Ejemplos de filtros comerciales disponibles. Evaluación del funcionamiento y de las características reales de dos de ellos.

En la actualidad se puede encontrar en el mercado un amplio abanico de filtros basados en métodos estadísticos. Hay dos navegadores que ya incluyen en sí mismos filtros bayesianos: "Mozilla" y "The Opera M2" (sin embargo el filtro de éste último tiene una tasa de falsos positivos alta).

Para los gestores de correo existen una serie de soluciones que pueden instalarse para mejorar las herramientas de filtrado que presentan (en el caso de Outlook, uno de los más utilizados, son bastante ineficaces). Algunas de las más populares son Spammunition, SpamBayes, Spam Bully, InboxShield, Junk-Out, Outclass, Disruptor OL, y SpamTiger.

En este apartado expondremos los resultados de la utilización de dos de los mejores filtros bayesianos comerciales desde el punto de vista del usuario, (según Graham, P.): **SpamBayes y POPFile**. Para la elaboración de estas conclusiones se llevó a cabo una prueba en la que se contabilizaron el número de mensajes de correo electrónico válidos y el Spam que se recibían, así como la actuación de los dos filtros ante ellos. Las pruebas fueron realizadas bajo las siguientes hipótesis:

- Se usó el protocolo POP3 para descargar los mensajes de correo.
- Puesto que los filtros bayesianos requieren entrenamiento, y su exactitud aumenta con tiempo, la prueba se realizó durante un mes (del 1 al 31 de julio de 2003).

- Tras la segunda semana, la dirección de correo electrónico en evaluación se hizo pública en varias listas de distribución para averiguar cómo se comportaban los filtros ante el Spam que proviniera de estas fuentes.

- El número máximo y mínimo de mensajes diarios que se recibieron en la dirección de correo electrónico donde se instalaron los filtros durante la prueba, se ha reflejado en la siguiente tabla. En ella se han diferenciado dos periodos: El primer periodo (los 15 primeros días) y el segundo, los 15 últimos días tras la inclusión de la dirección de correo en diferentes listas de distribución.

  Un ejemplo de interpretación de la tabla es el siguiente: Para la casilla del primer periodo correspondiente al número de mensajes válidos recibidos: Durante los 15 primeros días del transcurso de la prueba se recibieron al día entre 2 y 30 mensajes válidos, de un total diario que osciló entre 30 y 60 mensajes (casilla tercera de la izquierda).

	1º periodo	2º periodo
Máximo-mínimo número de mensajes válidos al día	30-2	70-20
Máximo-mínimo número de mensajes válidos al día	50-5	60-40
Máximo-mínimo número total de mensajes al día.	60-30	130-60

Tabla 2. Resumen del número de mensajes recibidos durante la realización de la prueba

Es necesario puntualizar que, asumiendo que la filtración bayesiana uniforme no es siempre perfecta (tasa de falsos positivos siempre distinta de cero), el filtro SpamBayes incorpora una solución que funciona muy bien en la práctica. En lugar de calificar los mensajes entre Spam o no Spam, agrega una tercera categoría denominada mensajes "dudosos". El usuario puede configurar cuál es el nivel a partir del cual el mensaje calificado como dudoso se envía a la carpeta de Spam o a la de no Spam.

Los resultados de las pruebas realizadas se reflejan en los gráficos siguientes. En la parte de arriba, se representan los mensajes clasificados erróneamente como Spam en función del tiempo a partir del inicio de la prueba, para los dos filtros evaluados (SpamBayes y POPfile). En el gráfico inferior, podemos apreciar el número de mensajes Spam no filtrados en función del tiempo, también para ambos filtros.

Se puede apreciar el buen comportamiento de los filtros, ya que tras el periodo de entrenamiento (unos 5 días en el caso mayor), ambos tienen una tasa de errores y falsos positivos bastante baja.

Sin embargo, se puede advertir como la tasa de falsos positivos es oscilante a lo largo del tiempo. Esta característica podría considerarse grave, pues incluso un solo e-mail incorrectamente clasificado como Spam es demasiado, ya que nunca se está seguro de la importancia que tenía dicho mensaje. El filtro SpamBayes es bastante mejor en este aspecto, puesto que no dio ningún falso positivo tras su periodo de entrenamiento. Para el parámetro errores, de nuevo se puede apreciar que los resultados del SpamBayes son superiores.

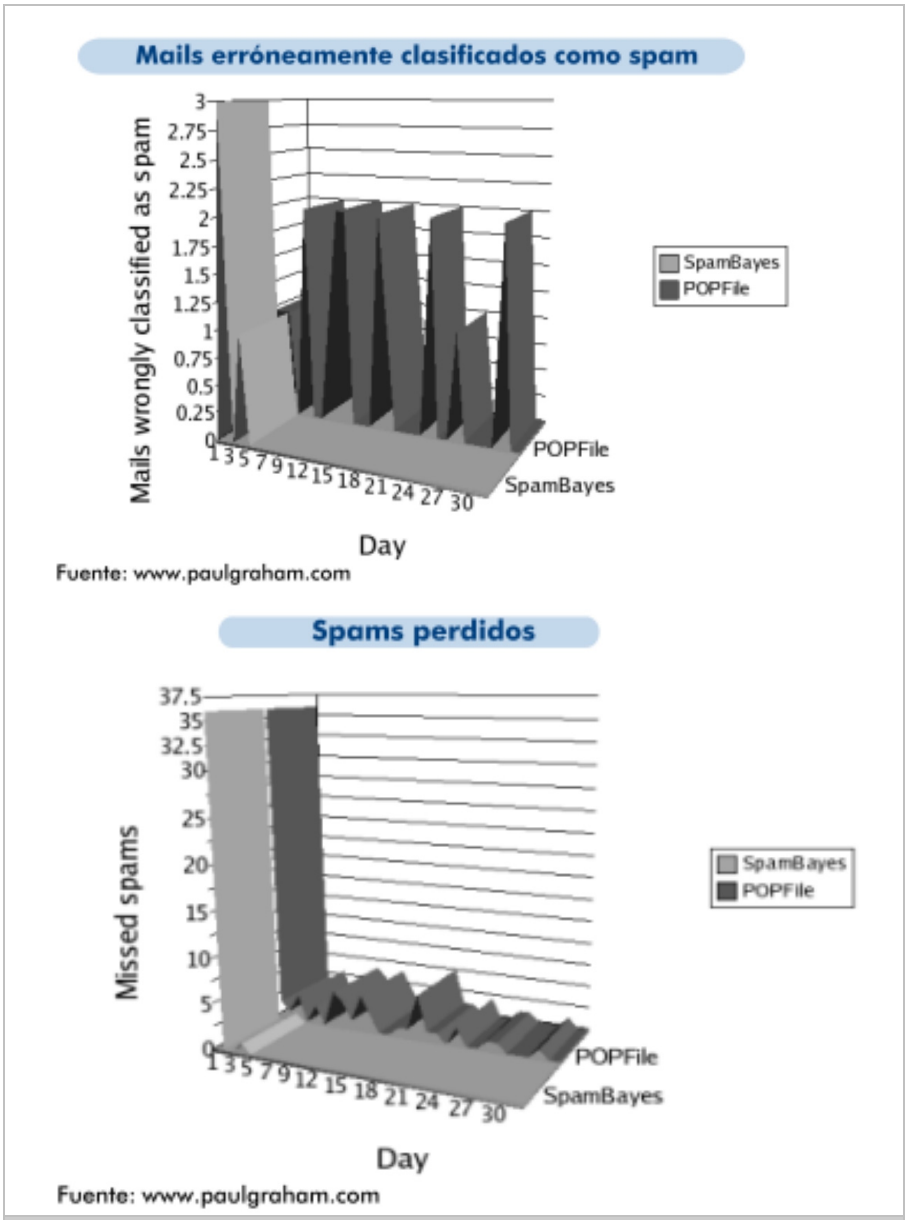

Figura 11: Comparativa de los parámetros principales de dos filtros comerciales

El porqué de esta diferencia es el hecho de poseer una tercera clasificación de los mensajes como "dudosos". Sin embargo esto hace que la comparación no sea totalmente justa, puesto que sus principios de funcionamiento son distintos. Buscando realizar una comparación más real, en el siguiente gráfico se han incluido los mensajes clasificados por el filtro SpamBayes como "dudosos":

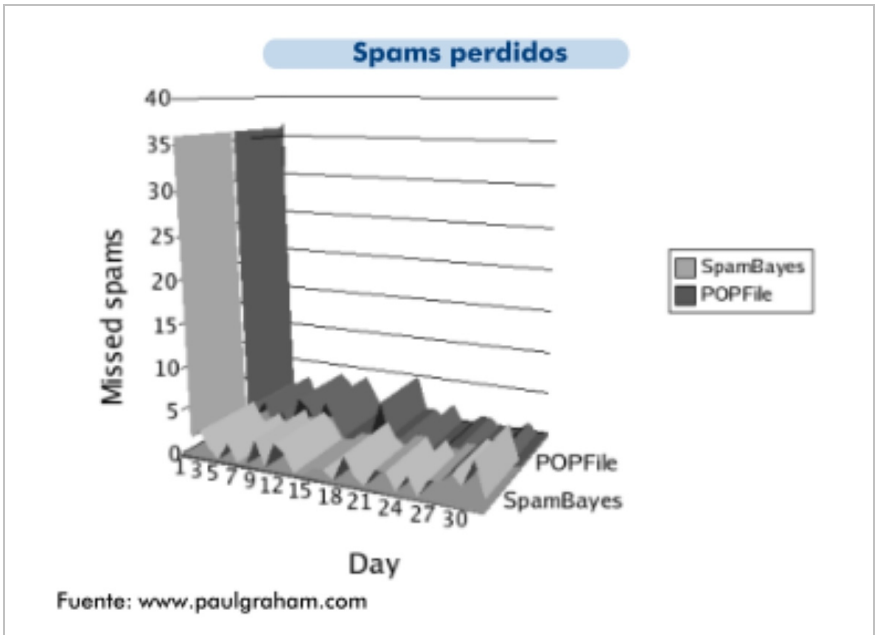

Figura 12: Comparación real entre los filtros SpamBayes y POPFile

En el gráfico se observa que el filtrado bayesiano básico que incorporan ambos filtros es más o menos igual, si consideramos que éste califica todos los mensajes dudosos como correo válido para evitar falsos positivos.

La principal conclusión de los resultados de este experimento es que en total, con ambos filtros, **se consiguieron tasas de aciertos de 97.75% con pocos falsos positivos**, dato bastante bueno. Sin embargo, **pruebas realizadas en cuentas de correo de otros usuarios demostraron que se pueden conseguir tasas del 99%**.

Análisis del tipo de palabras que utiliza un filtro bayesiano en su decisión estadística

Como hemos mencionado anteriormente, para el cálculo de la probabilidad de que un mensaje sea Spam se tienen en cuenta todas las características del mensaje, tanto el contenido del cuerpo, como el de la cabecera.

De la cabecera se pueden obtener muchos datos interesantes, tales como: El remitente, el origen del mensaje u otros en apariencia menos importantes como la hora en la que se realizó el envío, que pueden servir de gran ayuda en la clasificación del mensaje.

Un mensaje que se haya enviado en horas de madrugada, es más probable que sea Spam.

A continuación, se presenta un ejemplo del tipo de palabras del **cuerpo del mensaje** que un filtro bayesiano califica con alta probabilidad de ser Spam[13]. Después de cada palabra, aparece entre paréntesis la probabilidad que le corresponde (a mayor probabilidad, más posibilidades de que el mensaje que la contenga sea Spam). Como se puede deducir de la explicación anterior, estas palabras no son estándar ni iguales para todos los usuarios, sino que el propio filtro las elige según los mensajes que han llegado al buzón de dicho usuario.

Palabras que presentan grandes probabilidades de ser Spam:

- Money (2356/48).
- Sex (1989/34).
- Pronombres en segunda persona, you (1560/1034), your (1465/367), our (1118/125).
- Palabras que indican urgencia u obligación, must (201/116), important (125/24), critical (13/5), urgent (32/1)
- Palabras que expresan tiempo, January (40/24), today (186/23) (not yesterday (1/7)), week (68/27), month (186/16), year (129/43). Esto sucede a pesar de que en el cuerpo de los mensajes legítimos a menudo aparecen este tipo de palabras.
- Palabras relacionadas con una respuesta por parte del destinatario, reply (215/17), call (235/90), email (909/143), telephone (76/8), letter (100/9), requirements, require (52/25), obligation (106/2), must (201/116).
- Palabras neutras, get (710/390), are (1065/635), make (383/229), trust (40/24), this (1299/809).

[13] Las palabras citadas a continuación han sido tomadas de las pruebas efectuadas por Bowers, J. (www.jerf.org) con un filtro bayesiano. Se trata de un usuario de lengua inglesa, por lo que las palabras están en inglés.

Palabras que presentan pequeñas probabilidades de ser Spam:

- Las contracciones inglesas, I'm (46/462), we'd (1/14), I'll (24/126). Excepciones, won't (99/56), you'd (69/33).
- Pronombres en primera persona, mine (4/27), I'd (14/150), I'm (46/462).
- Palabras que expresan sentimientos negativos, hate (5/42), kill (2/46), sad (1/7), evil (1/27).
- Lenguaje coloquial o slang en inglés, acrónimos coloquiales en la lengua inglesa como YMMV, smileys like (1/84), (2/104). También otras palabras propias del mundo en que se mueve el usuario.
- Palabras neutras, but (314/887), should (140/261), they (289/495), that (921/1260).

Copyright 1999-2003 Jeremy Bowers. www.jerf.org

Aunque el ejemplo ha sido tomado de un usuario concreto, y de habla inglesa, las palabras que aparecen con altas y bajas probabilidades pueden corresponderse con las que estarían definidas para un usuario más o menos estándar. Así, si nos fijamos en características de los mensajes Spam, **llegamos a la conclusión de que palabras como dinero, sexo, aquellas que expresan urgencia u obligación y las que están relacionadas con una respuesta por parte del destinatario, es fácil encontrarlas en este tipo de mensajes**.

Por otra parte, **expresiones muy coloquiales y estilo de redacción en primera persona son características que todos usamos al escribir y recibir nuestros mensajes**. Además, **la mayoría del Spam que se recibe está en inglés**, con lo que probablemente muchas palabras con alta probabilidad de Spam de nuestro filtro estarían en esta lengua.

Con este ejemplo no se quiere indicar que las características de los mensajes válidos y Spam son iguales en todos los usuarios, todo lo contrario. Por ello, la ventaja más importante de los filtros basados en métodos estadísticos es su adaptación dinámica al usuario y al Spam de cada momento.

Ventajas del filtrado bayesiano frente a filtrados estáticos. Adaptación a la evolución del Spam

Entre las más importantes ventajas del filtrado bayesiano destaca, como ya hemos indicado, que **este tipo de filtros puede adaptarse al correo de cada usuario concreto, pero también a los mensajes indeseados que reciba**. Conozcamos otras ventajas de este tipo de filtrado:

- **El método bayesiano tiene en cuenta la totalidad del mensaje**: En efecto, reconoce palabras clave que identifican el Spam, pero también reconoce palabras que denotan que se trata de mensaje válido. Por ejemplo, no todo el correo que contiene las palabras "free" y "cash" es Spam. El método bayesiano encontraría relevantes las palabras "cash" y "free" pero también reconocería el nombre del contacto de negocio que envió el mensaje, y de ese modo lo clasificaría como legítimo.

  En otras palabras, el filtrado bayesiano es una estrategia más inteligente que otros métodos porque examina todos los aspectos de un mensaje, en oposición al análisis de palabras clave que clasifican un mensaje como Spam en base a un solo conjunto de palabras fijo.

- **Un filtro bayesiano está constantemente auto-adaptándose**: Mediante el aprendizaje continuo a través de los nuevos mensajes (Spam y válidos), el filtro bayesiano evoluciona y se adapta a ellos. Así, si surgen nuevas técnicas Spam, el filtro aprenderá a reconocer el nuevo tipo de mensajes no deseados.

  Por otro lado, también se reconfigura ante los posibles cambios que se den en el correo válido que llega al usuario. De este modo, si éste comenzara a recibir mensajes de correo electrónico deseado de una determinada lista de distribución relacionada con un tema que pueda asociarse a mensajes Spam, y del que antes nunca se había recibido ningún mensaje, el filtro se adaptará y permitirá la entrada de este nuevo tipo de mensajes, pero no de mensajes Spam.

- **La técnica bayesiana es sensible al usuario**: Para tener éxito y hacer que se entreguen sus mensajes, los Spammers tienen que enviar correo que no sea atrapado por los filtros personalizados de la víctima. Como el método bayesiano tiene en cuenta el perfil de correo del usuario, detecta el Spam con mayor facilidad, pues los Spammers necesitarían saber el perfil de correo de dicho usuario para ser capaces de superarlo. Dado que el Spam tiene su propio vocabulario y carácter, el filtro bayesiano puede atraparlo con facilidad.

  Sin embargo, no es sencillo para los Spammers cambiar sus argumentos de venta para tener en cuenta el perfil de correo del usuario, pues una de las principales características del Spam es que es masivo y no personalizado.

- **El método bayesiano funciona adaptándose a cualquier lengua y es internacional**: Un filtro antiSpam bayesiano al ser adaptable, puede utilizarse con cualquier idioma necesario, siempre que éste utilice como separadores de palabras el carácter espacio (" "). La mayoría de las listas de palabras clave indicadoras de Spam disponibles para filtros estáticos, sólo lo están en inglés y son por lo tanto mucho menos útiles en regiones de habla no inglesa. El filtro bayesiano también tiene en cuenta ciertas desviaciones del lenguaje o los diversos usos de ciertas palabras en áreas diferentes, incluso si se habla el mismo idioma. Esta inteligencia lo habilita como un filtro más efectivo.
- **Un filtro bayesiano es más difícil de burlar que un filtro de palabras**: Para intentar demostrar e ilustrar esta ventaja, enumeraremos a continuación las diversas técnicas que hemos observado que los Spammers utilizan (o podrían utilizar) con la intención de burlar el filtro, y cómo éste "aprendería" a detectarlas.

PRIMERA TÉCNICA:

Un Spammer avanzado que quiera engañar a un filtro bayesiano podría elegir las palabras de su mensaje de tal forma que utilizara menos aquéllas con alta probabilidad de pertenecer a un mensaje Spam (palabras que habitualmente indican Spam como free, Viagra, etc.), o más aquellas que generalmente indican correo válido (como un nombre de contacto válido, los apodos de los amigos o términos que se usan normalmente en el ámbito laboral de cada usuario). Esto último es imposible porque el Spammer tendría entonces que conocer el perfil de correo de cada destinatario.

Además, si los Spammers intentaran burlar el filtro mediante palabras que normalmente se califican como buenas, no les resultaría suficiente porque en un mensaje Spam típico, un montón de palabras con alta probabilidad se encuentran ya en la cabecera. Éstas últimas irían aumentando la probabilidad de calificar el mensaje como Spam. Por otro lado, utilizando palabras neutras, por ejemplo la palabra "public", no funcionaría ya que éstas son dejadas de lado en el análisis final (sólo se utilizan las "m" con probabilidades más cercanas a 0 ó 1). Por tanto, la técnica de utilizar palabras "más apropiadas" no engañaría al filtro.

SEGUNDA TÉCNICA:

Incluir en los mensajes palabras que típicamente indican que se trata de un mensaje Spam pero intentando encubrirlas. Por ejemplo, utilizando "f-r-e-e" en lugar de "free". Otro ejemplo sería utilizar la palabra "5ex" en lugar de "Sex". También podrían utilizar como separadores hipervínculos html, espacios en blanco y otros caracteres, por ejemplo "fr ee" en lugar de "free", "frèé" o "fr.ee" en lugar de "free"). Pero esto sólo incrementará la probabilidad de que el mensaje sea Spam, ya que un usuario legítimo raramente escribirá la palabra "free" como "f-r-e-e".

En este caso, el filtro bayesiano advierte automáticamente estas palabras que nunca se usarían en mensajes válidos por regla general, por lo que sería capaz de adaptarse para atrapar este tipo de Spam.

TERCERA TÉCNICA:

Enviar mensajes que no contengan texto, sólo imágenes. Los mensajes con imágenes tampoco engañarían al filtro por varias razones. Para empezar, las cabeceras que sugieren que el mensaje es Spam nunca pueden omitirse. Además el filtro comprueba tanto texto como código HTML. En el cuerpo del mensaje probablemente habrá un link a la imagen, y ambos contendrán una dirección URL, la cual probablemente tenga una alta probabilidad de ser Spam. Con el hipervínculo, la imagen tendrá alguna clase de nombre, y éste está normalmente lejos de ser aleatorio. Por tanto, cualquier imagen que contenga el Spam tendrá asociadas en el cuerpo del mensaje, o en el código HTML, algunas palabras, que servirán para catalogar el mensaje como Spam.

CUARTA TÉCNICA:

Añadir al mensaje palabras invisibles, tratando de confundir al filtro: "Si el usuario no puede verlas, el filtro tampoco". Ejemplos de esto, pueden ser añadir texto en blanco sobre fondo blanco, cabeceras de los mensajes que incluyan las palabras deseadas, o incluir palabras aleatorias antes del código HTML. Sin embargo el filtro es capaz de leer el código HTML de los mensajes y sus cabeceras, por lo que estas técnicas no funcionarían.

QUINTA TÉCNICA:

Insertar una falsa etiqueta HTML que contenga un texto largo, por ejemplo, de una noticia. Si observamos el código de un mensaje, las etiquetas van entre los caracteres "<" y ">". Los bloques de texto largo en el código del mensaje son omitidos por los servidores HTML, por tanto aparecerán como etiquetas no válidas. Además, la etiqueta necesita definirse en el código del mensaje, por lo que de ninguna manera pasará desapercibida para el filtro.

SEXTA TÉCNICA:

Otra forma de intentar burlar el filtro podría ser que el contenido del mensaje solamente fuera un hipervínculo al sitio a promocionar, estando la URL del hipervínculo codificada en decimal, hexadecimal u octal. Este tipo de tácticas obligarían a que el filtro decodificara el texto HTML. Algunos filtros ya reconocen estas variantes y traducen las URLs a su forma canónica.

SÉPTIMA TÉCNICA:

Reemplazar el texto del Spam por código Javascript tal que se ejecutara al abrir el mensaje. Éste sería un buen truco, a no ser porque el usuario rara vez codifica sus mensajes en Javascript. Sin embargo, los filtros actuales no presentan buenas soluciones ante esta táctica.

Se ha puesto de manifiesto la imaginación de los Spammers y cómo un filtro basado en métodos estadísticos podría seguir funcionando correctamente ante ellas. Podemos concluir que el uso masivo de estos filtros podría ser el fin de mensajes que anuncian temas muy concretos tales como los hipotecas, pornografía, etc., pues es muy difícil anunciar hipotecas sin usar ninguna palabra tal y como "préstamo", "interés", "hipoteca", etc., que por otra parte son muy raramente utilizadas en usuarios comunes.

Aplicación del filtrado bayesiano en servidores

Aplicar el filtrado bayesiano en servidores de e-mail es algo más complejo que en los buzones de compañías o de usuarios individuales, puesto que debe existir una manera para que los usuarios individualmente entrenen el filtro, ya que no es fácil establecer un perfil correcto para todos los usuarios de un proveedor. Varios ejemplos de filtros bayesianos que trabajan en servidores son SpamProbe, Razor y Bogofilter.

Es interesante comentar la filosofía de uso de **Razor**[14]:

Se trata de un sistema de detección y seguimiento de mensajes Spam, distribuido y colaborativo. Su funcionamiento está basado en que el Spam típicamente opera enviando idénticos mensajes a cientos de personas. El sistema de Razor permite que la primera persona que reciba el Spam, lo añada a la base de datos, para que el resto de las personas bloqueen ese mensaje en concreto.

Su algoritmo calcula sumas de verificación de estos mensajes Spam conocidos y también se almacena en la base de datos distribuida. Si se recibe un mensaje nuevo, se computa la suma de verificación y se compara con las sumas de verificación en la base de datos central. Si coinciden, se rechaza el mensaje.

Razor basa su funcionamiento también en cuentas especiales de correo distribuidas en Internet, con el único propósito de ingresar en las listas de direcciones de todos los Spammers. Estas cuentas sólo captan Spam y no correo normal y contribuyen a actualizar la base de datos. Los clientes también pueden enviar mensajes a Razor para que el sistema los incluya.

La gran ventaja de este sistema es que existe una alta probabilidad de que los mensajes ya sean conocidos como Spam antes de que lleguen al buzón de correo. El sistema filtra alrededor del 80% del Spam, con la característica de que no tiene ningún otro proceso o técnica de filtrado, por lo que detecta muy pocos falsos positivos.

[14] Consultar http://razor.sf.net

Otra alternativa para los filtros estadísticos en servidores es la utilización de filtros basados en métodos heurísticos, que proporcionan mejores características en este tipo de entornos.

Según la empresa MessageLabs, la tasa de Spam filtrado mediante técnicas bayesianas, que en usuarios individuales llega hasta el 99%, en servidores desciende entre el 80 y el 95%. Sin embargo, los filtros basados en métodos heurísticos, proporcionan en media un porcentaje de aciertos en torno al 95%.

6.3. Comparativa tras el análisis de las medidas contra el Spam

En este capítulo hemos estudiado que se puede realizar un filtrado de mensajes **configurando el servidor de correo electrónico para que rechace unas determinadas transacciones SMTP que presenten evidencias de ser Spam**. Esta medida consigue evitar un porcentaje de Spam pequeño, pero tienen la gran y exclusiva ventaja de avisar al servidor emisor de que su mensaje no será recibido. Además, consume muy pocos recursos del servidor receptor.

Una de las medidas basadas en el análisis de las transacciones SMTP que presenta mayor controversia es la basada en **listas negras**. Éstas rechazan las transacciones SMTP (y por tanto de los mensajes) que provengan de determinadas direcciones IP. Los defensores de las listas negras alegan que son una medida justa puesto que ejercen presión al proveedor que aloja a Spammers, haciendo que mejore su configuración (en el caso de que sus servidores estén abiertos). También evitan que este tipo de práctica pudiera serles rentable. Sin embargo, también tienen una serie de inconvenientes:

- El porcentaje que se recibe de Spam de un grupo de remitentes concreto, representará un porcentaje pequeño del Spam total que se recibe, ya que los Spammers cambian dinámicamente de dirección.
- El hecho de incluir un servidor en una lista negra implica que no se reciba ningún mensaje que provenga de él, sea Spam o no.

Por otro lado, las medidas de **filtrado basadas en contenidos** presentan como ventajas principales:

- Disminuyen notablemente el Spam de los buzones, al ser enviado a una carpeta separada del correo válido.
- Si los filtros eliminan algún mensaje correcto, siempre es posible buscarlo en las carpetas de correo no deseado.

- La decisión de qué es o no Spam recae en el usuario que lo recibe, ya que es él quien define los filtros. En el caso de los filtros de servidor, esta decisión se establece en la "política institucional para el uso del servicio de correo electrónico".

- Usar un filtrado basado en contenidos puede evitar el abuso que supone incluir un servidor "inocente" en una lista negra.

La utilización de filtros basados en contenidos puede poner fin a la ficción que muchas veces se esconde tras el opt-in. En efecto, el opt-in que dicen practicar algunas compañías no es sino una forma de enmascarar el Spam.

Una de las empresas que presume poseer mayor número de direcciones obtenidas mediante opt-in tiene alrededor de 60 millones de direcciones correctas, casi todas de usuarios domésticos. 60 millones de usuarios de Internet representan alrededor de la mitad de los usuarios de EEUU. Sin embargo si se preguntara a éstos si recuerdan haber solicitado esta publicidad, probablemente no lo harían. Este ejemplo ilustra que existe mucho engaño en este ámbito.

Sin embargo, el filtrado de mensajes basado en contenidos también cuenta con una serie de aspectos negativos:

- El Spam es encaminado por las líneas de comunicaciones y procesado como mínimo por las estafetas de correo electrónico, por tanto no elimina los problemas del consumo de recursos.

- Los mensajes que se descartan pueden ser en algunos casos de importancia para el usuario y, sin embargo, ni emisor ni receptor son avisados. Para evitar el problema, los emisores deberían preocuparse de comprobar que sus mensajes han sido leídos por los destinatarios.

- No se trata de técnicas que tengan efecto en la erradicación del Spam ya que:

  - Ni emisores ni proveedores responsables reciben ningún tipo de información: No se les avisa que se está llevando a cabo una actividad incorrecta, con lo que lo desconocen y pueden ser también víctimas de los Spammers.

  - Los mensajes llegan realmente a recibirse: Lo que se hace con ellos es esconderlos en lugares habilitados al efecto (carpetas en el usuario final o directorios en el caso de filtros en el servidor).

En la siguiente tabla se presenta de forma comparativa las ventajas y desventajas de ambas filosofías de filtrado.

	Listas negras (DNS)	Análisis del diálogo SMTP	Filtros de palabras	Métodos heurísticos	Métodos estadísticos
Precisión	0 - 60%	hasta 30%	80%	95%	99%+
Falsos positivos	10%	-	2%	0.5%	0.1%

Tabla 3. Comparativa de las características de los distintos filtros. Fuente: MessageLabs, www.Spamconference.com

Estos resultados despiertan esperanzas con relación a poder llegar a controlar el Spam, sin embargo los límites del Spam son insospechados y habrá que ver qué nos depara el futuro.

6.4. Hacia dónde llevan las nuevas medidas contra el Spam. Opinión de los grandes proveedores

Según algunos grandes proveedores de Internet, que son los mayores afectados por el Spam desde el punto de vista económico, los filtros antiSpam no ofrecen una solución decisiva a su problema, por lo que intentan buscar nuevas herramientas y tácticas.

Bill Gates, presidente de Microsoft, lidera un movimiento que está empezando a tomar fuerza y que apuesta por combatir el Spam haciendo que **los Spammers paguen por los recursos que utilizan**. Actualmente éstos pagan un precio marginal cercano a cero por realizar sus envíos. Para los Spammers esta situación representa una estrategia de beneficio seguro: "*envía tanto como puedas, porque incluso un si un usuario de cada millón se transforma en cliente, es rentable*". Una solución obvia podría ser por tanto cobrar por el envío de estos mensajes.

En el World Economic Forum celebrado en Davos (Suiza) en enero de 2004, Bill Gates defendió que la **tecnología de filtrado junto con esquemas de pago** podría frenar y eliminar el Spam en **dos años**.

Otras compañías también opinan que un sistema de pago podría contribuir a reducir las pérdidas que deben afrontar los proveedores de servicio. Veamos algunas ideas en línea con este planteamiento:

- Richard Gingras, director de la compañía Goodmail Systems, propone crear algo similar a unos "***sellos electrónicos***", de forma que los Spammers que deseen que sus envíos masivos sean entregados asuman un coste por ello. Bajo este sistema, los Spammers serían libres de comprar estos sellos, al igual que los que realizan buzoneo a través del sistema de correos convencional. Sin embargo, esto introduciría en sus economías un gasto extra y justo. En esta situación los mensajes de los Spammers que no compraran los sellos, serían ilegítimos y los proveedores podrían filtrarlos con mayor facilidad, con lo que se reduciría el Spam, incluso si el sistema es adoptado sólo parcialmente.

Sin embargo, según otras opiniones, este sistema podría ser inviable al tener que procesar millones de paquetes de datos en los que se fragmenta cada mensaje, tratando de separar los que deben cobrarse.

Amazon afirma que compraría un millón de "sellos de e-mail" a 0,01 dólares cada uno, si sus mensajes de confirmación automática de pedidos que le reportan una parte importante de sus ventas, no fueran filtrados como Spam por error.

Ello redundaría en un beneficio de 10.000 dólares para el proveedor de servicio. Goodmail, como compañía encargada de la gestión de este sistema, pondría los sellos a los mensajes de Amazon como cabeceras encriptadas, y enviaría la clave para desencriptarlos al ISP. El ISP en este caso podría identificar los mensajes de Amazon y entregarlos a los buzones de los consumidores.

- Un método adicional, propuesto por la compañía IronPort System, es **no cargar en los emisores todo el coste de los mensajes, sino sólo el de aquéllos que hayan provocado una queja de los receptores.** Esta compañía ha venido ofreciendo desde hace poco más de un año un servicio a emisores masivos de mensajes. Se trata de un contrato de tal forma que, a cambio de previo pago, entrega sus mensajes a los receptores. Los emisores deberán abonar además un pago extra si los emisores se quejan del mensaje. La idea es disponer de una especie de lista blanca que eventualmente crece con los emisores que sean calificados como honestos por los usuarios, y en otro caso, son incluidos en listas negras.

- Balachander Krishnamurthy, de AT&T Labs, propone un sistema en el cual el ISP establecería un **consorcio** (similar al que establecen los bancos con Visa), en el que el **proveedor actuaría como modelador entre el emisor y los usuarios**. Se daría a los emisores que establecieran el contrato un número de créditos limitados. Cada vez que un receptor declarara un mensaje como no solicitado al modelador, se cobraría al emisor de ese mensaje 1 dólar, por ejemplo. Una vez agotado el crédito asignado (por ejemplo 200 dólares), el modelador suspendería el servicio a ese emisor.

Los esquemas propuestos también servirían para intentar solucionar otro gran problema: El envío de Spam mediante la propagación de virus (Sobig, MyDoom), que convierten a los ordenadores de usuarios inocentes en máquinas de enviar Spam. En el último sistema descrito, el crédito limitado de los usuarios infectados por un virus de este tipo se agotaría en pocos segundos, con lo que pararía de propagarse. El PSI podría detectar que en estos casos los usuarios son víctimas, y devolverles el servicio una vez solucionado el problema.

Sin embargo, estos sistemas basados en que la queja del usuario revierta en un coste para el Spammer podrían ocasionar que, aunque los problemas económicos de los proveedores se atenúen, crezcan para los usuarios. En efecto, en esta situación recibirían a su buzón muchísimos más mensajes que en la situación actual, puesto que éstos llegarían con el visto bueno del proveedor y no se filtrarían. Además el usuario debería emplear mucho más tiempo en abrirlos, decidir si son o no ofensivos, y efectuar una queja. De hecho, es probable que la gran mayoría de los usuarios no se quejara.

Por otro lado, los planteamientos estudiados tienen en común que si el proveedor detecta que un mensaje es "Spam legítimo", lo entrega. Por tanto sólo están beneficiando a la empresa que realiza el Spam, a la que le resulta rentable pagar por él, y al mismo proveedor, que consigue ingresos extra. En ningún caso se beneficia al usuario, que en esta situación se vería inundado de Spam.

6.5. Cómo se debe actuar ante el Spam recibido: Quejas y denuncias

¿Qué podemos hacer ante la recepción de Spam? Existen determinadas medidas a adoptar, distintas según seamos usuarios o administradores de correo electrónico en alguna organización. Es importante destacar que todas ellas contribuirán de forma importante a luchar contra el Spam.

Acciones desde el punto de vista del usuario

Las entidades que luchan contra el Spam aconsejan que **nunca se debe actuar perdiendo la ética o la superioridad moral contra los sitios remitentes de Spam o de contenidos deshonestos**. Es decir, nunca se debe amenazar con violencia, pagar con la misma moneda efectuando envíos masivos de mensajes, atacar el sitio con métodos de piratería electrónica o hacking y, en general, recurrir a ningún otro medio no ético. Como ya se ha comentado, los Spammers a menudo falsifican las cabeceras de los mensajes para ocultar su identidad y en su lugar añaden la identidad de terceros que son inocentes o que no existen. Por tanto, si respondemos a la dirección origen que aparece en el mensaje con más Spam, lo único que conseguiremos será causar daños a gente inocente o generar tráfico y colapsar la red.

Tampoco se debe responder nunca al mensaje de correo electrónico no deseado, con el fin de que eliminen la dirección de correo de una supuesta lista. En algunas ocasiones el Spam viene acompañado con una lista de nombres de quien se dice que han expresado su deseo de recibir comunicaciones comerciales, y que puede solicitar la baja de la lista cuando se quiera; en realidad a menudo sólo contiene víctimas escogidas al azar, por lo que está incurriendo en un acto ilegal (según las leyes de protección de datos). Otras veces el mensaje Spam enuncia que eliminarán la dirección de correo de aquellos usuarios que lo soliciten. La realidad es que casi nunca lo hacen, sino todo lo contrario.

No debemos dejarnos convencer por los productos, servicios o promociones que se anuncian en el Spam, ya que en primer lugar se trata de una práctica ilegal, y en segundo, suelen ser actividades fraudulentas o estafas.

Lo que se debe hacer es efectuar una **queja o denuncia**. En ésta se debe incluir:

- La cabecera del e-mail (ésta contiene los datos que pueden llevar a la identificación del Spammer)
- Una copia del mensaje original y
- Los motivos que nos han llevado a efectuar la denuncia.

Podemos **enviarla al administrador de nuestro proveedor de servicio de correo electrónico** o PSI para que él tome las medidas pertinentes. Su dirección es normalmente postmaster@dominio_PSI o abuse@dominio_PSI.

Herramientas disponibles para los usuarios:

Además de efectuar una queja, el usuario debe intentar protegerse del Spam mediante alguna herramienta de filtrado.

Los proveedores gratuitos de correo electrónico web casi siempre incluyen alguna herramienta de este tipo:

Ya.com (Mixmail) ofrece la posibilidad de configurar filtros de correo no deseado dependiendo del grado de seguridad que se requiera para la cuenta (alta, media y baja). Además envía los mensajes calificados como "correo no deseado" a una carpeta específica.

Hotmail también posee una herramienta parecida con la que podemos elegir entre varios niveles de filtrado:

- "*Predeterminado*", en el que identifica como Spam los mensajes más claros
- "*Alto*" que capturará la mayor parte del Spam, aunque también puede equivocarse con algún mensaje deseado; y
- "*Exclusivo*", con el que sólo llegarán a la bandeja de entrada los mensajes de remitentes incluidos en la lista de contactos.

Se puede crear también una **lista negra propia de cada usuario** mediante el bloqueo de remitentes. Los mensajes que provienen de estos remitentes o de sus dominios se eliminan directamente, sin llegar a ninguna carpeta de la cuenta del usuario. Así mismo se pueden **crear listas de remitentes seguros**, cuyos mensajes nunca serán calificados como correo no deseado por el filtro.

Un aspecto a tener en cuenta es que los mensajes que provengan de algunas listas de distribución a las que estemos suscritos, puede que sean calificados como correo no deseado. Esto ocurrirá si la configuración de los mensajes en el campo "Para" no es la de nuestra cuenta de correo. Para que esto no suceda, se presenta la opción de calificar la dirección de la lista como "lista segura". Otra opción interesante para combatir el correo no deseado es la posibilidad de **bloquear los gráficos con formato HTML**. Es una opción útil para bloquear imágenes ofensivas o dispositivos de rastreo como los web bugs, que están basados en imágenes transparentes.

Yahoo! por su parte, complementando a las herramientas comentadas para Hotmail, ha desarrollado un dispositivo denominado Spamguard que reduce la cantidad de Spam que llega a las cuentas de sus usuarios. Se trata de unas **baterías de filtros que se reconfiguran en tiempo real, con ayuda de los propios usuarios**. Yahoo! recomienda para ello hacer click en el enlace "es Spam" en todos los mensajes de Spam que se salten el filtro para estudiarlos e incluir sus remitentes al sistema Spamguard con el fin de ir mejorándolo.

Dejando a un lado el correo web, el cliente de correo más utilizado por el usuario medio (sin conocimientos tecnológicos específicos) es **Outlook** de Microsoft. Este cliente de correo, en su última versión, ha incorporado herramientas específicas contra el Spam, basadas en **filtrar las frases más usadas por los Spammers**. También presenta otra opción que permite marcar un mensaje que no hemos solicitado y automáticamente **colocar al remitente en algo similar a una lista negra propia**, para que sea rechazado por el software cuando intente nuevamente enviar un mensaje. Aunque se puede considerar un gran avance, ya que en versiones anteriores la única forma de filtrado que presentaba era la opción de bloquear remitentes, estos tipos de filtrado no resultan muy efectivos.

Hay otras soluciones externas especializadas más efectivas, que el usuario puede agregar e instalar para mejorar las que incorpora Outlook. Las tres más populares son:

- **Spam Attack Pro**: Incorpora una lista de mensajes Spam a la que se puede ir añadiendo otros mensajes propios. Puede conseguirse en la dirección www.sofwiz.com/html/Spam_attack_pro.htm
- **Spam Exterminator** (www.unisyn.com/Spamex): Revisa el correo en busca de Spam conforme a una base de datos con 17.000 direcciones.
- **Spamkiller** (www.Spamkiller.com): Es uno de los más completos. Puede trabajar con diferentes tipos de filtros. Detiene los mensajes según el remitente, palabras clave, título o cualquier otra indicación que el usuario especifique.
- Si se desea instalar un filtro bayesiano, también existen varias posibilidades como **Spammunition, SpamBayes, Spam Bully, InboxShield, Junk-Out, Outclass, Disruptor OL o SpamTiger**.

Acciones desde el punto de vista del administrador de correo electrónico

El administrador del correo electrónico de una organización que es víctima de Spam tiene al alcance de su mano la posibilidad de combatirlo de la forma más efectiva. Desde su responsabilidad de administrador, debe estar comprometido con la lucha contra el Spam no permaneciendo pasivo ante el problema.

En primer lugar, el administrador **debe intentar proteger su organización de los ataques de los Spammers**, acción que puede llevarse a cabo mediante una combinación de las herramientas expuestas en este apartado. Dependiendo de las características concretas de la organización y de su política, le interesará un tipo u otro de medidas.

En segundo lugar, **debe atender las quejas de los usuarios, ya sean de su organización o externos**. Estas quejas pueden aportar datos de interés a cerca de los Spammers. También informan al administrador de que desde su organización se están llevando a cabo actividades relacionadas con el Spam. Este último caso sería de extrema gravedad, por lo que deberían tomarse cuanto antes las medidas pertinentes para intentar atajar el problema, definidas por la organización a la que pertenece.

Por otra parte, **ha de intentar localizar las direcciones origen del Spam que ha llegado a la organización**. Habrá de tener en cuenta que las cabeceras de los mensajes pueden estar manipuladas y, por tanto, ser falsas o erróneas. Deberá estudiarlas con atención, con el fin de identificar la verdadera fuente del Spam y no dejarse engañar por las posibles direcciones trampa que los Spammers hayan introducido para ocultar su identidad.

Si se obtiene la identidad del emisor de Spam, **se debe efectuar una queja o denuncia al responsable del dominio origen y de la dirección IP origen del Spam.** Las direcciones de correo de dichos responsables (si el dominio o dirección IP están adecuadamente configurados) pueden obtenerse a través de la consulta a la base de datos whois que corresponda. La queja será enviada al postmaster del dominio origen cuya dirección puede ser postmaster@dominio_origen o abuse@dominio_origen . De cualquier manera, antes de enviar un mensaje a estas direcciones siempre habrá que asegurarse, en la medida de lo posible, de que efectivamente existen.

Si se trata de Spam que ofrece servicios de empresas, organismos o individuos españoles, a los cuales no se les ha autorizado para que nos envíen comunicaciones comerciales, **se debe comunicar este hecho a los organismos pertinentes**. Estos organismos son entre otros: La Agencia de Protección de Datos (www.protecciondedatos.org), el Ministerio de Industria Comercio Y Turismo (www.setsi.min.es) y organismos nacionales de lucha contra el Spam, como la Asociación de Usuarios de Internet (www.aui.es/contraelSpam).

Si el Spam viene de fuera de España, siempre podemos comunicarlo a organismos internacionales de lucha contra el Spam como Euro Cauce (www.euro.cauce.org/es/index.html) o Spam Abuse (http://Spam.abuse.net). Para Spam procedente de Estados Unidos podemos remitir la queja a la Comisión Federal del Comercio de Estados Unidos (FTC, Federal Trade Commission), en uce@ftc.gov.

Puede ocurrir que la dirección del emisor del mensaje corresponda a una persona inocente, que desconoce el proceso que se está llevando a cabo, por lo que el mensaje que se envíe debería ser siempre en **un tono educado y con carácter informativo**. También es interesante destacar que bastantes personas de las que llevan a cabo prácticas abusivas con el correo electrónico, no lo hacen de forma intencionada para molestar y por ello es importante informarlas educadamente.

Estas quejas pueden servir como realimentación y ayudar a los organismos de lucha contra el Spam a tomar medidas contra los Spammers, a identificar en mejor medida nuevas técnicas de Spam, etc.

Como ya expusimos en el apartado ”Acciones desde el punto de vista del usuario”, lo que nunca se debe hacer es bombardear con mensajes a la dirección de correo electrónico del Spammer, aunque se tenga la seguridad de que sea ésta verdaderamente. Esta acción tiene varios posibles “efectos secundarios” que son peores que los propios derivados del Spam:

- Si por casualidad esa dirección no fuera correcta, se estaría bombardeando a un inocente.
- Se pueden producir efectos en otros usuarios de ese proveedor, que nada tienen que ver con el problema.
- Los Spammers profesionales tiene unos filtros por lo general de mayor calidad, por lo que no les afectará este tipo de bombardeo.
- Se está suministrando direcciones de correo electrónico a una persona que las va a utilizar para enviar basura en el futuro.

CAPÍTULO 7: ESTADÍSTICAS SOBRE EL E-MAIL Y EL SPAM

Este capítulo recoge un conjunto de estadísticas que permiten valorar la evolución del correo electrónico y del Spam a nivel mundial y nacional.

Se ha incluido un estudio realizado por la AIMC (Asociación para la Investigación de Medios de Comunicación) a finales del 2003 con más de 30.000 respuestas, en el que se recoge información, obtenida a través de encuestas y sondeos, sobre el uso del correo electrónico en España y la percepción que tienen los usuarios españoles de fenómenos como el Spam.

7.1. Evolución del e-mail en el mundo

A continuación se presentan diferentes gráficas con la evolución del correo electrónico en el mundo.

E-mails enviados en los últimos tres años

Año	Valores x 10^{12}
2001	9
2002	11
2003	12.5

Tabla 4. Correos enviados en los últimos tres años

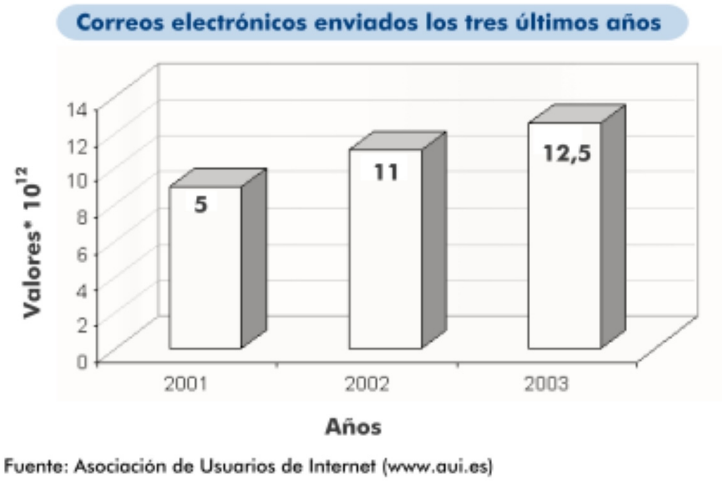

Figura 13

Número de buzones de correo en el mundo

Año	Valores en millones
2001	547
2002	708
2003	930
2004	1258
2005	1715

Tabla 5. Evolución del número de buzones de correo

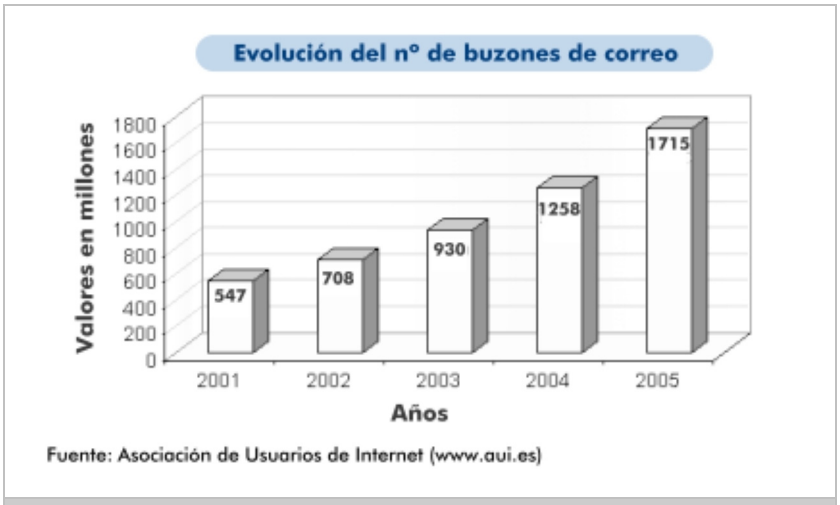

Figura 14

Tipos de buzones de correo

Tipo de buzón	Valores
Webmail	38%
Correos internos (empresas/organizaciones)	36%
ISP - Usuarios finales	13%
ISP corporativo	7%
Negocios externalizados (outsourced)	4%
Teléfonos móviles	2%

Tabla 6. Tipos de buzones, 2003

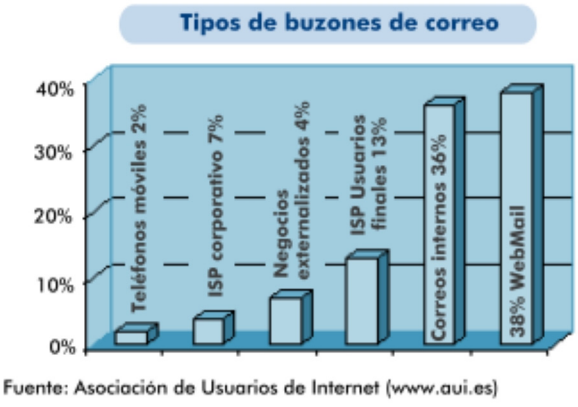

Figura 15

7.2. Evolución del e-mail en España

A continuación se presentan diferentes gráficas de la evolución del correo electrónico en España, desde Octubre de 1996 hasta Noviembre de 2003.

Servicios utilizados durante el último mes

Fecha	www (%)	Correo (%)
Octubre/Noviembre 96	72,1	66,2
Febrero/Mar 97	75,8	61,6
Abril/Mayo 97	78,3	67,8
Octubre/Noviembre 97	77,7	66,2
Febrero/Mar 98	80,9	74,7
Abril/Mayo 98	80,4	76,3
Octubre/Noviembre 98	83,1	77,6
Febrero/Mar 99	84,1	78,5
Abril/Mayo 99	82,8	74,7
Octubre/Noviembre 99	81,3	78,2
Febrero/Mar 00	88,2	79,3
Abril/Mayo 00	86	81,3
Octubre/Noviembre 00	85,7	72,6
Febrero/Mar 01	89,8	75

Abril/Mayo 01	89,7	74,2
Octubre/Noviembre 01	92,2	77,9
Febrero/Mar 02	91,4	75,8
Abril/Mayo 02	90,3	80,5
Octubre/Noviembre 02	88,5	78
Febrero/Mar 03	90,6	80,2
Abril/Mayo 03	**93,5**	**82,9**
Octubre/Noviembre 03	**92,3**	**82,8**

Tabla 7. Servicios utilizados durante el último mes

Figura 16

Disponibilidad de E-mail

A continuación se puede ver una clasificación de las diferentes cuentas de correo de que disponen los usuarios de e-mail. La suma de porcentajes es superior al 100%, ya que un número significativo de encuestados declararon dos o más respuestas.

	Absolutos	%
BASE	**40.865**	**100**
Particular	39.092	95,7
Personalizada en el trabajo/centro de estudios	19.273	47,2
General en el trabajo/centro de estudios	5.112	12,5
No dispongo	42	0,1
NS/NC	93	0,2

Tabla 8. ¿Dispone de dirección de e-mail?

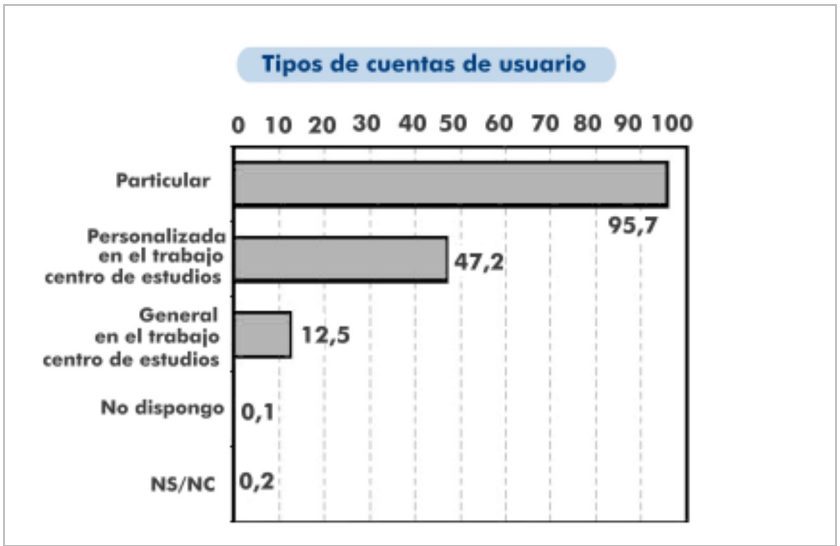

Figura 17

Número de direcciones de e-mail

	Absolutos	%
BASE (dispone de e-mail)	**40.730**	**100**
Una	7.069	17,4
Dos	13.003	31,9
Tres	9.219	22,6
Más de tres	11.032	27,1
NS/NC	407	1,0

Tabla 9. Si dispone de e-mail, ¿a través de cuántas direcciones diferentes recibe su correo?

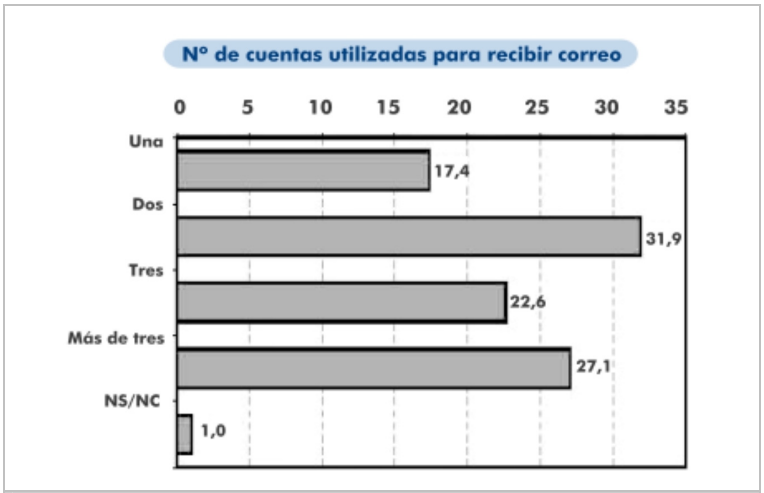

Figura 18

Tipo de direcciones de e-mail

	Absolutos	%
BASE (dispone de e-mail)	**40.730**	**100**
Sólo dispone de dirección/es convencionales (POP3 / IMAP)	10.483	25,7
Sólo dispone de dirección/es a través de una página Web (mensajería gratuita ofrecida por Hotmail o diferentes portales)	12.209	30,0
Dispone de ambos tipos de direcciones de correo	17.813	43,7
NS/NC	225	0,6

Tabla 10. Su dirección o direcciones de correo son del tipo…

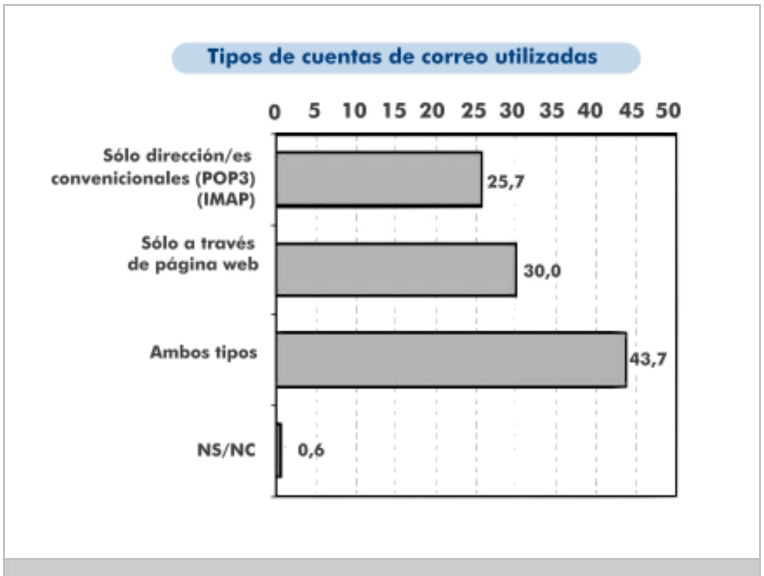

Figura 19

Software de correo electrónico

	Absolutos	%
BASE (dispone de e-mail)	**40.730**	**100**
Outlook (Microsoft)	20.833	51,1
Messenger (Netscape)	6.534	16,0
CC:mail (Lotus)	752	1,8
Eudora	619	1,5
Exchange (Microsoft)	493	1,2
Otro programa	2.482	6,1
A través de página web	7.193	17,7
No sé	1.501	3,7
NS/NC	323	0

Tabla 11. ¿Qué software de correo electrónico utiliza preferentemente?

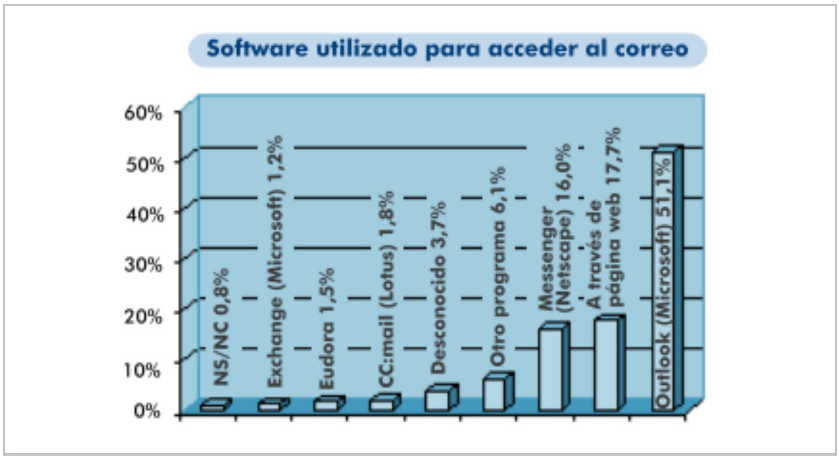

Figura 20

Correos electrónicos recibidos/enviados

	Absolutos	%
BASE (dispone de e-mail)	**40.730**	**100**
...recibe?		
Menos de 5	1.859	4,6
Entre 5 y 20	12.461	30,6
Entre 21 y 50	11.893	29,2
Entre 51 y 100	7.162	17,6
Más de 100	7.305	17,9
NS/NC	50	0,1

...envía?		
Menos de 5	9.751	23,9
Entre 5 y 20	19.305	47,4
Entre 21 y 50	7.253	17,8
Entre 51 y 100	2.698	6,6
Más de 100	1.521	3,7
NS/NC	202	0,5

Tabla 12. En una semana media, ¿cuántos correos electrónicos…

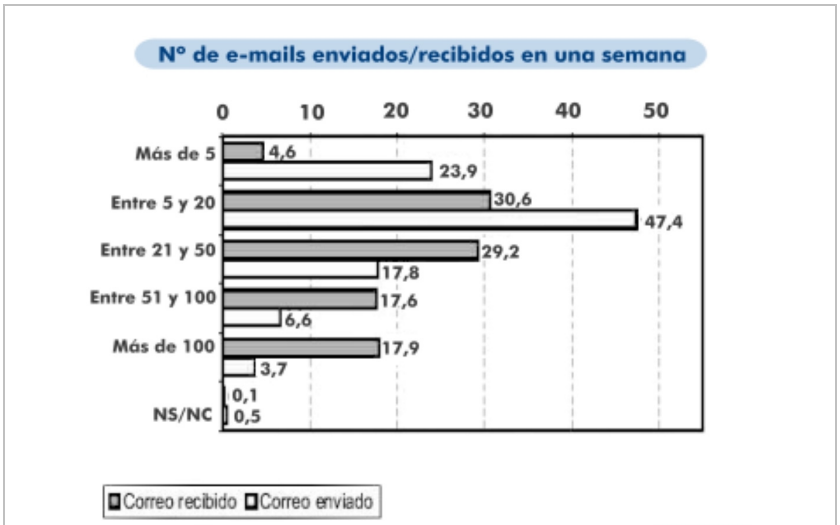

Figura 21

Spamming – Frecuencia

	Absolutos	%
BASE (dispone de e-mail)	**40.730**	**100**
Nunca he recibido ninguno	1.049	2,6
Menos de 1	1.936	4,8
Entre 1 y 5	6.569	16,1
Entre 6 y 10	7.165	17,6
Entre 11 y 25	7.891	19,4
Entre 26 y 50	5.895	14,5
Entre 51 y 100	4.263	10,5
Entre 101 y 200	2.843	7,0
Entre 201 y 500	1.917	4,7
Más de 500	1.077	2,6
NS/NC	125	0,3

Tabla 13. En una semana media, ¿cuántos mensajes no solicitados/deseados recibe?

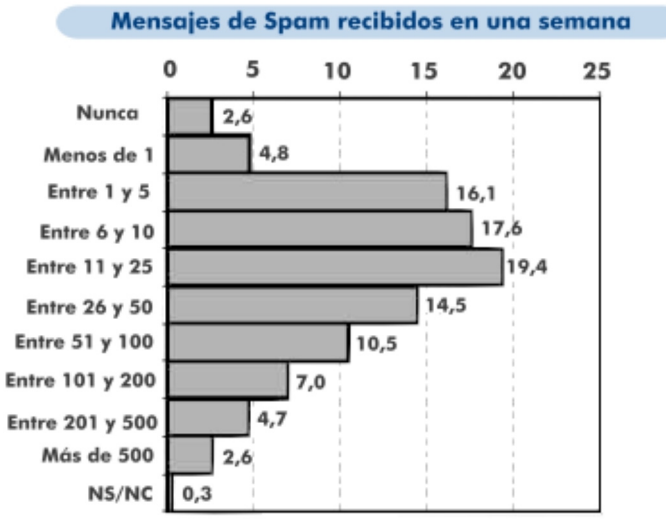

Figura 22

Spamming – Opinión

	Absolutos	%
BASE (dispone de e-mail)	**40.730**	**100**
Dada su utilidad habría que promover su desarrollo	524	1,3
No hacer nada. La situación está bien tal como está	1.162	2,9
Debería prohibirse y perseguirse legalmente esta práctica	13.191	32,4
Crear lista de empresas/personas que realizan estas actividades para filtrar mensajes	10.038	24,6
Crear registro con direcciones de aquellos que no quieran recibir mensajes (lista Robinson)	12.397	30,4
No sé, no tengo opinión al respecto	3.080	7,6
NS/NC	338	0,8

Tabla 14. Concerniente a la situación creada por el correo no solicitado, ¿con cuál de las siguientes respuestas está más de acuerdo?

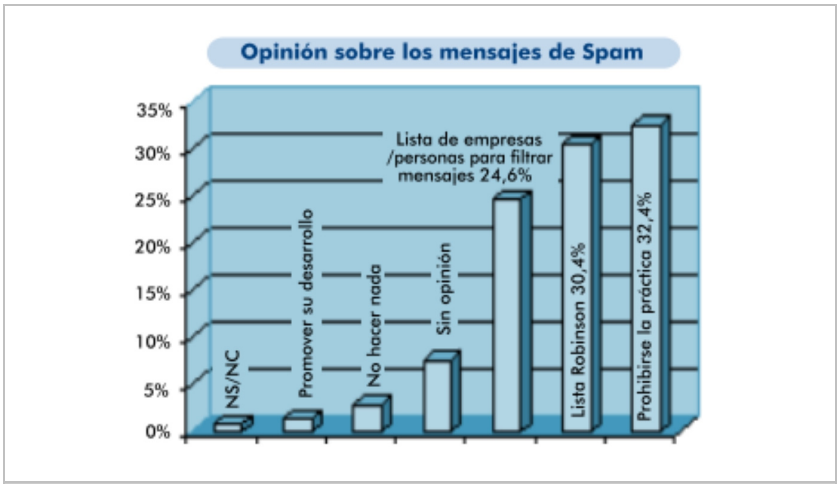

Figura 23

7.3. Análisis de la situación del Spam en cifras

En este apartado se han analizado y comparado los resultados de diferentes estudios sobre el Spam, con el fin de aportar una serie de datos más o menos objetivos acerca de: Qué tipos de negocios se promocionan mediante Spam, qué volumen de Spam circula en Internet, cuáles son los costes que ocasiona y la opinión de los usuarios. Por último también se han incluido unos datos interesantes obtenidos a partir de entrevistas realizadas a varios Spammers, que pueden aportarnos su visión.

Naturaleza del Spam

Categorías:

El tipo de productos y servicios que se intenta promocionar a través del Spam son básicamente **productos financieros, bienes de consumo y pornografía**. Para realizar el siguiente análisis, cuyos resultados se muestran en la próxima tabla, se han tenido en cuenta los resultados de tres estudios[15]: De la Asociación de Usuarios de Internet en España (AUI), de la Comisión Federal del Comercio de Estados Unidos (FTC) y de la compañía norteamericana Clearswift.

[15] El estudio realizado por la AUI se llevó a cabo durante el mes de abril de 2003, en el que se recibió un total de 5627 mensajes no solicitados en sus cuentas de correo electrónico. El estudio de la Comisión Federal del Comercio de Estados Unidos de Estados Unidos, "False Claims in Spam, a report by the FTC's Division of Marketing Practices", fue realizado en abril de 2003 analizando 1000 mensajes Spam tomados de una muestra aleatoria de más de 11 millones de mensajes Spam. Por último, el estudio "Índice de Spam" realizado por la compañía norteamericana Clearswift en su tercera edición (junio-agosto 2003) fue realizado para explicar las tendencias y usos del marketing directo a través de Internet. Los resultados de este estudio han sido tomados del artículo "Los productos de consumo y de salud son los que más utilizan el Spam", www.noticiasdot.com

AUI	FTC	Clearswift
		Bienes de consumo (31%)
Vacaciones (12%)	Viajes / Ocio (2%)	
Informática / Internet (software + ordenadores y periféricos) (10%)	Informática / Internet (7%)	
	Otros productos / servicios (16%)	
	Educación (1%)	
	Salud (10%)	Salud (21,2%)
Pornografía (15%)	Contenidos de adultos (18%)	Pornografía (13,6 %)
Productos financieros (12%)	Productos financieros (17%)	Productos financieros (17,2%)
Trabajo fácil (10%)	Inversiones / Oportunidades de negocio (20%)	
	Otros (9%)	Otros (5,4%)
Casinos / juegos de azar (14%)		Ofertas de juegos (6%)
Sorteos (11%)		
Cartas encadenadas (7%)		
		Estafas y timos 2%
		Spam interrelacionado 3,6%

Tabla 15. Comparativa de los productos y servicios promocionados mediante Spam

Fuentes: FTC, AUI, y estudio Clearswift

Dado que los estudios estaban planteados desde diferentes perspectivas, para poder establecer una comparación entre ellos, se han distribuido los temas de manera que los que se refieran a grupos similares queden colocados en la misma fila de la tabla.

Así, en el estudio de Clearswift, se observa que los bienes de consumo representan el tema con mayor porcentaje de Spam observado. Los temas que se presentan en los tres estudios con porcentajes similares son los contenidos pornográficos y los productos financieros, por lo que no cabe lugar a dudas que se trata de dos grupos muy presentes en el Spam. Por otro lado, se observa que en Estados Unidos (estudios de la FTC y de Clearswift) aproximadamente un 20% del Spam está relacionado con temas de salud. En el estudio realizado a usuarios españoles (AUI), es importante el porcentaje referido a sorteos, casinos y juegos de azar (un 35%).

Días, horas y tamaños de los mensajes:

Durante el mes de abril de 2003, la AUI recolectó los mensajes no solicitados recibidos en sus cuentas de correo electrónico con el fin de elaborar **estadísticas por hora, día y mes**, y **observar su evolución en cantidad y tamaño**. De este estudio realizado con un total de 5627 *e-mails* recibidos no solicitados, a razón de 201 por día, se extrajeron las siguientes **conclusiones**:

- Lunes y martes parecen ser los días preferidos por los Spammers para enviar sus mensajes, decayendo hacia el fin de semana. Jueves y domingos aparecen como los días menos propensos para realizar esta actividad.

- El horario preferido por los Spammers es desde las 13:00 a las 18:00 horas, mientras que el más desfavorable parece ser la madrugada. Si tenemos en cuenta que el 80% estaba escrito en inglés, podríamos deducir que este horario coincide con las primeras horas de actividad en Estados Unidos (de 8 de la mañana a la 1 del mediodía).

- En cuanto al tamaño, la inmensa mayoría de los Spammers envía mensajes inferiores a 10 Kilobytes, aunque se recibieron casi 30 mensajes no solicitados superiores a 40 Kilobytes.

- En total, recibieron unos 32,8 Megabytes de Spam, un promedio de casi 1,2 Megabytes por día. Esto, para un usuario de una cuenta de correo en Internet cuyo buzón tenga una capacidad de 5 Megabytes, por ejemplo, significaría el bloqueo de su cuenta en unos cuatro días.

Se advierte una evolución importante en la cantidad de Spam recibido desde los primeros días hasta finales del mes de estudio, lo que indica la tendencia creciente del Spam, aunque el periodo de estudio sea de solamente un mes.

Origen del Spam por países:

Un estudio realizado durante el mes de marzo de 2003 por la compañía **MessageLabs**, proveedora de sistemas de seguridad informática, analizó el origen de 104 millones de mensajes Spam. Este estudio indica los porcentajes de mensajes clasificados por país de origen.

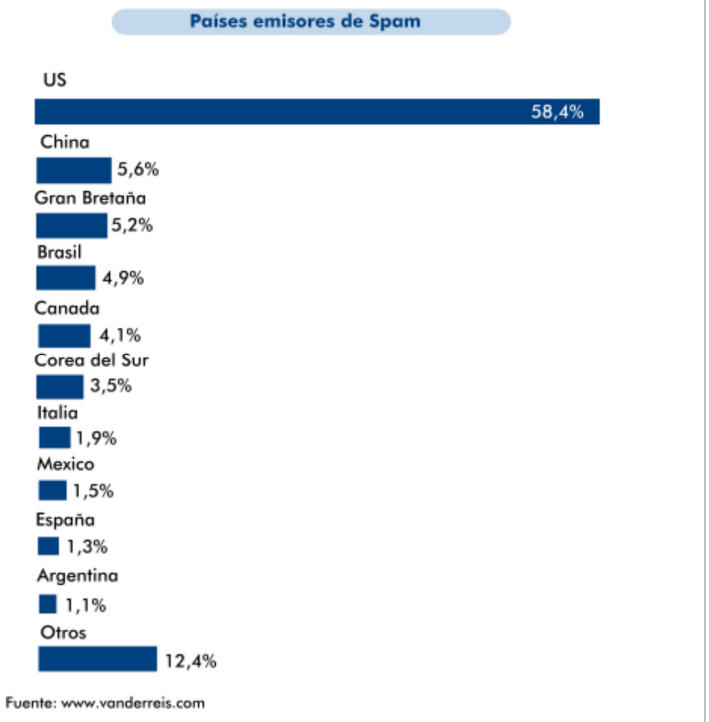

Figura 24

El primer país "productor" de Spam es Estados Unidos, con el 58% de los mensajes, seguido muy de lejos por otros países como China (5,6%), Gran Bretaña (5,2%) y Canadá (4,1%). Estas cifras corroboran el hecho comprobado por todos de que la mayoría del Spam está escrito en inglés. Otro dato interesante es que España está entre los 10 primeros países productores de Spam, aún contando con una ley que lo prohíbe. Aclarar que este puesto es por direcciones IPs que en muchos casos son IPs residenciales hackeadas por Spammers de fuera de España.

Si nos remitimos a un estudio reciente publicado por **Sophos** la procedencia del Spam por países varía ligeramente:

El 42,53% de los correos electrónicos no deseados tiene su origen en Estados Unidos. Corea de Sur ocupa la segunda plaza por volumen (15,42%) de emisión de correos basura, sin pasar por alto que el Spam procedente de este país se ha triplicado desde el pasado mes de febrero. Por el contrario, Canadá, que en febrero ocupaba dicha posición, ha conseguido reducir más de la mitad (desde un 6,8% a un 2,9%).

China y Hong Kong se colocan en la tercera posición al emitir un 11,62% del total, seguidos de Brasil (6,17%), Canadá (2,91%) y Japón (2,87%). Completando la lista pero con porcentajes inferiores al dos por ciento aparecen Alemania (1,28%), Francia (1,24%), España (1,16%) y Reino Unido (1,15%); mientras que México (0,98%) y Taiwán (0,91%) constituyen el origen de porcentajes inferiores al uno por ciento. El 11,76% restante del total se reparte entre diversos países.

Cantidad de Spam que circula en Internet

Según los datos que baraja el Ejecutivo comunitario[16], en 1999 el porcentaje de tráfico debido a los mensajes Spam frente al total del tráfico en Internet era del 5%, en 2001 representaba el 7% del total y en 2003 representa más de la mitad del tráfico de Internet. De modo que el tráfico debido al Spam se ha multiplicado por siete en tan solo dos años, por lo que se ha convertido en una amenaza para el desarrollo y la confianza de los usuarios en las comunicaciones electrónicas. En la siguiente gráfica podemos apreciar esta tendencia de crecimiento exponencial.

Figura 25

Sin embargo estas cifras no muestran el volumen de Spam en Internet en la segunda mitad del año 2003 y principios de 2004. Para ver qué ha ocurrido en el último año, podemos acudir a los datos aportados por el estudio realizado por Brightmail[17]. Éste indica que el Spam representó en febrero de 2004 el 62% de los e-mails que se envían y reciben en Internet. En la gráfica siguiente puede apreciarse la tendencia del porcentaje de Spam en Internet desde marzo de 2003.

[16] Esta información ha sido obtenida del artículo "La UE anuncia medidas contra el '*Spam*' por la desconfianza que causa" (27 de enero de 2004), www.elmundo.es/navegante

[17] Esta información ha sido obtenida del sitio web www.aui.es/contraelSpam

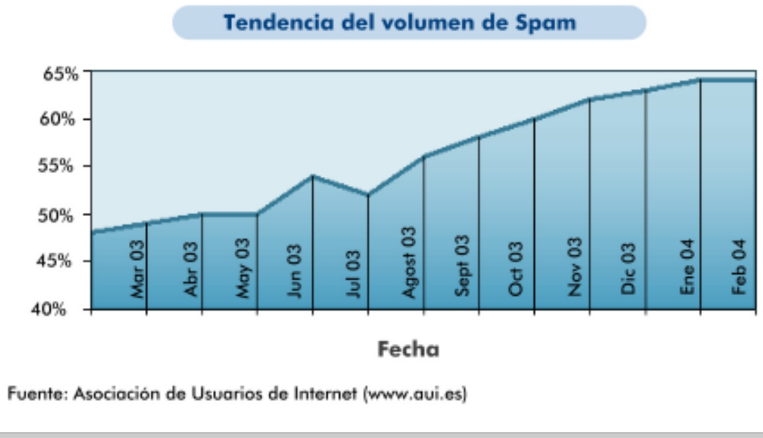

Figura 26

En la gráfica se aprecia un pico significativo del volumen de Spam entre agosto y octubre de 2003. El máximo entre estas fechas tuvo lugar concretamente el 26 de agosto de 2003 y fue debido al efecto del **virus *Sobig***, el cual batió todas las marcas de Spam.

Un aspecto a destacar, es que los datos presentados para mediados de 2003 hablaban de que el Spam representaba aproximadamente el 50% del tráfico de Internet a fecha de julio de 2003. Sin embargo, después de la infección del virus, los niveles de Spam no volvieron a niveles de fechas anteriores, sino que tras la desinfección de los equipos, el Spam continuó creciendo con una tendencia al alza aún más acusada. Visto esto, podemos pensar que este crecimiento aún puede aumentar más y más, dado que otros virus más recientes como el *MyDoom*, se han extendido por Internet con la misma filosofía.

Cantidad de Spam recibido por los internautas:

Para analizar el número de mensajes Spam recibidos por los internautas españoles, hemos observado varios estudios. En primer lugar presentamos los resultados de las encuestas realizados por la AIMC en 2001 y 2002, que representan el usuario medio español de correo electrónico con una edad superior a 14 años[18].

[18] "4ª encuesta a Usuarios de Internet de la AIMC febrero 2001" y "5ª encuesta a Usuarios de Internet de la AIMC febrero 2002". Las encuestas se realizaron a una base imponible de 43.592 usuarios que poseen *e-mail*. Fue realizada en febrero de 2001 (4ª Encuesta) y en febrero de 2002 (5ª Encuesta) a una muestra del EGM que es probabilística y representativa de la población española de 14 ó más años.

¿Con qué frecuencia recibe mensajes no solicitados/deseados?	AIMC F-2001	AIMC F-2002
Más de uno al día	17,8 %	40,3 %
Uno al día	4,4 %	4,9 %
Varios a la semana	25,1 %	27,3 %
Uno a la semana	5,4 %	3,5 %
Varios al mes	13,2 %	9,3 %
Uno al mes	4,9 %	2,5 %
Con una frecuencia menor	14,9 %	7,6 %
Nunca he recibido ninguno	14,1 %	4,3 %
NS/NC	0,3 %	0,3 %

Tabla 16. Número de mensajes Spam que reciben los usuarios. Fuente: AIMC, 2001 y 2002

Lo más destacable de los resultados mostrados, es que un 22,2% de los usuarios de correo electrónico padecía el Spam en 2001, pasando a ser casi la mitad (un 45%) en 2002. Además, observamos cómo decrece el porcentaje de usuarios que reciben Spam con frecuencias menores de varios por semana. Son datos importantes a tener en cuenta porque se refieren a un usuario español medio mayor de 14 años, no a usuarios experimentados que hacen gran uso del servicio.

A continuación adjuntamos los gráficos obtenidos de un estudio realizado por la AUI entre abril y mayo de 2003[19].

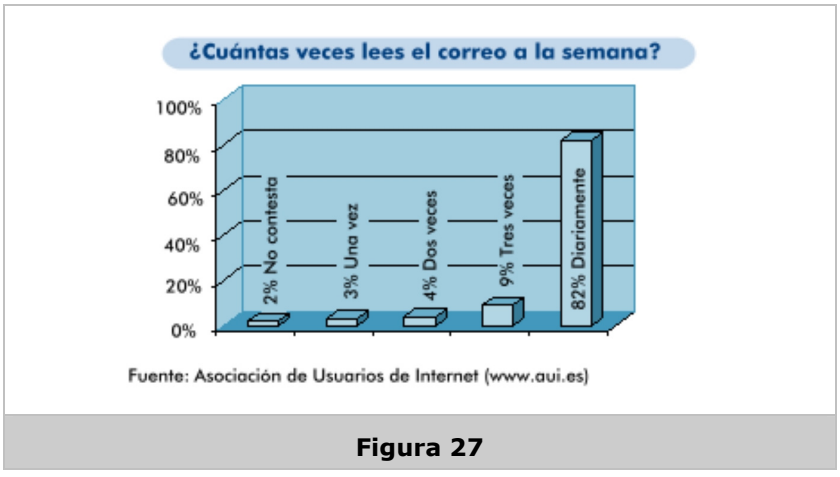

Figura 27

[19] Encuesta realizada por la Asociación de Usuarios de Internet (AUI) a través de su página web (www.aui.es) entre abril y mayo de 2003, con un número de respuestas de 2054. Esta encuesta no es representativa de la población total española, al igual que la efectuada por la AIMC, sino de un porcentaje de internautas experimentados y con interés sobre el tema, que navegan en la página de esta asociación y que están lo suficientemente concienciados con el tema.

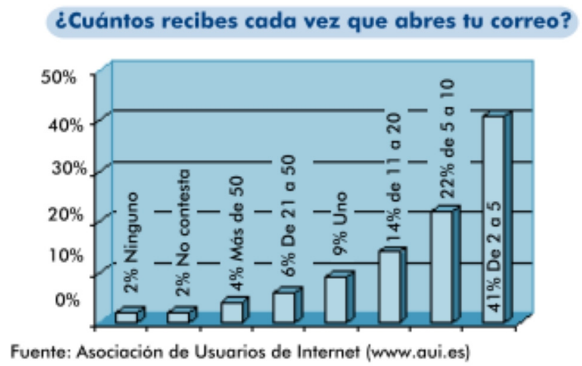

Figura 28

El segundo gráfico muestra los porcentajes de usuarios que reciben el número de mensajes Spam indicados. Se observa que la mayoría de los usuarios recibe entre 2 y 5 e-mails no solicitados (un 41%). Es significativa también la proporción de usuarios que reciben más de 20 (un 10%), destacándose un 4% que recibe más de 50 mensajes Spam cada vez que lee su correo, suponiendo que se lee el correo el número de veces a la semana indicado en el primer gráfico (82% a diario).

Estos resultados muestran que el Spam no es sólo un problema que afecta a las empresas o a las cuentas de usuarios avanzados y administradores, sino que afecta a todos los usuarios. Así, los datos nos indican que en Hotmail, el proveedor de correo web más utilizado de Internet con 110 millones de usuarios, transcurridos varios días de abrir una cuenta de correo (aunque no se haya usado), el internauta podrá comprobar cómo el 80% de los mensajes que recibe son Spam[20]. Algo parecido ocurre con otros grandes proveedores, como American Online, que indicó[21] que bloquea unos 2.000 millones de mensajes de correo masivo a diario, una media de 67 por cada cuenta de e-mail.

Este gran volumen de mensajes recibidos por los internautas, redunda en un coste y un empleo de tiempo en borrar y clasificar los mensajes no deseados. Así, según Basex[22], los usuarios gastan unos 15 minutos diarios en comprobar y borrar el Spam que les llega.

---

[20] Datos obtenidos del artículo "¡Muerte al *Spam*!" (30 de abril 2003), Rodríguez, G., www.libertaddigital.com

[21] "El volumen del correo masivo amenaza el futuro del '*e-mail*'" (1 de mayo de 2003), www.iblnews.com

[22] Dato obtenido del estudio "Spam E-mail and Its Impact on IT Spending and Productivity" (diciembre de 2003), Spira, J. B., realizado por Basex Inc., www.basex.com

Costes derivados del *Spam*.

Costes que afrontan las empresas:

El instituto estadounidense especializado Basex, realizó un estudio en diciembre de 2003[23] para intentar estimar los costes que supone el Spam a las compañías en el mundo. Para ello, estimó que los gastos de las empresas, debidos al Spam, pueden clasificarse en:

- pérdida de productividad de los empleados,
- saturación de los sistemas de correo electrónico,
- ancho de banda,
- costes de almacenaje,
- soporte a los usuarios,
- software antiSpam
- y formación a los usuarios.

Con todo ello estimó un gasto cercano a 20.000 millones de dólares al año en todo el mundo. Tal y como afirma el estudio, las pérdidas oscilan entre los 600 y los 1.000 dólares por salario y empleado al año, lo que implica que, por ejemplo, una empresa con 15.000 trabajadores contratados afronta un gasto anual de más de 12 millones de dólares sólo por culpa del Spam.

Otro estudio anterior publicado por el Instituto Ferris Research[24] en enero de 2003, estimaba que el Spam iba a costar unos 10.000 millones de dólares en 2003 tan solo en las empresas estadounidenses. Durante el 2002, para las mismas empresas, el coste del Spam ascendió a 9.000 millones de dólares, mientras que para las europeas ascendió a los 2.500 millones. El cálculo realizado por la firma Ferris Research, tuvo también en cuenta la utilización de ancho de banda, el uso de soporte técnico y la pérdida de productividad del trabajador, que representaban aproximadamente un 40% del total de pérdidas financieras.

Estos datos han hecho que las compañías y los gobiernos, no sólo los proveedores de servicio, se hayan tomado en serio este problema.

---

[23] "Spam E-mail and Its Impact on IT Spending and Productivity" (diciembre de 2003), Spira, J. B., realizado por Basex Inc., www.basex.com.

[24] Información obtenida de los artículos "El '*Spam*' cuesta 20.000 millones de dólares a las empresas en todo el mundo" (30 de diciembre de 2003), www.elmundo.es/navegante y "¡Muerte al *Spam*!" (30 de abril 2003), Rodríguez, G., www.libertaddigital.com.

Costes que afrontan los usuarios:

Los usuarios también deben hacer frente a los costes derivados del Spam.

- Por un lado, **indirectamente**, puesto que si las compañías tienen que afrontar un gasto extra, esto se traducirá en algunas ocasiones en un aumento de los precios de los servicios que les presten.
- De **forma directa**, el usuario también debe hacer frente a costes, sobre todo derivados del tiempo que necesita para limpiar su buzón de Spam. Podemos concluir que éste no es nada despreciable, dados los datos acerca de la cantidad de mensajes que reciben los usuarios cada vez que abren su correo, expuestos anteriormente.

La opinión de los usuarios

Como se ha deducido del análisis que se está llevando a cabo, **todos nos vemos afectados por el problema**, aunque los afectados más directamente son las compañías, debido a los grandes costes que deben afrontar. Sin embargo, desde el punto de vista de este informe, lo más interesante es analizar cuál es la opinión de los internautas y cuáles son sus reacciones ante el Spam.

Para conocer estos datos, hemos llevado a cabo un análisis de los resultados de varios estudios a los que haremos mención a lo largo de este apartado, entre ellos, el del centro de investigaciones Pew Internet and American Life Project[25], los de la AIMC para los años 2001 y 2002, el de la AUI[26] y el realizado por TACD[27].

---

[25] Estudio realizado en junio de 2003 entre 1.400 usuarios de Internet. Datos obtenidos del artículo "Los internautas esconden sus direcciones *e-mail* por miedo al "*Spam*"", www.noticiasdot.com

[26] "4ª encuesta a Usuarios de Internet de la AIMC febrero 2001" y "5ª encuesta a Usuarios de Internet de la AIMC febrero 2002". Las encuestas se realizaron a una base imponible de 43592 usuarios que poseen *e-mail*. Fue realizada en febrero de 2001 (4ª Encuesta) y en febrero de 2002 (5ª Encuesta) a una muestra del EGM que es probabilística y representativa de la población española de 14 ó más años.

La encuesta fue realizada por la Asociación de Usuarios de Internet (AUI) a través de su página web (www.aui.es) entre abril y mayo de 2003, con un número de respuestas de 2.054.

[27] "Consumer Attitudes Regarding Unsolicited Commercial Email (Spam)", octubre-diciembre de 2003. Realizado por TACD (Transatlantic Consumer Dialogue), y obtenido de http://www.tacd.org/docs/?id=225. El estudio se realizó mediante una encuesta a 21.102 personas de 36 países. Se observa que los porcentajes de las respuestas de las personas de los distintos países eran similares, por lo que se concluye que la opinión sobre el Spam es global.

Actitud de los usuarios ante el Spam:

Como ya hemos dicho, los más afectados por el Spam, desde el punto de vista económico, son las grandes compañías y los proveedores de servicio de Internet. Por ello, en la mayoría de las ocasiones ellos sí tienen una visión más o menos adecuada de la dimensión del problema. Sin embargo, **los usuarios no están adecuadamente informados**.

Es interesante saber que **a principios de 2003, el 69% de los usuarios españoles de correo electrónico no sabía qué es el Spam,** según un estudio realizado por Yahoo[28]. Éste indica también que los usuarios españoles y los franceses son los que consultan su correo electrónico con menos frecuencia en Europa. Curiosamente, el Spam es la primera causa de stress de los usuarios alemanes, por delante de los atascos de tráfico o de las compras navideñas.

Durante el año 2003, el espectacular aumento del Spam cambió el concepto que los usuarios tienen del correo electrónico. Los estudios consultados coinciden en que el usuario medio del correo electrónico opina que el Spam es muy molesto (entre un 96% y 92%). Además, según el estudio de Pew Internet and American Life Project, la mitad de los usuarios de Internet encuestados dice que el Spam, les ha hecho tener menos confianza en todo el e-mail en general, mientras que uno de cada cuatro señala que ahora usa el correo electrónico menos. La mayoría de los encuestados dijo que no daba su dirección electrónica a los sitios web, en un esfuerzo por mantenerse fuera de las listas de los Spammers.

El mismo sondeo encontró que la mayoría siente que puede hacer poco para bloquear los mensajes que llegan a sus buzones electrónicos todos los días y más de la mitad dijo que la inundación de Spam hace difícil encontrar los mensajes que desean. Resultados similares se desprenden del estudio realizado por TACD, en el que el 52% de los usuarios ha comprado menos o nada en Internet debido a su preocupación por el Spam.

Lo que más debería preocuparnos de los resultados de ambos estudios (ambos coinciden en este punto), es el hecho de que **aproximadamente la mitad de los usuarios encuestados tiene menos confianza en Internet en general**, lo que le ha llevado a comprar menos a través de este medio y a usar menos el correo electrónico.

---

[28] Información obtenida del artículo "Las cifras del correo basura", A. B. F., www.elmundo.es/navegante

Opinión de los usuarios acerca de las medidas que deberían tomarse para combatir el Spam:

Al igual que hemos venido haciendo en otros apartados, comenzamos analizando los estudios de la AIMC para los años 2001, 2002 y 2004[29].

Hemos de interpretar los resultados teniendo en cuenta que a principios de los años 2001 y 2002, un porcentaje muy importante de usuarios españoles (un 69%) no conocía el problema y su trascendencia. Por tanto, la siguiente tabla debe entenderse desde esta perspectiva. En todo caso, observamos ya el rechazo y la preocupación por tomar alguna medida para combatir el problema (72,6% en 2001 y el 83% en 2002).

¿Con cuál de las siguientes preguntas está más de acuerdo en relación con el Spam?	AIMC F-2001	AIMC F-2002	AIMC F-2003
Dada su utilidad habría que promover su desarrollo	3,8 %	3%	1,3%
No hacer nada. La situación está bien tal como está	8,2 %	5%	2,9%
Debería prohibirse legalmente esta práctica.	21,7 %	30%	32,4%
Crear lista de empresas/personas que realizan estas actividades para filtrar mensajes	21,9 %	25%	25,6%
Crear registro con direcciones de aquéllos que no quieran recibir mensajes (lista Robinson)	29 %	28%	30,4%
No sé, no tengo opinión al respecto	13,5 %	8%	6,6%
NS/NC	1,9 %	1%	0,8%

Tabla 17. Opinión de los usuarios acerca de posibles medidas para solucionar el problema del Spam. Fuente: AIMC, 2001 y 2002

Del año 2001 al 2004 se observa cómo aumenta significativamente el porcentaje de usuarios que piensan que debe prohibirse o crear listas negras, y decrecen los porcentajes de todas las demás contestaciones relacionadas con no tomar medidas o que no se tiene opinión acerca del tema.

Datos tomados del estudio de TACD (a fecha de diciembre de 2003) y de usuarios de distintos países, muestran que:

- el 82% de ellos piensa que los gobiernos deberían permitir que se les enviaran mensajes sólo habiéndolos solicitado previamente (*opt-in*),

[29] La encuesta se realizó a una base de 43.592 usuarios que poseen e-mail. Fue realizada en febrero de 2001 y febrero de 2002 por AIMC a una muestra del EGM que es probabilística y representativa de la población española de 14 ó más años.

- el 14% permitiendo el envío de mensajes siempre y cuando se facilite una forma de darse de baja de la lista (opt-out)
- y sólo el 2% considera que no hay que tomar ninguna medida.

La AUI en España fue más allá y planteó a los internautas quién debería perseguir esta práctica. Los resultados se muestran en el siguiente gráfico:

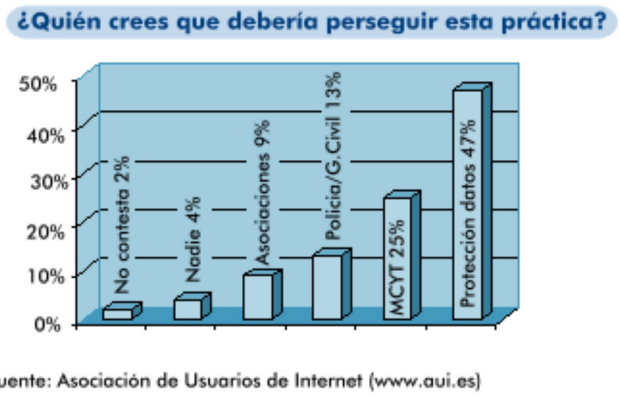

Figura 29

Reacción del usuario tras recibir los mensajes:

Según TACD, el 62% de los usuarios encuestados dice que usa algún tipo de filtrado como forma de combatir el Spam, pero sólo el 17% afirma que funcionan bien.

Un dato interesante es que un elevado porcentaje de los usuarios se queja a alguien de los e-mails no deseados:

- Según el estudio de Gartner Group[30], el 44% de los encuestados se quejan en este sentido. El 64% envían improperios al origen del Spam, el 53% se quejan al proveedor de acceso de Internet, el 34% al proveedor del Spammer, el 24% a la compañía que se beneficia del Spam, el 10% a amigos y conocidos, y el otro 10% al Gobierno.
- Por otra parte, según el estudio del TACD, el 24% se queja al emisor del mensaje, el 21% a su proveedor de Internet, el 14% al proveedor del que proviene el mensaje, el 9% a alguna organización de lucha contra el Spam y el 4% a alguna agencia gubernamental. Esta predisposición de los usuarios a efectuar una queja es muy positiva, ya que demuestra que están comprometidos con la causa.

[30] Los principales resultados de este estudio han sido obtenidos del artículo "La mayoría de los cibernautas son víctimas del correo indeseado", Tortello M. A., www.aui.es

- Sin embargo, según el estudio del centro de investigaciones Pew Internet and American Life Project, alrededor del 7% dijo que ha comprado un producto o servicio que le fue ofrecido en un e-mail no solicitado, mientras que un tercio indicó que había hecho clic en un enlace para obtener más información de la proporcionada por un mensaje Spam. Y, por último, dos tercios de ellos dijeron que habían hecho clic en un enlace para ser retirados de una lista de e-mail de Spammers. Dados estos últimos datos, el usuario en este punto sí necesitaría tener más información, puesto que responder de alguna manera a estos mensajes es lo que propicia que el Spam sea rentable para alguien.

Las cifras del negocio de los Spammers

Por último, hemos creído ilustrativo comentar algunas **cifras que se barajan acerca de las ganancias de los Spammers**, la tasa de respuesta que se deriva del Spam, etc. Hay que destacar que estas cifras no están soportadas por estudios objetivos (al igual que en apartados anteriores), sino por testimonios y supuestas entrevistas a Spammers, por lo que se advierte que estos datos sólo deben tomarse a modo de curiosidad.

Algo a destacar es la afirmación de Steve Linford, del proyecto Spamhaus (www.Spamhaus.org), con gran experiencia en la lucha contra el Spam, que dice que 150 Spammers son responsables del 90% del total del Spam que circula.

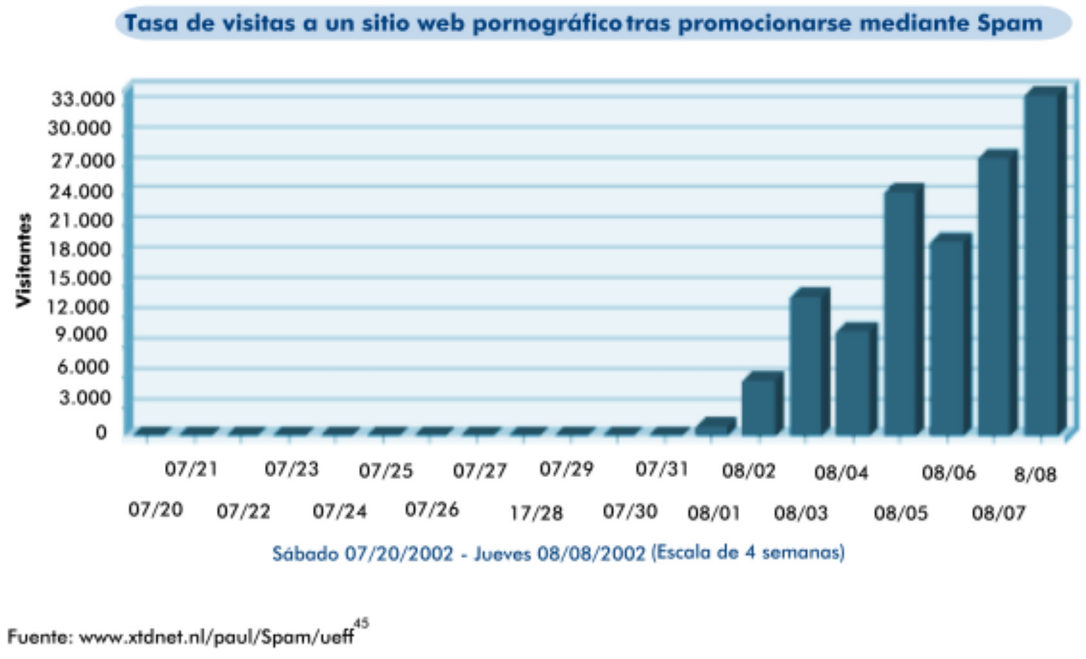

Figura 30

En primer lugar, en el gráfico anterior se demuestra cómo es de rentable promocionarse mediante Spam para cierto tipo de negocios. En él se aprecia la evolución de visitas que experimentó un sitio web anónimo dedicado a la pornografía, tras promocionarse mediante Spam.

Observamos cómo desde el 20/07/2003 que comienzan los envíos hasta el 08/08/2003 (menos de un mes) el número de visitas del sitio *web* aumenta desde un número insignificante de ellas, hasta 33.000.

Pero ¿cuántos son los honorarios de un buen Spammer? ¿Cuáles son los recursos que deben emplear para ello? Las respuestas a estas preguntas las encontramos en un artículo[31] del "Detroit Free Press" en el que se dice haber entrevistado a uno de los mejores Spammers, Ralsky, que con 57 años dice ser el maestro del Spam más viejo. Vive en una casa de 740.000 dólares (en un lugar que mantiene en el anonimato para evitar las amenazas de las que es víctima por parte de antiSpammers), tras irse al extranjero para evitar las leyes contra el Spam del estado de Virginia, donde operaba anteriormente. El Spam le ha hecho rico, promocionando sobre todo métodos para perder peso, casinos on line, ofertas para vacaciones, hipotecas o farmacias on line. Dispone de 20 ordenadores dispuestos en array, servidores y una línea de alta velocidad (de tipo T1). Controla 190 servidores de correo electrónico, 110 localizados en el sur de Estados Unidos, 50 en Dallas y 30 más en Canadá, China, Rusia y la India.

En 1997 comenzó su carrera como Spammer consiguiendo 6.000 dólares en una semana por hacer un envío masivo. Hoy, según Ralsky, cada computadora es capaz de enviar sobre 650.000 mensajes cada hora (más de un billón al día), encaminados a través de empresas de Internet extranjeras deseosas de venderle ancho de banda.

Según John Mozena of Grosse Pointe Woods, fundador de Coalition Against Unsolicited Commercial E-Mail (www.cauce.org), una organización de lucha contra el Spam, sus operaciones son sofisticadas, siendo difícil de localizar el emisor, por usar cientos de dominios para enviar su Spam.

Dice trabajar en esto 18 horas al día y su modo de operación es el siguiente: por un lado, se concentra en actualizar y aumentar su base de datos de direcciones de correo electrónico, que contaba a finales de 2002 con 250 millones de direcciones. Por otra parte, sigue a través de Internet los mensajes enviados, para confirmar que llegan a sus receptores.

En sus mensajes incluye un código tal, que si el mensaje es abierto, envía un mensaje de respuesta. De ahí puede comprobar la efectividad de sus campañas. El 0,33% de los mensajes son abiertos. La tasa de respuestas que consigue en media es del 0,25%, es decir, 625.000 respuestas de los 250 millones de direcciones que contiene su base de datos. Normalmente cobra una comisión por cada venta, pero ha conseguido hasta 22.000 dólares por un único envío a las direcciones de su base de datos completa.

---

[31] "Spam king lives large off others' *e-mail* troubles" (22 de noviembre de 2002), Wendland, M., http://www.freep.com/money/tech/mwend22_20021122.htm

Él dice que no hace nada ilegal y prefiere llamar a sus mensajes e-mail marketing en lugar de Spam. Asegura respetar el opt-out y ser fiel a la regla de no enviar ningún mensaje con contenido pornográfico. Por ello borra de su base de datos cada día 1.000 direcciones que solicitan no recibir más mensajes publicitarios y las conserva en otra base de datos que contiene 89 millones de direcciones.

Otras fuentes[32] nos indican que lo que cobra un Spammer por cada venta que consigue o por realizar un envío a un determinado número de direcciones de correo electrónico, puede variar mucho. Por ejemplo, según la empresa Symantec un Spammer medio puede cobrar 1.500 euros por mandar un millón de mensajes.

Los datos con respecto a la tasa de respuesta oscilan desde 0,001% a 0,25% (es decir, de 10 a 250 respuestas por cada millón de mensajes enviados).

Los costes a los que tienen que hacer frente los Spammers, según la compañía Emarketer[33], son en media de 0,00032 céntimos por cada Spam enviado, es decir 3,2 dólares por cada millón de mensajes enviados. Si volvemos a las cifras del Spammer Ralsky, le costaría 800 dólares cada envío a todas sus direcciones de la base de datos.

Sin embargo esta cifra (0,00032 ctm/Spam) es muy optimista. Según otros datos[34], el coste estaría en torno a los 250 dólares por cada 500.000 envíos (0,05 céntimos por mensaje, aunque esta cifra no sería extensible a más mensajes, puesto que el coste se iría reduciendo cuanto mayor fuera el número de mensajes enviados).

---

[32] "Técnicos y gobiernos sacan la artillería pesada contra el "*Spam*"", Molist, M. ((c) 2003), www.aui.es; "Spam king lives large off others' *e-mail* troubles" (22 de noviembre de 2002), Wendland, M., http://www.freep.com/money/tech/mwend22_20021122.htm; "For Bulk E-Mailer, Pestering Millions Offers Path to Profit", Mangalindan, M. (The Wall Street Journal, 13 de noviembre de 2002); www.alanluber.com; "Inside the *Spammer*'s world" (29 de junio de 2001), Livingston, B., http://news.com.com; "For Bulk E-Mailer, Pestering Millions Offers Path to Profit" (13 de noviembre de 2002), Mangalindan, M. del Wall Street Journal, http://www.alanluber.com

[33] "Técnicos y gobiernos sacan la artillería pesada contra el "*Spam*"", Molist, M. ((c) 2003), www.aui.es

[34] Véase el artículo "For Bulk E-Mailer, Pestering Millions Offers Path to Profit" (13 de noviembre de 2002), Mangalindan, M. del Wall Street Journal, http://www.alanluber.com

Estas cifras nos hacen llegar a dos **conclusiones**:

- Las tasas de respuesta del Spam son muy bajas, pero no lo son tanto para que el Spam no resulte rentable, tanto para la empresa anunciante, como para el Spammer.

- Igualmente, los costes de enviar un Spam son muy bajos, pero no lo suficiente para que el Spam sea rentable para cualquier tasa de respuesta o para cualquier negociación de comisión para el Spammer[35].

Por ello, **el Spam no es rentable para cualesquiera negocio o condiciones**.

[35] Véase el artículo "For Bulk E-Mailer, Pestering Millions Offers Path to Profit".

CAPÍTULO 8. VULNERABILIDADES DEL CORREO Y TÉCNICAS PARA PREVENIRLAS

La sencillez de los protocolos de correo electrónico, principalmente el de envío (SMTP), convierten a esta herramienta en vulnerable ante aquéllos que desean abusar de su simplicidad para eludir costes y/o responsabilidades, tal y como hemos visto en los capítulos precedentes. Uno de los principales objetivos en la lucha contra del Spam es conseguir actuar antes de que el correo basura "salga" a la Red, ya que una vez enviado genera esos importantes costes, así como complicaciones al resto de agentes que intervienen en la cadena de distribución.

Por ello resulta de vital importancia conocer las vulnerabilidades que presenta el correo electrónico, especialmente las aprovechadas por los Spammers, y tratar de eliminarlas, de forma que las medidas adoptadas en la lucha contra el Spam, descritas en el capítulo 6, resulten mucho más eficaces. El estudio de estas vulnerabilidades y cómo prevenirlas es el objeto del presente capítulo.

8.1. Falsificación del remitente

Como ya se ha expuesto a lo largo de este informe, una de las debilidades significativas del protocolo SMTP es que, tal y como funciona en la actualidad, **permite a cualquier cliente de correo asumir la identidad que desee.**

Esta vulnerabilidad es continuamente explotada por los Spammers para, mediante la falsificación de la dirección que remiten los mensajes, atravesar las barreras de comprobación de reputación que pudieran existir en el servidor de destino. Si fuera posible tapar este agujero, entonces dichas medidas podrían ser mucho más eficaces bloqueando el Spam.

No olvidemos que cuando se usa una dirección falsa hay dos perjudicados: el receptor del Spam y el propietario cuya dirección ha sido utilizada por el Spammer. Éste empezará a recibir devoluciones y quejas de los usuarios afectados. En algunos casos incluso puede suponerle que su servidor aparezca en una lista negra y quede también bloqueado para recibir sus correos normales.

Ya que el protocolo de envío de correos (SMTP) no realiza una autenticación de la persona que envía el correo, es relativamente fácil ocultar la identidad del remitente del mensaje, sustituyéndola por direcciones de origen falsas. Resulta muy difícil identificar a la persona física que ha enviado el correo y que ha podido cometer algún delito sirviéndose de éste. Una solución parcial es la de utilizar **autenticación en el momento de enviar el correo**, recurriendo a una extensión al protocolo SMTP, reflejada en la RFC 2554 y conocida como **ESMTP (Extended SMTP).**

8.2. Usurpación de identidades

La **suplantación de la identidad del dominio** se da en el protocolo SMPT, y es un caso más de falsificación del remitente. Se hace creer al receptor que el correo procede de alguien de confianza o conocido. Esta vulnerabilidad está intentando ser resuelta mediante diferentes **sistemas de identificación de remitente**, entre los que destacan:

Correo SMTP con Autorización de Dominio (David Green):

La propuesta describe mecanismos para especificar registros de recursos del tipo "Mail Transmitter" en el sistema de DNS, procedimientos de configuración de los servidores SMTP para hacer búsquedas efectivas de esos registros y métodos de configuración de los Agentes de Usuario de Correo para que puedan realizar filtrados en base a los registros.

Método RMX DNS RR para autorización SMTP ligera. (Hadmut Danisch [12]):

En esta iniciativa se propone un nuevo mecanismo de autorización para el transporte SMTP que se basa exclusivamente en mecanismos de seguridad organizativa y no requiere – pero permite – la utilización de mecanismos criptográficos.

Protocolo de Originador Designado DMP (Gordon Fecyk):

Contiene un procedimiento para identificar máquinas autorizadas para realizar envíos SMTP y almacenar la información en registros DMP. Adicionalmente se propone otro procedimiento por el que los servidores destinatarios de correo realizarán búsquedas en dichos registros, pudiendo rechazar o marcar los mensajes de correo que provengan de fuentes no identificadas en ellos.

Sender ID (Microsoft):

Propuesta de la empresa Microsoft para resolver el problema de la suplantación de dominios. Mediante Sender ID se pretende verificar que cada mensaje de correo electrónico realmente se ha originado en el dominio desde el que dice haber sido enviado. Este proceso se lleva a cabo comprobando que la dirección del servidor de origen está en una lista de servidores registrados, a los que el responsable de dominio o el destinatario de correo han autorizado a enviar correo. La comprobación se realiza automáticamente en el servidor de destino, antes de entregar el mensaje al destinatario.

Si la verificación resulta positiva, el mensaje se entrega normalmente; si falla, se realiza un análisis más profundo del mensaje sospechoso, que puede ser rechazado o marcado como engañoso (dependiendo de la configuración del software del servidor).

Sender Policy Framework – SPF (Wong Meng Weng y Mark Lentczner [15]):

Con el funcionamiento tradicional del sistema de correo, los diversos dominios hacen públicos sus registros de correo (MX) en el DNS, de manera que el resto del mundo sepa qué máquinas son las responsables de recibir correo para cada dominio en concreto.

Lo que propone SPF es que cada dominio publique registros "MX inversos", de manera que declare públicamente qué máquinas están autorizadas para enviar correo desde él.

De esta manera, al recibir un mensaje que se origina desde un dominio dado, se pueden analizar los registros "MX inversos" para asegurarse de que el correo proviene de quien debe.

Domain Keys (Yahoo [16]):

Propone la creación de un sistema de autenticación de dominios mediante criptografía de clave pública. El servidor de origen deber realizar dos tareas. Primeramente, el administrador del servidor genera una pareja de claves pública/privada que se utilizará para firmar los correos que se envíen desde el dominio. La clave pública se publica en el DNS, mientras que la privada se guarda en el servidor de correo. Posteriormente, cada vez que un usuario autorizado dentro del dominio va a enviar un mensaje, el sistema de correo automáticamente utiliza la clave privada almacenada para firmar digitalmente el mensaje.

Cuando el servidor de destino recibe un mensaje, extrae la firma digital y el supuesto dominio origen del mensaje. A continuación, obtiene la clave pública de ese supuesto dominio de los registros del DNS. Con la clave pública se podrá verificar que el mensaje de correo se envió desde el dominio origen y que no ha sido modificado durante su recorrido.

Si la comprobación falla, entonces algo ha sucedido, y el servidor de destino podrá marcar el mensaje y entregarlo, descartarlo o tomar alguna otra acción.

Todas estas propuestas tienen algo en común**: Proporcionan un mecanismo para que el servidor de correo de origen se autentique, previniendo de esta manera que algún Spammer lo suplante.** De todas ellas, SPF parece ser la más extendida en la actualidad, con más de 8000 servidores de correo que declaran utilizarla, y contando con el apoyo de grandes corporaciones como AOL, Google, Earthlink, etc.

Sender ID y DomainKeys también tienen sus defensores. Una iniciativa interesante, desarrollada en el marco del grupo MARID del IETF, pretendía fusionar SPF y Sender ID en una única especificación. Lamentablemente, la insistencia de Microsoft en restringir el uso de la tecnología a base de patentes y licencias ha hecho que el IETF tome la decisión de desmantelar el grupo, por lo que el futuro de la iniciativa queda totalmente en el aire.

8.3. Envío masivo

Como su propio nombre indica, **el envío masivo consiste en el uso de los servidores de correo de manera indiscriminada para el envío de una gran cantidad de correos electrónicos**. Esta vulnerabilidad, junto con las ya estudiadas, son las técnicas utilizadas por los Spammers para llevar a cabo sus propósitos.

En este caso, el problema no está tan relacionado con el protocolo de envío (SMTP) sino con la **política de uso de un servidor de correo electrónico**.

Limitación del número de envíos

Se puede limitar el número de mensajes que pueden salir desde un servidor de correo como mecanismo para evitar la realización de envíos masivos. Para ello **se escoge un límite que sea lo suficientemente alto como para no perturbar a los usuarios que estén realizando un uso legítimo del servicio, pero suficientemente bajo para que los Spammers no puedan realizar sus actividades.** Habitualmente, estos límites se ponen por minuto, hora o día.

Recientemente el proveedor Hotmail ha impuesto un límite de 100 mensajes salientes por día y por cuenta de correo. Este número se eligió porque, según sus datos históricos de utilización del servicio de correo electrónico, el 99% de sus casi 110 millones de usuarios en todo el mundo no llegan a alcanzar la cifra de 100 envíos diarios.

El **mecanismo de limitación de tasa** resulta muy atractivo para los PSIs, ya que la mayor parte de los servidores de correo actuales pueden ser configurados para ponerlo en funcionamiento. Además, el coste extra en el que incurre el proveedor es bajo.

La parte negativa de esta medida es que **puede impedir que usuarios normales, que ocasionalmente necesiten realizar envíos por encima del umbral** (por ejemplo, enviando invitaciones a una fiesta), **puedan llevarlos a cabo.** Por otro lado, los Spammers pueden **"esquivar" este mecanismo** por el sencillo procedimiento de crear una gran cantidad de cuentas de correo con el mismo proveedor, y utilizar cada cuenta para enviar mensajes manteniéndose dentro de los límites. Sin embargo, la puesta en operación de la limitación de tasa es tan sencilla que no existen motivos de peso para no hacerlo, creando así una primera línea de defensa contra el Spam.

Virus y zombies que utilizan el puerto 25

Todos los mensajes de correo enviados sobre Internet se enrutan a través del puerto 25 del servidor de correo (puerto al que se conecta el cliente para solicitar el envío). Actualmente ya existen muchos PSIs que están **bloqueando dicho puerto** en sus servidores de correo para evitar los envíos masivos procedentes de zombies que han sido infectados en los dominios a los que dan servicio.

Según datos de Julio del 2004, se estima que un 40% del total de Spam se envía desde máquinas zombi.

Si el puerto 25 está bloqueado, entonces el originador de un mensaje de correo se ve forzado a enviarlo a través del servidor de correo de su propio PSI. De esta manera, los mensajes se ven sujetos a las diversas medidas de control de Spam que el PSI del originador tenga en funcionamiento (por ejemplo, la ya citada limitación de la tasa máxima de mensajes).

Otros PSI **están bloqueando el puerto 25 de manera selectiva**, por ejemplo sólo para direcciones que parecen enviar demasiados mensajes de correo.

Sin embargo, aunque es una medida muy efectiva, también es cierto que puede causar problemas a usuarios que necesitan hacer un uso legítimo de esta funcionalidad. Por ejemplo, los que necesitan mantener su propio servidor de correo o comunicarse con un servidor de correo en una red remota para enviar los mensajes (por ejemplo, compañías de web hosting).

Existe un puerto especifico, el 587 (ver RFC 2476), reservado para conversaciones SMTP autentificadas, que constituye la alternativa cuando el usuario quiere usar el servidor de correo de su dominio y su proveedor ha bloqueado el puerto 25 (siempre que su servidor de correo soporte esta funcionalidad).

Pago por envío

Una propuesta que cuenta con grandes defensores, ya que ha demostrado su eficacia ante problemas similares en el correo postal, es **introducir mecanismos de pago en el correo electrónico**, bien pagando por cada mensaje enviado o recurriendo a algún sistema de pago por suscripción mensual.

En teoría, el coste de enviar cada mensaje debería ser lo suficientemente bajo como para que un usuario medio se lo pueda permitir, pero lo suficientemente caro como para que a los Spammers les resulte inviable enviar millones de mensajes cada día.

Manteniendo la cifra de 100 mensajes diarios en media por cada usuario normal, si cada mensaje cuesta 0.1 céntimos de euro, el coste del servicio de correo sería de unos 36 euros al año. Sin embargo, el coste que debería afrontar un Spammer de los que envían un millón de mensajes diarios, sería de 1.000 euros al día, lo que haría que el negocio del Spam fuera bastante menos rentable.

No obstante, los detractores de la idea sostienen que la implantación de este tipo de mecanismos a nivel global es inviable, debido a la reticencia (o imposibilidad) de los usuarios corrientes a pagar por un servicio que hoy en día obtienen gratuitamente. Quizás por ese motivo, las diversas iniciativas desarrolladas en torno a mecanismos de pago están orientadas hacia un modelo de negocio empresarial[36].

La adopción de mecanismos de pago a nivel global parece inviable a corto plazo debido a:

- Reticencias de los usuarios (como ya se ha mencionado)
- Necesidad de estandarización y múltiples acuerdos internacionales, ya que la arquitectura de Internet es inherentemente cooperativa y requiere que todos los participantes estén de acuerdo.

[36] Ver el ejemplo de la compañía Goodmail Systems y su propuesta de "sellos electrónicos" en el apartado "6.4. Hacia dónde llevan las nuevas medidas contra el Spam. Opinión de los grandes proveedores", del capítulo 6.

- Necesidad de establecer una compleja estructura de pagos y verificaciones, que sea lo suficientemente buena como para resistir los ataques que seguramente realizarán los Spammers.

- Existencia de varias soluciones propietarias en el mercado actualmente, por lo que los PSIs tienen un miedo lógico a "casarse" con una solución que no triunfe o que les tenga cautivos en el futuro.

Por este motivo, es necesario encontrar un modelo de negocio suficientemente bueno y que se implante con éxito en algún ámbito concreto antes de pensar en la adopción a nivel global.

Es importante remarcar el papel que pueden jugar en este proceso **los organismos de Correos y Telégrafos** que son los que deben buscar nuevas formas y valores en el correo electrónico como prolongación de su negocio tradicional. La ventaja de estos organismos es que disponen de una cultura de normalización, cuentan con reglas para cooperar en el ámbito internacional, no tienen intereses en los sectores relacionados con el medio electrónico (telecomunicaciones, proveedores de contenidos,...), tienen amplia experiencia en la normalización y, lo que es más importante, pueden añadir valor a una herramienta que va a marcar su futuro próximo.

CAPÍTULO 9. MARCO REGULADOR Y LEGAL DEL CORREO ELECTRÓNICO

En este capítulo se abordan las leyes que regulan el funcionamiento del correo electrónico. En concreto, se estudian aquéllas que tratan de impedir la práctica del Spam y las medidas que proponen para lograrlo. Una correcta legislación ayudaría a frenar el avance del Spam y podría convertirse en una eficaz herramienta de lucha contra éste.

Se estudia en este capítulo con mayor detalle el caso de la legislación española, para después pasar a analizar la situación en la Unión Europea y Estados Unidos.

9.1. En España

El marco regulador y legal que se puede aplicar al correo electrónico en España esta recogido en:

- **LSSI**: Ley 34/2002 de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico
- **LGT**: Ley 32/2003 de 4 noviembre General de Telecomunicaciones
- **Código Penal Español:** Ley-Orgánica 10/1995 de noviembre
- **Ley Orgánica de protección de datos de carácter personal,** 15/1999

En la LSSI se pueden encontrar los artículos 21 y 22 (modificados posteriormente por la LGT de 4 de noviembre del 2003) relacionados con el correo electrónico. En el artículo 21, punto uno, se expone la prohibición expresa de realizar comunicaciones comerciales a través de correo electrónico o medios de comunicación equivalentes sin la autorización expresa de los destinatarios de las mismas.

La LGT añade un punto 2 a este artículo para adecuarse a la Directiva 2002/58/CE, en donde se flexibilizan los requisitos para correos enviados por empresas, restringiendo el primer punto a la no existencia de una relación contractual previa lo cual, según algunos juristas, contradice a lo dispuesto en la LSSI. En el artículo 22 se especifica la obligación de las empresas a poner a disposición del usuario una forma fácil y gratuita de darse de baja en la recepción de correos comerciales. Además éstas han de informar a sus clientes de la utilización que se va a hacer de sus datos personales.

En el código penal, en el artículo 197, se contempla la privacidad y la intimidad del correo electrónico, por lo que teniendo en cuenta estas disposiciones la Ley Orgánica de protección de datos es aplicable por extensión al correo electrónico. Existen otros artículos en los que se contemplan una serie de delitos informáticos que, aunque no hacen referencia expresa al correo electrónico, citan que éste es la herramienta utilizada para infringir la ley. Algunos de estos artículos son el 248, estafas realizadas mediante manipulaciones informáticas, o el 256, en el que se penaliza la utilización de equipos de telecomunicación (servidores de correo por ejemplo) sin la autorización de su propietario.

La Agencia de Protección de Datos, responsable de investigar y perseguir los abusos

En España, el encargado del hacer que la LSSI se cumpla es la Agencia de Protección de Datos (APD o AEPD). Al considerarse la dirección de correo electrónico como un dato de carácter personal y privado, la APD vela por su seguridad y por el cumplimiento de la legislación correspondiente.

Una legislación adecuada es requisito imprescindible para que la prevención del Spam resulte efectiva. Sin embargo, ésta por si sola resulta claramente insuficiente y ha de ir acompañada de actividades eficaces de inspección y control.

La actuación de la Agencia se rige fundamentalmente por dos leyes:

- **Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD):** En su Título VI regula las funciones de la AEPD respecto de la protección de datos, define la figura del Director de la Agencia, marca el carácter del Registro General de Protección de Datos, etc.

- **Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI):** Atribuye a la AEPD competencias específicas en el marco de los ya mencionados artículos 21 y 22, respecto de las comunicaciones comerciales no solicitadas.

Funciones atribuidas a la AEPD

De acuerdo con el marco legal arriba mencionado, la AEPD tiene las siguientes funciones:

a) De carácter general:

Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.

b) En relación con los afectados:

- Atender sus peticiones y reclamaciones
- Informar de los derechos reconocidos en la Ley
- Promover campañas de difusión a través de los medios de comunicación

c) En relación con quiénes tratan datos:

- Emitir autorizaciones previstas en la Ley
- Requerir medidas de corrección
- Ordenar, en caso de ilegalidad, el cese en el tratamiento y la cancelación de los datos
- Ejercer la potestad sancionadora
- Recabar ayuda e información que precisen
- Autorizar las transferencias internacionales de datos

d) En la elaboración de normas:

- Informar acerca de los proyectos de normas de desarrollo de la LOPD.
- Informar acerca de los proyectos de normas que incidan en materias de protección de datos.
- Dictar instrucciones y recomendaciones de adecuación de los tratamientos a la LOPD.
- Dictar recomendaciones en materia de seguridad y control de acceso a los ficheros.

e) En materia de telecomunicaciones:

Tutelar los derechos y garantías de los abonados y usuarios en el ámbito de las comunicaciones electrónicas, incluyendo el envío de comunicaciones comerciales no solicitadas realizadas a través de correo electrónico o medios de comunicación electrónica equivalente.

f) Otras funciones:

- Velar por la publicidad en los tratamientos, publicando anualmente una lista de los mismos
- Cooperación internacional
- Representación de España en los foros internacionales en la materia
- Control y observancia de lo dispuesto en la Ley reguladora de la Función Estadística Pública
- Elaboración de una memoria anual, presentada por conducto del Ministro de Justicia a las Cortes

De esta manera, **la AEPD tiene competencias en el ámbito específico del Spam con contenido comercial**, tanto para investigar las denuncias recibidas como para sancionar las posibles infracciones que se encuentren tras el oportuno procedimiento de investigación. La AEPD puede sancionar directamente a Spammers situados en territorio nacional o a aquéllos que, estando localizados dentro de la Unión Europea, afecten con sus actividades a usuarios en España.

El número de denuncias que recibe la APD hasta la fecha es relativamente bajo (menos de 200 el año 2003) lo cual contrasta con el elevado volumen de Spam. El número de casos resueltos también es muy bajo, debido a la dificultad de identificar al responsable y aplicar la legislación española más allá de nuestras fronteras.

El **procedimiento de investigación** que sigue la AEPD frente a una denuncia por Spam es el mismo que en un caso referente a la protección de datos. Una vez recibida la denuncia por parte del afectado, los inspectores inician las oportunas actuaciones encaminadas a esclarecer la situación, que en el caso del Spam, normalmente implican:

- Inspección de las cabeceras SMTP de los mensajes de correo recibidos, para intentar determinar su procedencia. Investigación del dominio origen mediante servicios del tipo whois (http://www.whois.net).
- Una vez averiguado el origen, puede realizarse una petición de información al emisor de los correos, presunto Spammer, para que acredite por ejemplo, el método por el que ha obtenido las direcciones de correo, si dispone del consentimiento expreso de los destinatarios para enviarles los correos, etc.
- En paralelo, los propios inspectores tienen competencia para realizar inspecciones "in-situ", tanto en la sede del presunto Spammer, como en la sede del PSI que le proporciona los servicios de conectividad.

Si una vez finalizado el procedimiento de investigación, se determina que ha existido infracción, se dictará la oportuna sanción administrativa mediante resolución del Director de la AEPD. La sanción vendrá determinada por la LOPD o LSSI, dependiendo del tipo específico de infracción que se haya producido.

Tipo de sanciones que impone la AEPD:

Las sanciones que puede imponer la AEPD dependen del tipo de abuso:

- **Spam de contenido comercial:** Caen dentro de lo que la ley denomina "comunicaciones comerciales no solicitadas", pudiendo ser sancionadas en base a los artículos 21 y 22 de la LSSI. Las sanciones máximas son de 30.000 € para infracciones de carácter leve y de 150.000 € para infracciones graves.

- **Phishing:** Contra estos correos se puede actuar de dos maneras. Por un lado, según la LOPD, pueden constituir una infracción grave ("*recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas*", o bien "*Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley o con incumplimiento de los preceptos de protección*") o incluso muy grave ("*recogida de datos en forma engañosa y fraudulenta*"). En el primer caso, las sanciones oscilarán entre 60.001 y 300.000€. En el segundo, entre 300.001 y 600.000 €.

  Otra posible vía de actuación es la vía civil o penal, que cae fuera de las competencias de la AEPD. Cuando durante el proceso de investigación se encuentren indicios de delito, lo que en el caso del phishing es bastante plausible dada la naturaleza fraudulenta del mismo, la Agencia dará cuenta de los hechos inmediatamente a la Brigada de Investigación Tecnológica de la Policía Nacional (www.mir.es/policia/bit), al Grupo de Delitos Telemáticos de la Guardia Civil (http://www.guardiacivil.org/telematicos/victima00.htm) o a la Fiscalía del Estado para que sean ellos los que se encarguen del asunto.

- **Otro tipo de correos no deseados:** Aquí se podrían encuadrar correos utilizados para la distribución de virus, troyanos y demás "*malware*". Contra este tipo de correos no cabe actuación directa de la AEPD. Sin embargo, existen dos posibilidades indirectas de actuación: por un lado, se puede actuar como en el caso anterior y dar cuenta de la situación a la Policía Nacional o Guardia Civil. Por otro, es posible sancionar los efectos que el correo malicioso pueda producir y que caigan dentro del ámbito de la LSSI o LOPD. Una situación que caería dentro de este ámbito es la recepción de un correo no solicitado que contiene un troyano, y que, al ser leído, instala de manera maliciosa dicho troyano en el ordenador del usuario, quedando este convertido en máquina zombie, que luego será utilizada por el Spammer para realizar los envíos masivos de correos. Aquí sí sería posible seguir el procedimiento antes mencionado para imponer la sanción al Spammer que originó el correo malicioso.

Barreras que disminuyen la eficacia en la persecución legal del Spam:

A pesar de los mecanismos presentados en secciones anteriores, en la práctica la persecución del Spam se ve dificultada por una serie de barreras.

Por un lado, el artículo 12 de la LSSI, referente al deber de retención de datos de tráfico relativos a las comunicaciones electrónicas, dice lo siguiente:

"*Los operadores de redes y servicios de comunicaciones electrónicas, los proveedores de acceso a redes de telecomunicaciones y los prestadores de servicios de alojamiento de datos deberán retener los datos de conexión y tráfico generados por las comunicaciones establecidas durante la prestación de un servicio de la sociedad de la información por un período máximo de doce meses, en los términos establecidos en este artículo y en su normativa de desarrollo*".

Teniendo en cuenta la inexistencia del correspondiente desarrollo reglamentario, (a fecha de noviembre de 2004), la situación real es que no existe obligación de guardar los datos de tráfico, así que muchos PSI no lo hacen o los almacenan durante un periodo de tiempo muy corto (un día).

Este hecho dificulta enormemente el seguimiento de los casos de Spam. Cuando se recibe una denuncia o notificación de un ciudadano por este motivo, es perfectamente posible que los datos sobre los correos que han dado origen a la denuncia (servidor de correo origen, fecha en la que han pasado por el PSI, etc.) ya hayan desaparecido de los servidores del PSI, así que aunque la AEPD investigue con la máxima celeridad, se verá en grandes dificultades para probar lo sucedido.

Por otro lado, otro problema que también se da es que, en la actualidad, las sanciones que se están imponiendo a los Spammers tienen un importe muy inferior al máximo que prevé la legislación (típicamente 3.000 €). El efecto disuasorio que tienen las sanciones se ve así muy mermado, ya que el Spammer paga sin rechistar y continúa con su lucrativa actividad (que obviamente le está proporcionando unos beneficios muy superiores al importe de la sanción).

También hay que considerar que el carácter del Spam en sí es otra barrera que dificulta las labores de inspección y control. El Spam procedente del extranjero suele hacer uso de mecanismos de ocultación de identidad, como la falsificación de cabeceras SMTP, lo que complica enormemente su seguimiento. Y no digamos ya si su origen está en un país como China, Argentina o Nigeria, con una legislación y problemática completamente distintas a la de la UE: huelga decir que en estos casos el Spammer escapa a todo castigo y sigue tranquilamente con su actividad.

En el caso específico del phishing, es prácticamente imposible seguir la pista del originador. Según datos de la OCDE, en Junio de 2004 el tiempo de vida medio de una Web de phishing era de 2.25 días. De esta manera, incluso si la denuncia se hace el mismo día en el que se recibe el correo fraudulento, se dispone de una ventana muy corta en la que comprobar la web en la que el delincuente informático recoge las claves de los usuarios.

Extractos de la legislación española aplicable al correo electrónico

Artículo 197. (Código Penal):

1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

Artículo 248. (Código Penal):

1. Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.

2. También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero, apropiado exceda de cincuenta mil pesetas. Si se tratara de cosas de valor artístico, histórico, cultural o científico, la pena será de prisión de seis meses a dos años.

Artículo 256. (Código Penal):

El que hiciere uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular, ocasionando a éste un perjuicio superior a cincuenta mil pesetas, será castigado con la pena de multa de tres a doce meses.

Artículo 21. Prohibición de comunicaciones comerciales realizadas a través de correo electrónico o medios de comunicación electrónica equivalentes. (Modificación de la LSSI en la LGT de 4 de noviembre de 2003):

1. Queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas.

2. Lo dispuesto en el apartado anterior no será de aplicación cuando exista una relación contractual previa, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente.

En todo caso, el prestador deberá ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo y gratuito, tanto en el momento de recogida de los datos como en cada una de las comunicaciones comerciales que le dirija.

Artículo 22. Derechos de los destinatarios de servicios. (Modificación de la LSSI en la LGT de 4 de noviembre de 2003):

1. El destinatario podrá revocar en cualquier momento el consentimiento prestado a la recepción de comunicaciones comerciales con la simple notificación de su voluntad al remitente. A tal efecto, los prestadores de servicios deberán habilitar procedimientos sencillos y gratuitos para que los destinatarios de servicios puedan revocar el consentimiento que hubieran prestado. Asimismo, deberán facilitar información accesible por medios electrónicos sobre dichos procedimientos.

2. Cuando los prestadores de servicios empleen dispositivos de almacenamiento y recuperación de datos en equipos terminales, informarán a los destinatarios de manera clara y completa sobre su utilización y finalidad, ofreciéndoles la posibilidad de rechazar el tratamiento de los datos mediante un procedimiento sencillo y gratuito. Lo anterior no impedirá el posible almacenamiento o acceso a datos con el fin de efectuar o facilitar técnicamente la transmisión de una comunicación por una red de comunicaciones electrónicas o, en la medida que resulte estrictamente necesario, para la prestación de un servicio de la sociedad de la información expresamente solicitado por el destinatario.

9.2. En Europa

Actualmente, existen dos normas fundamentales que establecen el marco legislativo europeo con respecto al Spam:

- **Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de Junio de 2.000**, relativa a ciertos aspectos legales de los servicios de la Sociedad de la Información, en especial al comercio electrónico, en el mercado europeo ("Directiva sobre el comercio electrónico").
- **Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2.002,** relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas ("Directiva sobre la intimidad y las comunicaciones electrónicas").

El ámbito de estas normas con respecto a las comunicaciones electrónicas compete exclusivamente a las comunicaciones comerciales no solicitadas, realizadas con propósitos de marketing directo, a través del correo electrónico y demás medios equivalentes. De esta manera, se establecen tres reglas fundamentales:

- **El envío de mensajes electrónicos con fines comerciales se supedita al consentimiento previo de los abonados (opt-in).** Se prevé una excepción limitada para los mensajes de correo electrónico (o SMS) enviados por una empresa a clientes existentes y referidos a servicios o productos similares. Este régimen se aplica a los abonados que sean personas físicas, pero los Estados miembros pueden hacerlo extensivo a las personas jurídicas.

- Es **ilícito disimular u ocultar la identidad del remitente** por cuenta de quien se efectúa la comunicación.

- Todos los mensajes electrónicos deben mencionar una **dirección de respuesta válida donde el usuario pueda pedir que no se le envíen más mensajes**.

Como podemos concluir, no quedan prohibidos todos los mensajes electrónicos comerciales no solicitados.

Está prevista una excepción a esta norma cuando los datos electrónicos para el envío de correo electrónico o SMS/MMS se hayan obtenido en el marco de una relación contractual previa ("consentimiento previo suave"). En el marco de la relación proveedor-cliente ya existente, la empresa que obtuvo los datos de un cliente puede utilizarlos con fines de comercialización de productos o servicios similares a los que ya le vendió.

Esta excepción ha sido armonizada a escala comunitaria, y los estados miembros no tienen más remedio que aplicarla. No obstante, debe formularse de manera estricta para no comprometer el funcionamiento del régimen de consentimiento previo: incluso en este caso, la empresa debe indicar claramente, desde el momento en que obtiene los datos por vez primera, que éstos pueden ser utilizados con fines de venta directa (y, si procede, que pueden transmitirse a terceros a tal efecto) y ofrecer al consumidor la posibilidad de oponerse mediante un procedimiento sencillo y gratuito.

En Europa, la regulación del correo electrónico y las comunicaciones comerciales se ha desarrollado principalmente tomando como referencia la Directiva 2002/58/CE, basada en la filosofía opt-in: **el envío de comunicaciones electrónicas comerciales requiere de una solicitud o consentimiento previo del destinatario.**

Otras directivas relacionadas con el Spam

Una práctica vinculada al Spam, comentada en anteriores capítulos, es la **recolección de direcciones de correo electrónico**. Es decir, la recogida automática de datos personales en lugares públicos de Internet. Esta práctica es ilícita en virtud de la **Directiva general sobre protección de datos 95/46/CE**, esté o no efectuada de manera automática con ayuda de un programa informático.

El **Spam fraudulento y engañoso** puede resultar especialmente desagradable. Estas prácticas son ya ilícitas en virtud de las normas existentes en la UE sobre publicidad engañosa y prácticas comerciales desleales (por ejemplo la **Directiva 84/450/CEE** sobre publicidad engañosa). Generalmente, las leyes nacionales prevén también sanciones más severas en los casos más graves, incluidas sanciones penales.

Como sabemos, a menudo se perpetran actividades como la piratería o la suplantación de la identidad para facilitar el Spam, con el fin de enviarlo o acceder a bases de datos de direcciones o a máquinas de usuario. Una gran parte de estas actividades estarán cubiertas por la **Decisión marco relativa a los ataques contra los sistemas de información, que prevé sanciones penales**. Esta Decisión marco, basada en una propuesta de la Comisión, fue objeto de un acuerdo político en febrero de 2003 y debería ser adoptada oficialmente en breve plazo.

En numerosos estados miembros constituye ya delito penal el acceso ilícito a un servidor o un ordenador personal, o su uso indebido.

9.3. En EE.UU. y otros países

Como ya hemos abordado en anteriores capítulos, existe otra filosofía denominada **opt-out**, adoptada principalmente por países asiáticos (Japón y Corea) y americanos (EE.UU, Canadá y México). En este caso no se requiere una solicitud previa por parte del destinatario para el envío de comunicaciones publicitarias electrónicas, sino que **aquella persona que no quiera recibir este tipo de correos deberá hacérselo saber al remitente.** En Europa hay dos países que se han decantado por este modelo: Portugal y Holanda.

La legislación sobre las comunicaciones publicitarias electrónicas no deseadas en Estados Unidos se denomina **CAN-SPAM** (Controlling the Assault of Non-Solicited Pornography and Marketing Act). Esta ley va dirigida contra los e-mails no solicitados pornográficos, los que ofertan todo tipo de remedios para mejorar la imagen física y los que dan recetas para hacerse millonario de golpe.

Los **principales puntos de la ley** se pueden resumir en:

- Los usuarios que no deseen recibir Spam se apuntarán en una lista para tal efecto.
- Se prohíbe a los propagadores de estos correos que se escondan detrás de identidades falsas o encabezamientos engañosos.
- Los mensajes deben indicar su contenido con abreviaturas en el asunto del correo para que se puedan filtrar con facilidad.
- Se permite a los ESPs (no a los usuarios) establecer acciones legales contra los Spammers
- Se prohíbe recabar direcciones desde sitios web o "*adivinar*" direcciones mediante combinaciones de nombres conocidos y dominios de uso generalizado.
- El mensaje deberá incluir una dirección física de respuesta localizada en Estados Unidos.

En su votación, la Cámara de Representantes aprobó por unanimidad la legislación, en la que el Senado introdujo pequeñas modificaciones, sin alterar el espíritu de una ley que había sido defendida por ambos partidos, conocedores de su importancia electoral.

La legislación no proscribe por completo las ofertas comerciales a través del correo electrónico, sino que **obliga a las empresas a identificarse debidamente y a ofrecer a los consumidores la posibilidad de no volver a ser contactados.**

Los correos pornográficos deberán estar claramente etiquetados como tal y los mensajes de texto enviado a los teléfonos móviles estarán prohibidos, a menos que el consumidor los autorice.

Al ser una legislación federal, esta ley invalidará las iniciativas aprobadas previamente en 35 estados, algunas de las cuales, como en el caso de California, prohíben todo contacto no solicitado y da a los consumidores la posibilidad de querellarse directamente contra las empresas que envían "correos basura".

Como consecuencia de la aplicación de la ley CAN-SPAM, durante el primer semestre del 2.004 se han dictaminado diversas sentencias condenatorias y denuncias contra empresas que realizan Spam en EE.UU.

En Europa, en concreto en Francia, se ha obligado a un proveedor a cortarle el acceso a Internet a un usuario que practicaba el Spam, siendo éste sentenciado al pago de elevadas multas.

CAPÍTULO 10. INICIATIVAS DE COOPERACIÓN INTERNACIONAL

La cooperación internacional resulta fundamental en cualquiera de las líneas de lucha contra el Spam, ya que estamos ante un fenómeno de carácter global.

Se puede observar que en muchos países ni siquiera existe una responsabilidad definida de inspección y control, o si existe, está repartida entre diversos entes que muchas veces tampoco disponen de los medios idóneos para el adecuado desarrollo de sus funciones.

Tampoco se puede hablar de uniformidad entre las legislaciones anti-Spam de los diferentes países, especialmente fuera del ámbito comunitario y más aún si se trata de países subdesarrollados que no poseen ningún tipo de leyes en este sentido.

En el caso de la UE, también se observa que la autoridad encargada de hacer cumplir las disposiciones relativas a las comunicaciones comerciales no solicitadas, no es la misma en todos los Estados miembros. En la mayoría de los casos (como sucede en España) es la autoridad competente en materia de protección de datos (APD) la que asume la responsabilidad principal. En algunos países, no obstante, esta misión la cumple la autoridad nacional de reglamentación de las comunicaciones electrónicas (ANR). Y en otros, incumbe principalmente a las autoridades responsables de la protección de los consumidores (incluido el defensor del pueblo).

A menudo habrá que contar con más de una autoridad en la ejecución de las disposiciones relativas a las comunicaciones no solicitadas, lo que complica aún más las tareas de inspección y control.

De esta manera, no es fácil llegar a acuerdos de colaboración eficaces entre diversos países, ya que siempre serán acuerdos "de mínimos", es decir, se tendrán que fundamentar en los aspectos comunes entre las legislaciones de los países participantes, sin que en ningún caso puedan ir contra lo dictado en ellas.

Así, por ejemplo, en el caso del MoU (Memorandum Of Understanding) entre España y Estados Unidos las cláusulas del acuerdo deberán desarrollarse sobre la base de que la legislación vigente en EE.UU. es del tipo "opt-out", por lo que determinadas prácticas que son ilegales en España, resultan allí completamente lícitas.

En la actualidad, existen diversos foros en los que gobiernos de todo el mundo colaboran entre ellos y con el sector privado para desarrollar iniciativas que resulten eficaces contra el Spam. En este capítulo se aborda el **análisis de algunos de estos foros e iniciativas**.

10.1. Actividades contra el Spam en la OCDE

La **OCDE** es una organización de cooperación intergubernamental cuyos objetivos son fomentar el buen gobierno y la economía de mercado. Esta organización viene realizando diversas actividades para intentar reducir el problema del Spam y, recientemente, ha creado un grupo de trabajo exclusivamente dedicado al problema. Dicho grupo se denomina **OECD Task Force on Spam**.

Durante el año 2004, la OCDE ha organizado, en Febrero y Septiembre, sendas **reuniones dedicadas totalmente al Spam**. A estas reuniones han asistido representantes de autoridades nacionales de reglamentación, de organismos de inspección y control y del sector privado, de un gran número de países de todo el mundo. Como resultado de estas reuniones, la OCDE ha decidido afrontar el problema del Spam desarrollando un toolkit o conjunto de herramientas y manuales que faciliten la lucha. Esta "caja de herramientas" anti-Spam de la OCDE consta de los siguientes elementos:

- **Un manual de regulación**, que debe contener datos sobre los enfoques que han tomado los diversos gobiernos a la hora de desarrollar sus leyes relativas al Spam. Esto permitirá a los líderes políticos tomar decisiones informadas al crear sus propias legislaciones o acordar la revisión de los marcos regulatorios.

- **Una panorámica de todas las iniciativas (formales e informales) de cooperación internacional en materia de lucha anti-Spam**, que ayude a identificar las posibles lagunas o redundancias, susceptibles de encontrarse entre las actividades que se realizan en el marco de esas iniciativas, y permita tomar acciones correctivas.

- **Un examen detallado de las iniciativas autorregulatorias de la industria**, tanto dentro de los diferentes estados como a nivel internacional.

- **Un análisis de las medidas técnicas, existentes y emergentes, en contra del Spam** (como puede ser la autenticación) **y de sus posibles impactos en la sociedad**.

- **Un compendio de materiales de formación y concienciación**, tanto en relación con el Spam en general, como en temas específicos como puede ser el phishing.

A fecha de noviembre de 2004, este conjunto de herramientas está en desarrollo. La OCDE ha solicitado no sólo la cooperación de los gobiernos de los estados miembros, sino también la de otros gobiernos, asociaciones empresariales y organismos de la sociedad civil.

10.2. Actividades en el ámbito de la ITU

Actualmente la ITU está llevando a cabo un congreso mundial para tratar el desarrollo de la Sociedad de la Información. Este congreso, denominado **World Summit on the Information Society (WSIS)** se compone de dos fases:

- La **primera fase** tuvo lugar en Ginebra, del 10 al 12 de Diciembre de 2003. En ella se trato una amplia gama de temas relativos a la Sociedad de la Información. Como conclusión de esta fase, se adoptaron una **declaración de principios** y un **plan de acción**.

- La **segunda fase** se debe realizar en Túnez, del 16 al 18 de noviembre de 2005.

Como parte del plan de acción obtenido de la primera fase del WSIS, se organizó una **reunión temática contra el Spam**, también en Ginebra, en julio de 2004. En dicha reunión participaron unas 200 personas, representando a diversas autoridades nacionales de reglamentación, organizaciones gubernamentales, asociaciones de consumidores, representantes de PSIs, miembros de la comunidad universitaria, asociaciones civiles, organizaciones empresariales, etc. **El objetivo de la reunión era doble**:

- Por un lado, concienciar a los participantes acerca del problema que supone el Spam e informarles acerca de las diversas iniciativas que se están desarrollando en todo el mundo para contrarrestarlo.

- Por otro, se pretendía crear un marco de cooperación anti-Spam con un alcance más amplio que otras iniciativas similares que se venían desarrollando anteriormente o en paralelo.

En el periodo que resta hasta noviembre de 2005, la ITU seguirá realizando actividades anti-Spam.

10.3. El papel de la Unión Europea

Las diversas instituciones de la UE son muy conscientes del problema que supone el Spam en la actualidad [10]. Una de las iniciativas que ha tomado la Comisión Europea es la **creación de un grupo de trabajo sobre las comunicaciones electrónicas no solicitadas**. Este grupo está compuesto por las autoridades nacionales de reglamentación y las autoridades responsables de inspección y control de los estados miembros, y se denomina **Contact Network of Spam Authorities (CNSA)**.

El **objetivo principal** de este grupo es desarrollar métodos de colaboración entre los estados miembros, que permitan el intercambio de información sobre denuncias relativas al Spam entre las autoridades competentes. Para ello, se ha elaborado una lista, que contiene las personas de contacto en cada país, y se está desarrollando un Procedimiento de Colaboración intra-europeo. Dicho procedimiento no será un documento vinculante legalmente, sino que debe verse como una declaración de intenciones de los participantes, para ser más proactivos en el seguimiento de las denuncias contra el Spam en el entorno de la UE.

10.4. El Plan de Acción de Londres

El **Plan de Acción de Londres para la Cooperación Internacional contra el Spam** es una declaración de intenciones en la que participan organismos de inspección y control, autoridades nacionales de reglamentación y representantes del sector privado de diversos países de todo el mundo. Se empezó a gestar en una reunión que tuvo lugar en Londres, el 11 de octubre de 2004, organizada por la FTC y la OFT (Office of Fair Trading) británica, y sigue en desarrollo a fecha de noviembre de 2004.

El plan de acción pretende **promover la cooperación internacional en todas las actividades que forman parte del enforcement** (actividades de inspección y control, iniciativas de autorregulación, de concienciación de la ciudadanía, etc.), así como **afrontar otros problemas derivados y relacionados con el Spam**, como el fraude, phishing y la distribución de virus, gusanos, etc.

Los miembros iniciales del plan han acordado abrir la participación en el mismo a cualquier otra entidad gubernamental o representante relevante del sector privado que tenga interés en hacerlo, con el razonamiento de que el éxito del plan será tanto más fácil cuanto mayor sea la red de participantes en él.

Una de las tareas que se debe desarrollar necesariamente es el estudio de cómo encaja el Plan en otras iniciativas, como las actividades de la OCDE y del grupo CNSA de la Comisión Europea. La OCDE y la Comisión ya han empezado a realizar este estudio. La versión definitiva y firmada del plan debería hacerse pública a corto plazo.

Los MoUs de colaboración entre países

Un MoU (Memorandum Of Understanding) es un **acuerdo de entendimiento entre dos o más países que desean colaborar en algún tema específico**.

En el marco de la lucha contra el Spam, en la actualidad existen diversos acuerdos de este estilo, ya firmados o todavía en desarrollo, para colaborar en actividades de reglamentación o de inspección y control. Como casos más relevantes, podemos citar el MoU trilateral entre EE.UU, Australia y el Reino Unido, el MoU entre Australia y Corea, y el que se está gestando entre la AEPD española y la FTC estadounidense para cooperar en la inspección y el control.

10.5. Participación de la AEPD en foros internacionales anti-Spam

La Agencia participa en diversas **iniciativas internacionales de cooperación en la lucha contra el Spam**:

- **Grupo CNSA** (Contact Network of Spam Authorities) de la Comisión Europea.
- **Plan de Acción de Londres** para la Cooperación Internacional contra el Spam.

Otra actividad de cooperación que conviene destacar es el desarrollo de un **MoU** (Memorandum of Understanding o Acuerdo de Entendimiento) entre las autoridades de inspección y control de España (AEPD) y Estados Unidos (FTC, Federal Trade Commission). El acuerdo, que aún no está cerrado, permitirá reforzar la cooperación entre ambos países en la persecución del Spam.

10.6. Otros foros internacionales

Aparte de los mencionados, existen diversos **foros internacionales** en los que los sectores público y privado de diferentes países realizan actividades de cooperación contra el Spam. Entre ellos están:

- **ASEM** (Reunión Asia-Europa)
- **APEC** (Cooperación Económica Asia Pacífico),
- **UNCTAD** (Conferencia de las Naciones Unidas para el Comercio y Desarrollo)
- **ICPEN** (Red Internacional de Protección del Consumidor)

Problemática de los países en vías de desarrollo

Dada la naturaleza global del problema del Spam, el **objetivo** perseguido en cualquier iniciativa de cooperación, como las presentadas en la sección anterior, es **lograr la participación efectiva del mayor número posible de países**. El motivo subyacente es reducir todo lo posible el número de "paraísos del Spam", es decir, aquéllos países que facilitan las actividades de los Spammers. Un conjunto de países que actualmente se puede considerar dentro de esta categoría es el de los países subdesarrollados y en vías de desarrollo, que se van incorporando paulatinamente a Internet de manera activa, pero que, por sus especiales características, tienen problemas mucho más serios que afrontar que el de servir de refugio a los Spammers.

En cualquier caso, algunos de estos países, Kenia, Sudán, Tanzania y Zambia, han manifestado recientemente, en el marco del ITU WSIS, ser conscientes del problema. Su declaración de principios afirma:

"Nosotros, como naciones en desarrollo, queremos manifestar públicamente que estamos totalmente de acuerdo con el hecho de que el Spam constituye un problema global que debe resolverse mediante la cooperación de todos los países. El Spam causa problemas sociales y morales en nuestros países, ya que, en ciertos casos, puede llevar a la comisión de delitos. Igualmente, causa la Denegación de Servicio en nuestras redes y pone en peligro el desarrollo del sector"

Además, solicitan que se les tenga en cuenta a la hora de desarrollar medidas internacionales, ya que no se quieren ver en la situación de tener que poner en práctica medidas para las que no están tecnológica y económicamente preparados.

CAPÍTULO 11. INICIATIVAS DE ÁMBITO NACIONAL

En lo que respecta a la lucha contra el Spam, tan importantes son las iniciativas puestas en marcha para combatirlo, como aquellas destinadas a lograr que los usuarios del correo electrónico tomen conciencia de su peligro, conozcan las herramientas de que disponen para combatirlo y sean conscientes de los diferentes mecanismos de denuncia existentes.

Este capítulo profundiza sobre estos aspectos, particularizando a la situación de España.

11.1. La iniciativa Confianza Online

Confianza Online es un **sistema de autorregulación para el comercio electrónico y la publicidad interactiva en el entorno de España**. Surge de la fusión de dos sistemas de autorregulación para Internet que ya existían previamente: El Código de Protección de Datos Personales en Internet de la AECE (1998) y el Código Ético de Publicidad en Internet de AUTOCONTROL (1999).

Ambos sistemas contaban también con sus respectivos mecanismos de aplicación de tales normas éticas en caso de controversia y en su día fueron sistemas de autorregulación pioneros, en un momento en el que aún no existían normas legales específicas en la materia.

A este proyecto de autorregulación para la publicidad y el comercio electrónico se han adherido también un grupo de asociaciones relevantes en los sectores de las comunicaciones comerciales y los nuevos medios electrónicos de comunicación a distancia, tales como la Asociación Española de Anunciantes (AEA), la Asociación Española de Agencias de Publicidad (AEAP), la Asociación de Centrales de Medios (ACM), la Asociación de Medios Publicitarios (AMPE), la Federación española de Comercio Electrónico y Marketing Directo (FECEMD), la Federación Nacional de Empresas de Publicidad (FNEP), la Asociación de Agencias de Marketing Directo e Interactivo (AGEMDI) y la Asociación Multisectorial de Empresas Españolas de Electrónica y Comunicaciones (ASIMELEC).

Sin olvidar la atención que se presta a la **protección de datos personales** en el desarrollo de ambas actividades, **el código está dividido en dos grandes áreas**:

- El área concerniente a las **comunicaciones comerciales** recoge las "normas sobre publicidad interactiva" reelaboradas por IAB Spain a partir del primitivo "Código sobre Publicidad en Internet" de AUTOCONTROL. De ese modo, pasan a integrarse en este cuerpo de normas éticas de vocación más amplia y cuya aplicación IAB Spain encomienda al Jurado de AUTOCONTROL.

- El área dedicada al **comercio electrónico**, fundamentalmente elaborada por AECE y movida por una clara vocación de permanencia, ha tratado de evitar normas excesivamente casuísticas, estableciendo principios y reglas de conducta generales. Dichas reglas resultan exigibles a los operadores en sus transacciones con los consumidores para la contratación de bienes y/o servicios a través de medios electrónicos de comunicación a distancia, con el fin de dar adecuada respuesta a la necesidad de mantener altos niveles de protección de sus derechos e intereses.

Las reglas contenidas en el Código han sido sometidas a la consulta de la AEPD, de la Dirección General para el desarrollo de la Sociedad de la Información y del Instituto Nacional de Consumo.

11.2. Acciones de concienciación y formación de los usuarios del correo electrónico

En muchos casos, los usuarios:

- Carecen de los conocimientos necesarios para saber cómo actuar ante los envíos de Spam.
- No son conscientes de las herramientas que les pueden ayudar a minimizar el problema.
- Desconocen los mecanismos de denuncia que tienen a su disposición.

Un problema relacionado y de importancia creciente es la realización de fraudes mediante el ***phishing***. En estos casos, la ignorancia del usuario no solamente le conduce a soportar las molestias asociadas a recibir un gran número de mensajes no deseados, sino que puede tener efectos catastróficos para su bolsillo.

Organismos y entidades de todo el mundo son conscientes del problema, por lo que vienen desarrollando, de manera cada vez más amplia, **campañas de concienciación** enfocadas a los usuarios finales, pero también a los responsables de sistemas y otros usuarios avanzados del correo electrónico que ya deberían conocerlo. Entre otras citamos las siguientes:

- **La Asociación Española de Usuarios de Internet (AUI)**, desarrolló en el año 2002 la campaña "**Rompe las cadenas: lucha contra el Spam**". En el 2003 puso en marcha la iniciativa **Pepi II** en colaboración con empresas e instituciones, con el objetivo de mejorar la calidad del correo electrónico. En el ámbito de ese proyecto, en el que se han involucrado los diferentes agentes que forman parte de la cadena del correo, se han desarrollado **herramientas** y **manuales** orientados a distintos tipos de agentes: Usuarios, creadores de contenidos, *webmasters*… Es, además, uno de los sitios con más información y más activos en la lucha contra el Spam en nuestro país. La información completa del proyecto puede obtenerse en:

  http://www.pepi-ii.com

La AUI también viene recordando, en todos los foros en los que participa, la importancia de este problema y la necesidad de implicar a todos los agentes, especialmente a los responsables del desarrollo de la Sociedad de la Información en España.

- El **Centro de Alerta Temprana Antivirus** de *Red.es.* En la URL

  http://alerta-antivirus.red.es/utiles/ver.php?tema=U&articulo=11

  tiene una página de introducción al problema del Spam, con información sobre las capacidades de diversas herramientas para luchar contra él.

  En el mismo sitio tenemos también información divulgativa sobre el *phising* y el fraude financiero en general.

- ***Ebay* España** ofrece un tutorial sobre cómo detectar y qué hacer con los correos electrónicos falsificados en la siguiente URL:

  http://pages.es.ebay.com/education/spooftutorial

  Conviene recordar que esta organización ha sido víctima del *phishing* en el pasado, por lo que es muy consciente del problema. *Ebay* ofrece el mismo tutorial en diversas lenguas, en todos los países en los que presta servicio.

- **La Brigada de Delitos Informáticos de la Guardia Civil** tiene una página con consejos de seguridad generales, pero no parece haber nada específico acerca del Spam:

  http://www.guardiacivil.org/telematicos/consejos.htm

- El **Centro Anti-Spam de Yahoo** es de los más completos, ya que ofrece información básica, artículos y manuales de utilización de las herramientas que Yahoo pone a disposición de los usuarios de sus servicios de correos. La información puede consultarse en la siguiente dirección de Internet:

  http://espanol.antiSpam.yahoo.com

- El **PSI Ono** ofrece un curso básico sobre diversos temas de seguridad en Internet, que incluye una introducción al Spam y su problemática:

  http://www.ono.es/busqueda/?id=88637790&pid=r&mode=ALL&n=0&query=curso+seguridad

El fin último de éstas y otras iniciativas similares es, por un lado, **evitar que el usuario sea víctima de fraudes y daños en su máquina** y, por otro, **hacer que la tasa de respuesta a los envíos de Spam se reduzca todo lo posible**.

CAPÍTULO 12. POLÍTICAS DE USO DE REFERENCIA PARA LOS PROVEEDORES

Sin lugar a dudas, los agentes con mayor responsabilidad para evitar los abusos del correo electrónico son los proveedores de servicio de correo (Electronic Service Providers – ESPs), los proveedores de acceso y los proveedores de servicio de alojamiento de servidores.

Ellos pueden poner en marcha políticas que eviten los abusos, comunicarlas a sus clientes y establecer procedimientos técnicos y organizativos, que permitan actuar de forma eficaz cuando se descubra un problema.

12.1. Políticas para los servidores / servicios de correo

Envío de correo

- **Relays cerrados** para evitar el uso del servidor de correo por agentes externos a los dominios gestionados. Utilizar nuestro servidor desde fuera, para enviar correo hacia fuera de nuestro servidor (rechazo de correo desde direcciones externas a nuestro dominio y destinadas a direcciones externas a nuestro dominio) (RFC 2505).

- **Relays locales cerrados** si es posible, evitando así la suplantación de identidades. No permitir el envío a usuarios de nuestro servidor sin que hagan un proceso de autenticación previo.

- Establecer un **procedimiento de control y monitorización de flujo de envío de mensajes** de cada usuario (RFC 2505).

- **Registro (logs) de todas las transacciones SMTP realizadas** (RFC 2505).

- A la hora del envío de un correo comprobar que la parte local de la dirección (anterior a símbolo @) del remitente es correcta y está registrada en el dominio (durante la transacción SMTP en el comando **MAIL FROM**) (RFC 2505).

- Comprobar que el cuerpo de un mensaje que se va a enviar no lleva **cabeceras *Received*** previas introducidas por el usuario.

- Utilizar **protocolo SPF** durante la transacción SMTP.

- Utilizar SMTP con autenticación: **ESMTP** (RFC 2554).

- Rechazar cualquier conexión en la que el **HELO/EHLO** sea alguna de las IP's de la organización, alguno de los dominios propios gestionados o algún nombre de máquinas propias, y no se trate de usuarios autenticados o máquinas que no sean de la organización.

Recepción de correo

- Establecer una **política de control y monitorización de flujo de mensajes recibidos** por los usuarios del sistema.
- Rechazar mensajes de correo que provienen de servidores de correo con una **IP dinámica**.
- Comprobar el **dominio** de la procedencia del mensaje en la transacción SMTP.
  - Rechazar correo procedente de dominios inexistentes (no tienen resolución DNS).
  - Rechazar correos cuyo dominio exista y la IP del remitente no esté contemplada en el registro correspondiente.
  - Aceptar correos cuyo dominio exista y la IP del remitente esté contemplada en el registro correspondiente.
  - Establecer política de actuación si el dominio existe pero no tiene registros de comprobación de remitentes.
- Rechazar mensajes de error provenientes de otros servidores en los que la dirección de correo electrónico que figure en la **cabecera *From*** no exista.
- Rechazar mensajes de error dirigidos a más de un usuario.
- Rechazar correos en los que el identificador del mensaje (**Message-ID**) o la **fecha** no sean sintácticamente correctos.
- Definir y comunicar una política sobre el tratamiento de los **virus**.

Registro DNS

- Definir los **registros** que hay que almacenar en el servidor DNS correspondiente.

Gestión de cuentas / buzones

- Establecer un **periodo de caducidad** para las cuentas. En caso de que una cuenta no reciba o envíe correo en ese periodo de tiempo, se eliminará o inhabilitará.
- Establecer el **límite superior** para el número de envíos de mensajes de correos en un espacio temporal determinado.
- Definir y comunicar la **política de filtrado** utilizada.
- Establecer un **protocolo** vía web y vía e-mail para gestionar incidencias o quejas de los usuarios relacionadas con el servicio de correo.
- Comunicar todas estas cláusulas al usuario.

12.2. Políticas para los usuarios de correo

Los usuarios son responsables de todas las actividades realizadas con las cuentas de correo electrónico que su ISP les proporciona.

El usuario no podrá:

- Con el envío de correos, contravenir la legislación vigente en materia de comunicaciones electrónicas.
- Utilizar servidores de correo, propios o ajenos, para el envío masivo (límite definido en la política de los servidores) de mensajes de correo no solicitados por el destinatario.
- Hacer un uso no autorizado de un servidor de correo ajeno para enviar un correo propio. Aunque el mensaje en sí sea legítimo.
- Falsificar las cabeceras de los correos electrónicos.
- Suplantar la identidad de terceras personas.
- Ocultar la identidad del emisor del correo.
- Revender el servicio en su totalidad o en parte a terceros, sin previo acuerdo con la empresa proveedora del servicio/servidor.
- Revelar su cuenta y clave a terceros. Las cuentas son personales e intransferibles.

12.3. Políticas para los que alojan equipos servidores de correo

Deben poner a disposición de los clientes que alojen servidores de correo las políticas de uso correspondientes, así como el compromiso de éstos a cumplirlas y a trasladarlas a sus usuarios, con penalizaciones en caso de incumplimiento.

CAPÍTULO 13. CONCLUSIONES

Los abusos en el correo electrónico tienen dos objetivos principales: Conseguir un beneficio económico (marketing, ventas...) o crear problemas de seguridad (usurpación de maquinas, virus, denegación de servicio...).

Los que buscan beneficio económico a través del Spam recurren a él porque les resulta rentable (la mayor parte de los gastos recaen en el receptor del correo y no en el emisor). Por tanto las soluciones para evitarlo pueden ir en la línea de incrementar los costes del agente que envía. Para los segundos es necesario recurrir a soluciones de carácter tecnológico. Éstas pasan porque haya productos que se adapten a las necesidades que surjan y, también, porque los técnicos que deben implantarlas sepan cómo hacerlo.

Es importante remarcar que en la lucha contra el Spam es imprescindible avanzar de forma coordinada, primero a nivel nacional, y luego a nivel internacional, para conseguir una cierta eficiencia en las políticas, iniciativas y propuestas que se pongan en marcha en los diferentes países. Finalmente conviene señalar lo fundamental de una concienciación real de todos los agentes (gobiernos, industria, reguladores, proveedores y usuarios), de forma que se asuma la importancia y magnitud que tiene este asunto y se pongan medios y recursos para luchar contra estos abusos.

13.1. Actuaciones y propuestas

Se presentan a continuación un conjunto de acciones, propuestas a partir de las conclusiones de este informe y agrupadas en torno a la categoría a la que hacen referencia.

Educación y sensibilización

En la medida en que los usuarios sepan protegerse de los abusos, cada vez resultarán menos atractivos a los que quieren aprovecharse de ellos. En esta línea se proponen una serie de acciones orientadas a los usuarios finales, en las cuales deberían participar tanto las administraciones como la industria, los medios de comunicación y las organizaciones de usuarios y consumidores.

- Campañas de concienciación y sensibilización en colaboración con todo el sector
- Creación de espacios y sitios de información orientados a este asunto
- Desarrollo de herramientas que permitan aminorar los efectos del Spam y que simplifiquen la tramitación de quejas, el análisis, la investigación...

Soluciones tecnológicas

- Creación de un grupo técnico para analizar y debatir las soluciones tecnológicas, con espacios virtuales y reuniones físicas, que elabore recomendaciones y guías de implementación de las soluciones de autenticación en los productos existentes en el mercado.

- Elaboración de estudios que analicen el impacto y las posibilidades de incorporar mecanismos de firma electrónica en el uso del e-mail, tanto en el ámbito empresarial como en el personal.

- Cursos de formación para los responsables de administrar servidores y servicios relacionados con el e-mail, adaptados a los productos que se utilizan para dar servicio de correo electrónico.

- Puesta en marcha de servicios de valor añadido sobre el e-mail desde organizaciones tipo "*Correos*" que permitan experimentar sobre la base de poner un precio a estos servicios.

No olvidemos que la historia se repite, así el correo postal también sufrió el abuso del Spam ya que originalmente el que pagaba era el que recibía el mensaje. La solución al problema fue cambiar el sistema obligando a que el pago lo realice el que quiera enviar y creando organizaciones (servicios postales) que en cada país velan por la calidad y la normalización de los procedimientos.

- Crear un grupo de trabajo para estudiar y proponer cambios en el protocolo del correo SMTP que haga propuestas a través de los organismos internacionales (IETF, ITU…)

Autorregulación y regulación

- Puesta en marcha de un sistema que permita medir y conocer la evolución del uso y abusos del e-mail.

- Elaboración de políticas de referencia para que sean utilizadas por los creadores de contenidos (webmasters), administradores de listas y proveedores de servicios de correo electrónico ESPs.

- Creación de una comisión permanente de lucha contra el Spam que reúna a todos los agentes con carácter trimestral, cuyo objetivo sea validar las políticas de referencia y estudiar y proponer iniciativas de lucha contra el Spam.

- Definir claramente en los reglamentos de desarrollo de la LSSI las obligaciones que deben cumplir los proveedores de correo en cuanto a almacenamiento de datos de conexión, actividad, etc., estableciendo claramente el tipo de datos, el plazo de almacenamiento y las obligaciones que tienen con respecto a las tareas de investigación y control de las autoridades.

- Creación de procedimientos muy simples para la denuncia del Spam con canales de comunicación separados para los usuarios y los proveedores de servicios de correo electrónico. Planteando incluso el desarrollo de programas para los usuarios finales, que se instalen en sus aplicaciones de lectura del correo (Outlook, Navegadores, Eudora...) y que permitan comunicar automáticamente todo aquello que éstos clasifiquen como Spam.

Coordinación internacional

- Crear, desde una organización gubernamental o colegial, una interfaz única que realice las funciones de secretaría técnica, en el ámbito español, con los grupos de trabajo e iniciativas de carácter internacional: OCDE, ITU, IETF, ICANN, UE.

  Esta secretaría técnica debería participar en todas las mesas e iniciativas que se pongan en marcha en el ámbito español. Asimismo debiera disponer de recursos humanos y materiales para realizar su trabajo, en especial la asistencia a todo tipo de foros y reuniones que, sobre este tema, se realicen en cualquier lugar del mundo.

- Crear un grupo de investigación con las universidades, para estudiar y proponer cambios en el protocolo del correo electrónico a través de los organismos internacionales.

13.2. Tendencias

No podemos ignorar que hay aplicaciones de la Sociedad de la información como la telefonía móvil, la mensajería instantánea o la voz sobre IP que pueden ser susceptibles de abusos similares al Spam.

Es sabido que la historia se repite, así que aprendamos del pasado para prevenir el futuro. Las aplicaciones de tipo Voz sobre IP en sistemas de tarifas planas pueden convertir a nuestro teléfono o nuestro buzón de voz, en un nuevo receptor de comunicaciones no solicitadas. Lo mismo nos puede suceder con otras aplicaciones que permitan envíos masivos con un nivel de costes muy bajo para el que los realiza.

CÓMO PREVENIR LOS ABUSOS EN EL CORREO ELECTRÓNICO: GUÍA DE USO PROFESIONAL PARA INGENIEROS DE TELECOMUNICACIÓN

Este capítulo es una recopilación de los consejos prácticos citados a lo largo de este informe. Su objetivo es que los Ingenieros de Telecomunicación puedan prevenir y contribuir a evitar los abusos en el Correo Electrónico desde tres ópticas diferentes: Como usuarios, como generadores de contenidos y, finalmente, como administradores de ordenadores y sistemas relacionados con el envío o recepción de e-mails.

Consejos para usuarios

Evita hacer pública tu dirección de correo:

Además de las páginas Web, esto es extensible a las listas de distribución, salas de chats, sitios Web, artículos, contribuciones o trabajos que envías etc. Quizá puedas abandonar estas listas pero en algunos casos es posible que tu dirección de correo electrónico siga accesible...y los Spammers puedan utilizarla. Si tienes que publicar tu dirección de correo utiliza alguno de estos trucos:

Si tienes que publicar tu dirección evita que pueda entrar en listas de Spam:

Para ello no publiques la dirección exacta, cambia algo que permita la lectura de la misma pero que no sea utilizable por los que las capturan masivamente.

Para publicar el correo nombre@sitio.es puedes utilizar estos seudónimos:

{nombre}@{sitio.es}, nombreARROBAsitio.es, …

Lee y entiende la política de privacidad cuando suministres tu dirección de e-mail en un sitio web:

Mirar si existe una política de privacidad clara y si permite a la compañía ceder a terceras partes tu correo, si tienen una dirección o una forma de contacto y en qué legislación se amparan. Si no encuentras la Política de Privacidad, te parece sospechosa o no tienes claro quién es el responsable de un web mejor que no les des tu e-mail.

Decide si te conviene utilizar más de una dirección de correo:

Una de ellas será para los mensajes más personales y la otra para usarla en las salas de chats o listas de distribución. Ésta última será desechable, de modo que si empieza a recibir Spam pueda cerrarse sin afectar a tu correo personal o profesional. También puedes dar tu dirección temporal en sitios que no te inspiren la suficiente confianza. Si luego tienes que prescindir de ella no afectará a tu buzón personal.

Usa un nombre poco común en tus cuentas de e-mail:

La elección de tu dirección de correo puede afectar a la cantidad de Correo Basura que recibas. Como ya hemos analizado en este informe, los Spammers tienen dos formas de conseguir direcciones: Rastrear las páginas webs, listas, foros…, o programar combinaciones de nombres posibles para un determinado proveedor de e-mail, esperando encontrar direcciones válidas. Por esta razón, un nombre común puede que tenga más cantidad de Spam que uno más complejo que combine letras y números.

Usa los filtros en tus programas de correo:

Las últimas versiones de los gestores de correo (Eudora, Outlook, etc.) incluyen herramientas para filtrar los e-mails, logrando que aquellos que no son deseados sean enviados a una carpeta distinta a la de entrada de tus correos.

Combate y denuncia los Abusos:

Si simplemente filtras el Correo no deseado que recibes y no lo combates estarás contribuyendo a que sigan con sus prácticas.

Puedes denunciar los abusos del Spam en estas direcciones:

Agencia de Protección de Datos: https://www.agpd.es

Guardia Civil: http://www.guardiacivil.org/

Asociaciones: http://www.aui.es/quejas

En cualquier queja, comunicado o denuncia que se haga sobre Correo Basura es muy importante incluir la cabecera del e-mail (generalmente no están visibles). Como sabemos, la información de la cabecera contiene datos importantes que deben ser conocidos por los organismos a los que envíes tu queja.

Qué NO hay que hacer frente a los envíos masivos de correo electrónico no solicitados:

Hay una regla importante que se debe recordar cuando nos enfrentamos con remitentes de Correos, no podemos atacarles infringiendo la legalidad, debemos mantener nuestra superioridad moral y denunciarlo por los cauces legales. En muchos casos además la información del remitente está falsificada. Por lo tanto, cuando nos encontremos con un remitente de Spam o con un sitio deshonesto, NO debemos:

- Amenazarlo con violencia o vandalismo.
- Bombardear el sitio con mensajes.
- Bombardear con mensajes al remitente del Correo Basura, que puede ser en muchos casos un tercero inocente.
- Atacar el sitio con métodos de piratería electrónica, técnicas de hacking...
- Intentar hacer caer el sitio por cualquier medio ilegal.

Cómo evitar engaños y abusos a través del Correo Electrónico:

Usa el sentido común, no abras los ficheros adjuntos a un mensaje si no lo esperabas, mantén actualizado tu sistema operativo, utiliza algún antivirus actualizado y haz copias de seguridad de la información que sea importante. Desconfía también de todos aquellos mensajes que exigen o recomiendan realizar una llamada a un número de tarificación adicional (803, 806, 805, 807,…) y de todos aquellos que te piden algo a través del e-mail en relación con una Web donde tengas información sensible (banco, seguros, administración electrónica,..).

Consejos para los que gestionan CONTENIDOS en páginas Web y Listas de distribución.

De carácter general

- No publiques direcciones de correo electrónico de terceros en tus páginas si no es estrictamente necesario.
- Es mejor publicar los correos en formato gráfico, sin enlace al e-mail o con algún sistema de protección para encriptar o componer las direcciones de correo, ya que los recolectores de e-mails rastrean todo el código Html y recogen todo aquello que tenga los símbolos "@" y "." en una misma palabra.

- En las webs es preferible incluir un formulario para dirigirse a alguien de nuestra organización antes que hacer pública una dirección de correo.

- Si gestionas listas no permitas altas sin que se validen a través del correo electrónico suscrito para evitar altas no deseadas. Envía siempre tus mensajes con un enlace o texto que permita darse de baja de forma sencilla y directa.

- Si gestionas foros o listas con los contenidos accesibles, es conveniente no escribir los e-mails de los participantes en los mensajes que se publican y si lo haces advierte de los riesgos a quien utilice estos foros.

- Siempre que puedas, intenta que las listas y foros de tu web dispongan de algún sistema de validación o moderación antes de hacer público un mensaje.

Pasos a seguir cuando alguien se suscribe a tu web vía e-mail

- Cuando alguien precise alguno/s de los servicios de tu página y te autorice a enviarle información es interesante que: Le informes sobre la finalidad y periodicidad aproximada de los comunicados o boletines que le vas a enviar, así como de quién es el responsable de los datos que nos suministra y si éstos se van a ceder a terceros.

- Procura que el consentimiento sea explicito para evitar que queden suscritos los que no han leído la información presentada (créenos es mejor para ti y para tu negocio).

- No pidas más datos de los que se necesitan, esto da confianza a los que utilizan tus productos y servicios.

- Si gestionas foros, listas o grupos de discusión, y se hacen públicos los datos que se piden, advierte de los riesgos que conlleva.

- Debes registrar la base de datos o fichero donde almacenas estos datos en la Agencia de Protección de Datos ya que el e-mail es un dato de carácter personal que es susceptible de ser tratado automáticamente.

Adquisición de bases de datos

Muchos gestores se preguntan si es adecuado comprar listas de direcciones para luego usarlas. Debes saber que la venta de datos sin consentimiento previo por el que aporta el titular del dato, está prohibida expresamente por la Ley Orgánica de Protección de Datos Personales y que constituye una falta muy grave, sancionada con una multa que puede ascender a 600.000 euros.

Si alguien te dice que está vendiendo listas de direcciones validadas, muéstrate escéptico, pídele el formulario de autorización de las personas de la lista y la cláusula donde se cede la transferencia de información. Lo más probable es que oculten su política de privacidad o que se atengan a legislaciones de otros países.

Lo aconsejable es que, ante una oferta de estas características y si no lo ves claro, te pongas en contacto con la Agencia de Protección de Datos. Ten en cuenta que la LSSI no permite los envíos de carácter comercial si no existe consentimiento previo de los usuarios.

Consejos para los ADMINISTRADORES de Correo

Políticas para los servidores / servicio de correo

Envío de correo:

- Relays cerrados para evitar el uso del servidor de correo por agentes externos a los dominios gestionados. Utilizar nuestro servidor desde fuera para enviar correo hacia fuera de nuestro servidor (rechazo de correo desde direcciones externas a nuestro dominio y destinadas a direcciones externas a nuestro dominio) (RFC 2505).

- Relays locales cerrados si es posible, evitando así la suplantación de identidades. No permitir el envío a usuarios de nuestro servidor sin que hagan un proceso de autenticación previo.

- Establecer un procedimiento de control y monitorización de flujo de envío de mensajes de cada usuario (RFC 2505).

- Registro (logs) de todas las transacciones SMTP realizadas (RFC 2505).

- A la hora del envío de un correo, comprobar que la parte local de la dirección (anterior a símbolo @) del remitente es correcta y está registrada en el dominio (durante la transacción SMTP en el comando MAIL FROM) (RFC 2505).

- Comprobar que el cuerpo de un mensaje que se va a enviar no lleva cabeceras Received previas introducidas por el usuario.

- Utilizar protocolo SPF durante la transacción SMTP.

- Utilizar SMTP con autenticación: ESMTP (RFC 2554).

- Rechazar cualquier conexión en la que el HELO/EHLO sea o bien alguna de las IP's de la organización, algunos de los dominios propios gestionados o algún nombre de máquinas propias, y no sean usuarios autenticados o maquinas que nos sean de la organización.

Recepción de correo:

- Establecer una política de control y monitorización de flujo de mensajes recibidos por los usuarios del sistema.
- Rechazar mensajes de correo que provienen de servidores de correo con una IP dinámica.
- Comprobar el dominio de la procedencia del mensaje en la transacción SMTP:
  - Rechazar correo procedente de dominios inexistentes (no tienen resolución DNS).
  - Aceptar correos cuyo dominio exista y la IP del remitente esté contemplada en el registro correspondiente
  - Rechazar correos cuyo dominio exista y la IP del remitente no esté contemplada en el registro correspondiente
  - Establecer política de actuación si el dominio existe pero no tiene registros de comprobación de remitentes.
- Rechazar mensajes de error provenientes de otros servidores en los que la dirección de correo electrónico que figure en la cabecera From: no exista.
- Rechazar mensajes de error dirigidos a más de un usuario.
- Rechazar correos en los que el identificador del mensaje (Message-ID) o la fecha no sea sintácticamente correcta.
- Definir y comunicar una política sobre el tratamiento de los virus.

Registro DNS:

Definir los registros que hay que almacenar en el servidor DNS correspondiente al menos en alguno de los existentes.

Gestión de cuentas / buzones:

- Establecer un periodo de caducidad para las cuentas. En caso de que una cuenta no reciba o envíe correo en ese periodo de tiempo, se eliminará o se inhabilitará.
- Establecer el límite superior para el número de envíos de mensajes de correos en un espacio temporal definido.
- Definir y comunicar la política de filtrado utilizado
- Establecer un protocolo vía web y e-mail para gestionar incidencias o quejas de los usuarios relacionadas con el servicio de correo.
- Comunicar todas estas cláusulas al usuario.

Políticas para los usuarios de correo:

Los usuarios son responsables de todas las actividades realizadas con las cuentas de correo electrónico que su ESP les proporciona.

El usuario no podrá:

- Contravenir la legislación vigente en materia de comunicaciones electrónicas al enviar correos
- Utilizar servidores de correo, propios o ajenos, para el envío masivo de mensajes de correo no solicitados por el destinatario (límite definido en la política de los servidores).
- Hacer un uso no autorizado de un servidor de correo ajeno para enviar un correo propio. Aunque el mensaje en sí sea legítimo.
- Falsificar las cabeceras de los correos electrónicos.
- Suplantar la identidad de terceras personas.
- Ocultar la identidad del emisor del correo.
- Revender el servicio en su totalidad o en parte a terceros, sin previo acuerdo con la empresa proveedora del servicio/servidor.
- Revelar su cuenta y su clave a terceros. Las cuentas son personales al titular del servicio e intransferibles.

Políticas para los que alojan equipos servidores de correo

Deben poner a disposición de los clientes que alojen servidores de correo las políticas de uso correspondientes, y el compromiso de éstos a cumplirlas y a trasladarlas a sus usuarios con penalizaciones en caso de incumplimiento.

AGRADECIMIENTOS

Este informe se ha realizado con el esfuerzo y contribuciones de diferentes personas y entidades que han aportado al Colegio Oficial de Ingenieros de Telecomunicación su conocimiento, saber hacer y los trabajos realizados sobre esta materia Por todo ello queremos hacer mención expresa a las siguientes organizaciones:

- **Asociación de Usuarios de Internet**, por poner a disposición de este informe todo el conocimiento y el material acumulado en las iniciativas de lucha contra el spam (www.aui.es/contraelspam) y para la calidad del correo electrónico: www.PePi-II.com

- **Ministerio de Industria, Turismo y Telecomunicaciones y Agencia de Protección de Datos**, por sus aportaciones en sus áreas de conocimiento.

- Y finalmente a todos los miembros del **Grupo de Nuevas Actividades Profesionales (NAP), del Colegio Oficial de Ingenieros de Telecomunicación**, por su tiempo y dedicación.

Por último queremos subrayar que el contenido del capítulo 5, corresponde al tercer bloque del proyecto de fin de carrera "**Aplicaciones y abusos de Internet como canal de comunicación del comercio electrónico**", realizado por **Marta Martín-Moreno Redondo** bajo la Tutoría de **Fernando Sáez Vacas**. Este trabajo fue presentado en la ETIST, de la Universidad Politécnica de Madrid, en Abril de 2.004. El texto completo puede encontrase en:

http://www.gsi.dit.upm.es/~fsaez/intl/proyectos/pfcmarta.html

A todos ellos nuestro sincero agradecimiento por su disponibilidad y generosidad para compartir este trabajo con el colectivo de ingenieros de telecomunicación y con la sociedad en general.

ANEXOS

Anexo 1: Protocolos de correo electrónico

A continuación se presentan de forma resumida y funcional los protocolos de correo electrónico actualmente en vigor. Este análisis se centrará en aspectos relacionados con el posible mal uso que se puede dar a este servicio. Para un análisis más detallado de estos protocolos consulte los documentos completos en la página web:

http://www.ietf.org/rfc.html

El IETF (Internet Ingineering Task Force, Equipo de Trabajo de Ingeniería de Internet)

El **IETF** (Internet Ingineering Task Force, Equipo de Trabajo de Ingeniería de Internet) es una comunidad internacional abierta, compuesta por diseñadores de redes, vendedores e investigadores preocupados por el desarrollo de Internet, y que apuestan por un fácil y sencillo uso de la Red.

El trabajo técnico que actualmente desarrolla el IETF está dividido en diferentes áreas: Enrutamiento, transporte, seguridad, etc., siendo cada una de ellas tratada por un grupo de trabajo diferente. La mayoría del trabajo realizado se lleva a cabo recurriendo a listas de correo, no obstante, también se organizan tres reuniones anuales.

El IETF cuenta con más de 75 grupos de trabajo, cada uno de ellos con una lista de correo en la que se discuten unos o más borradores bajo desarrollo. Cuando se alcanza el consenso en un documento, éste puede ser distribuido como una RFC (Request For Comments, Petición de Comentarios).

¿Qué son las RFCs?

Las RFCs son documentos de registro dentro de la comunidad de estándares e ingeniería en Internet. En ellas **se describen los estándares de protocolo en que se basa Internet para su funcionamiento**. Son de acceso abierto a todo el público.

El proceso de implantación de una RFC consta de tres fases:

1. **Proposed standard:** Especificación de propuesta de estándar.
2. **Draft Standard:** Borrador a partir del cual se producirá el proceso de desarrollo y estandarización.
3. **Internet Standard:** Se caracteriza por un alto grado de madurez técnica, siendo aceptado de forma universal.

Normativa RFC 2821 – SMTP

El protocolo SMTP (Simple Mail Transfer Protocol) se utiliza para el **envío de los correos electrónicos**. En él se describe el proceso de comunicación entre el cliente SMTP y un servidor SMTP utilizando el protocolo de transporte TCP. El proceso de determinar cuál es la dirección a la que va destinado el mensaje no es objeto de este protocolo.

Para realizar el envío de un correo electrónico hay que seguir los siguientes pasos:

1. El cliente SMTP se conecta al servidor SMTP, realizando un telnet por el puerto 25.
2. El servidor SMTP responderá con el código 220 si el servicio de correo está disponible. En caso contrario el código de respuesta será el 421.
3. Si el servicio está disponible el cliente se tiene que identificar. Para ello utilizará el comando **HELO** seguido del nombre de la máquina cliente (en este paso se queda registrada la IP, nombre de la máquina o literal de la ip (ip encerrada entre[ ]) del host desde el cual se va a mandar el correo electrónico).
4. El servidor SMTP responderá a la identificación con el código 250 seguido del nombre del servidor de correo. Cualquier otro código diferente a 250 indica que se ha producido un error.
5. A continuación el cliente indica quién es el remitente del mensaje utilizando el comando **MAIL FROM:** seguido de la dirección de correo correspondiente.
6. Si la acción se completa con éxito el servidor SMTP responderá con el código 250. Cualquier otro código indica error.
7. El siguiente paso es identificar el destinatario, para ello el cliente introducirá la/s dirección/es de correo a las que va destinado el mensaje con el comando **RCPT TO:,** si hay más de un destinatario éstos irán separados por comas.
8. Si el destinatario/s es aceptado por el servidor responderá con un código 250 seguido de la/s dirección/es de los destinatarios y de las palabras **Recipient Ok**.
9. El siguiente paso es informar al servidor que se va a empezar a introducir el cuerpo del mensaje, para ello se utiliza la orden **DATA**.
10. El servidor responderá con el código 354 para invitar al cliente a introducir su mensaje. Para indicar el final del mensaje se debe finalizar éste con un punto en una única línea, seguido de un retorno de carro.
11. Si el mensaje es enviado satisfactoriamente, el servidor responderá con el código 250.
12. Para terminar la conexión entre el cliente y el servidor se utiliza la orden **QUIT**.

Normativa RFC 2822 – Formato de mensajes de Internet

La RFC 2822 define el **estándar del formato de mensaje de Internet**. Se establecen una gran cantidad de campos, muchos de los cuales no son del interés de este informe, por lo que al igual que se ha hecho con la RFC 2821, sólo se tendrán en cuenta aquellos campos más significativos dentro del ámbito de la seguridad y autenticación de los correos electrónicos.

El correo electrónico se puede dividir en tres partes

- El cuerpo del mensaje.
- Los encabezados del mensaje.
- La envoltura del mensaje.

A continuación se presentan detalladamente cada una de ellas:

Cuerpo del mensaje:

Esta parte del mensaje es la que menos interés tiene para el análisis del correo electrónico. Aquí se encuentra la información escrita por el usuario remitente al usuario final. Es la información que se quieren transmitir entre ellos. La forma en que esta codificada viene determinada por la norma **RFC 2045.**

Encabezados del mensaje:

Los textos situados antes del cuerpo del mensaje se consideran cabeceras del mismo. En general, el software de transporte de correo no revisa ni altera los encabezados del correo, a excepción de la cabecera Received. Las cabeceras se pueden agrupar en diversos campos según su funcionalidad:

- Campos del Remitente
- Campos del Destinatario
- Campos de Referencia
- Campos de Seguimiento
- Campos de Extensión
- Campos definido por el usuario
- Otros campos

Campos del Remitente

Estos campos hacen referencia a la procedencia del mensaje. Son tres:

- **From**: Cuenta/s de correo que originaron el mensaje. Autor/es del mensaje. Este campo lo introduce el usuario (no debería contener ninguna dirección que no se corresponda con el/los autor/res del mensaje).
- **Sender**: Dirección de una cuenta de correo. Especifica el agente transmisor del mensaje, el encargado de remitirlo a la dirección de destino. Este campo lo introduce el usuario.
- **Reply-to**: Cuenta/s de correo a donde se dirigirán las respuestas al correo. En ausencia de este campo las respuestas se dirigirán a la/s dirección/es indicadas en el campo From. Este campo lo introduce el usuario.

Campos del Destinatario

Existen tres campos diferentes dentro de esta agrupación:

- **To**: Este campo contiene la/s direcciones de los principal/es destinatario/s del mensaje. Este campo lo introduce el usuario.
- **Cc**: Campo que indica la/s dirección/es a las que se les hará llegar una copia del correo, aunque el contenido del mensaje puede que no vaya dirigido expresamente a ellos. Este campo lo introduce el usuario.
- **Bcc**: Campo que indica la/s dirección/es a donde se remitirá una copia del mensaje. Los destinatarios indicados en To y en Bcc no ven este campo. Este campo lo introduce el usuario.

Campos de Referencia

También se pueden denominar campos de identificación. Existen varias cabeceras de las cuales se presentan cuatro:

- **Message-ID**: Esta cabecera hace referencia a un código de identificación único relacionado con el correo enviado. Este código es asignado por el servidor de donde sale el mensaje (máquina remitente). En ningún momento del camino seguido por el mensaje este número es cambiado o modificado por ningún servidor.

- **In-Replay-To**: Este campo contiene todos los identificadores de mensaje (ID) a los que este mensaje responde. Si hay mas de un identificador irán separados por comas, todos ellos encerrados dentro de < >. Este campo es generado por la aplicación cliente.

- **Reference**: Contiene todos los ID de los mensajes a los que éste hace referencia. Este campo es generado por la aplicación cliente.

- **KeyWords**: Este campo contiene palabras clave o frases que identifican el contenido del mensaje. Este campo es añadido por el usuario.

Campos de Seguimiento

Este conjunto de cabeceras, de nuevo está compuesta por varios campos, de los cuales únicamente se tratarán dos:

- **Return-Path**: Este campo es añadido por el último servidor que entrega el correo al usuario final. Contiene la ruta de acceso que ha tomado el mensaje desde su origen hasta su destino. Es la dirección de correo electrónico que se especificó en la transacción SMTP con la instrucción MAIL FROM:. Este campo puede no coincidir con el campo Form: de las cabeceras de origen.

- **Received**: Este campo es el más importante para la identificación del origen del mensaje. Existirán tantos campos Received como servidores SMTP por los que haya pasado el mensaje. Estas cabeceras se van añadiendo al mensaje según va pasando por los diferentes servidores de correo, siendo el primer campo Received el último servidor por el que ha pasado el correo. En el último de los Received esta reflejada la dirección IP del host origen y el dominio identificativo que se escribió detrás del comando HELO del protocolo SMTP. Estos campos son añadidos por los servidores.

Campos de Extensión

Estos campos únicamente dan información de cual es el formato del mensaje contenido en el correo. La utilidad de estas cabeceras es la de proporcionar soporte a Multipurpose Internet Multimedia Extensión (MIME). Las principales cabeceras son las siguientes:

- **MIME-Version**: Versión del protocolo que se está utilizando en la aplicación cliente. Esta cabecera es añadida por el cliente.

- **Content-Transfer-Encoding**: De nuevo esta cabecera es introducida por la aplicación cliente. Contiene información para poder visualizar correctamente el mensaje en su destino.

- **Content-Type**: Otro campo más que informa sobre la forma en la que esta codificada la información del mensaje. Añadido por la aplicación del cliente.

Otros campos

Otros campos definidos dentro de la RFC son:

- **Date**: Fecha y hora en la que el mensaje es entregado a la cola del servidor SMTP para su envío. Este campo lo establece el servidor origen.

- **Subject**: Este campo contiene un pequeño texto con la descripción del objeto del mensaje. Este campo es rellenado por el remitente del mensaje.

Campos definidos por el usuario

Existe la posibilidad de que el usuario defina sus propios campos, además de los ya establecidos por la RFC. Éstos deberán empezar siempre por X-, seguidos del nombre que se le quiera asignar al campo.

Algunos filtros de Spam añaden un campo llamado **X-Spam** para informar de que es posible que ese correo sea indeseado.

Campos obligatorios

La RFC 2822 obliga a que exista un mínimo de cabeceras, éstas son:

- **From**: Si esta cabecera no se rellena, automáticamente tomará el valor de la dirección de correo introducida en la transacción SMTP con el comando MAIL FROM:
- **Date**: Esta cabecera es añadida automáticamente por el servidor.
- **To**: Si esta cabecera no se rellena, automáticamente tomará el valor de la dirección de correo introducida en la transacción SMTP con el comando RCPT TO:
- **Received**: Esta cabecera es añadida automáticamente por los servidores de correo.
- **Message-ID**: Esta cabecera es añadida automáticamente por el servidor de correo origen.
- **Return-Path**: Esta cabecera es añadida automáticamente por el servidor de correo origen.

Envoltura del mensaje:

Esta parte del mensaje no está definida en la RFC 2822, sino que tiene más que ver con el protocolo SMTP, comentado en la RFC 2821, aunque por su gran relación con el formato del mensaje se ha decido incluirla en este apartado.

Como se explica en la descripción del protocolo SMTP, antes de mandar un correo electrónico se establece una conversación entre el cliente y el servidor. En ese intercambio de información se especifica el/los destinatario/s del correo y el remitente del mensaje, con los comandos **RCPT TO: y MAIL FROM:** respectivamente. Estos datos son los que utilizan los servidores de correo para encaminar el mensaje a su destino, y son los que forman la envoltura del mensaje.

Hay que destacar que estos dos datos son independientes de los reflejados en las cabeceras From: y To: especificados anteriormente en los encabezados del mensaje. Los datos de RCPT TO estarán siempre en la primera cabecera Received creada (ultima que se puede ver en el correo recibido). El dato de MAIL FROM siempre coincidirá con el campo de la cabecera Return-Path.

Anexo 2: Normativa RFC 2045 – MIME

Las cabeceras descritas en la RFC 2822 son suficientes para enviar correo codificado en texto ASCII, pero no son adecuadas para **mensajes multimedia**. Para tal propósito se creó esta RFC, la **MIME (Multipropose Internet Mail Extensions)**, un añadido a la RFC 2822.

Las cabeceras que añade este protocolo al cuerpo del mensaje han sido explicadas anteriormente en la sección "Campos de Extensión" de la RFC 2822:

- MIME-Version
- Content-Transfer-Encoding
- Content-Type

Este protocolo de codificación de datos no conlleva ningún posible problema relacionado con el uso malintencionado del correo electrónico, por lo que no se describirá en detalle su funcionamiento. La presentación de esta RFC ha tenido únicamente como objeto observar de dónde proceden ciertas cabeceras de e-mails, para la correcta interpretación de éstos.

Anexo 3: Normativa RFC 1939 – POP3

El protocolo POP3 (Post Office Protocol versión 3, Protocolo de oficina de correo), permite a los clientes de correo electrónico (UA) **recoger los mensajes de los servidores remotos (servidores POP) y guardarlos en las máquinas locales.**

Para recoger el correo de un servidor POP el cliente debe realizar una serie de pasos:

1. Tiene que abrir una conexión TCP en el puerto 110 del servidor POP.
2. El servidor POP responderá con un indicador de estado y una palabra clave. Si el servicio está disponible responderá con el indicador de estado positivo **+OK**, en caso contrario responderá con el negativo **-ERR**.
3. Si el servicio está disponible se pasa a la fase de autorización. El cliente se identificará con las ordenes **USER** y **PASS**.
4. El servidor responderá con **+OK** si el login y el password son los correctos, proporcionando acceso exclusivo al buzón.
5. El usuario puede utilizar el comando **LIST** para ver cuántos correos hay en el buzón.
6. Con el comando **TOP** <nº_mens> <líneas> el cliente puede recuperar la parte del encabezado de un determinado mensaje y un número de líneas del cuerpo del mensaje.
7. Para recoger un determinado mensaje, se utiliza el comando **RETR** <nº_mens>.
8. Para marcar un mensaje como leído se utiliza el comando **DELE** <nº_mens>.
9. Para terminar la sesión POP se utiliza el comando **QUIT**. Se eliminan aquellos mensajes que han sido marcados como leídos con el comando **DELE**. Hasta que no se invoca a la orden QUIT los mensajes marcados no son borrados del buzón.

Anexo 4: Normativa RFC 2060 – IMAP

El protocolo IMAP (Internet Message Access Protocol, Protocolo de acceso a mensajes de Internet) es un método utilizado por las aplicaciones cliente de correo electrónico **para obtener acceso a los mensajes almacenados remotamente**. En este caso los mensajes no son recuperados por el gestor de correo, sino que se trabaja con ellos directamente sobre el servidor.

Este protocolo es totalmente compatible con diferentes estándares de mensajes de Internet, como el protocolo MIME, que permite recibir correos con ficheros adjuntos.

En la RFC 2060 se definen una gran cantidad de instrucciones para poder interactuar con el servidor de correo y sus buzones. A diferencia de los demás protocolos, estas instrucciones van precedidas de una cadena de texto que elegirá el usuario arbitrariamente.

Los pasos fundamentales para trabajar con el correo electrónico utilizando este protocolo son los siguientes:

1. Establecer una comunicación TCP con el servidor IMAP por el puerto 143.
2. Si el servicio está disponible el servidor responderá con el estado **OK**, si no es así la respuesta será **BAD**.
3. El usuario deberá identificarse con el comando **LOGIN** <usuario> <password>, para poder tener acceso a los buzones.
4. Si el usuario y la contraseña son correctos el servidor devolverá un **OK**, en caso contrario un **BAD** o un **NO**, dependiendo de si los argumentos no son válidos, o se rechaza el usuario y la contraseña.
5. Una vez que el usuario ha sido autorizado, puede ver los buzones existentes con el comando **LIST** "" *.
6. Para ver el contenido de cada buzón se utiliza el comando **SELECT** <nombre_buzón>.
7. Se pueden crear otros buzones con el comando **CREATE** <nom_buzón_nuevo>.
8. También se pueden borrar buzones con el comando **DELETE** <nombre_buzón>.
9. Con el comando **FETCH** <num_mens> <parte_mens> se pueden ir viendo las diferentes partes de los mensajes del buzón que se haya seleccionado.
10. Con el comando **LOGOUT** se termina la sesión.

Existen muchos mas comandos para interactuar con el correo, aunque el proceso principal para la lectura de los mensajes es el que ha sido descrito.

Anexo 5: Normativa RFC 2505 – Anti SPAM

Esta RFC no posee el carácter de estándar, sino que es una serie de **prácticas recomendadas en los servidores de correo para evitar el Spam**. No se trata de la solución final contra el Spam, pero sí de una forma de reducir este fenómeno. Se pretende que los mensajes sean aceptados o rechazados en la transacción SMTP. Básicamente las recomendaciones que se presentan son las siguientes:

- Restringir el uso del servidor de correo por agentes externos al dominio/s gestionado/s por el servidor para mandar correos hacia el exterior del servidor.

- Rellenar las cabeceras Received con toda la información posible para poder encontrar el camino que ha seguido un determinado mensaje: IP del remitente, hora y fecha del mensaje, el argumento dado en el HELO de la transacción SMTP, información de autenticación si ésta se requiere para la transmisión...

- Tener un registro de eventos para poder seguir cualquier suceso que haya ocurrido.

- Rechazar correos provenientes de una determinada dirección IP.

- El servidor de correo ha de ser capaz de rechazar mensajes provenientes de un usuario específico, o de un dominio concreto, identificado durante la transacción SMTP en MAIL FROM:.

- El servidor debería disponer de herramientas para realizar un control de flujo de los mensajes enviados o recibidos.

- El servidor debería de disponer de un mecanismo para poder rechazar correos donde el campo MAIL FROM: contenga dominios inexistentes.

- El servidor solo debería permitir correo saliente donde el remitente indicado en MAIL FROM: de la transacción SMTP corresponde a un usuario registrado.

- El servidor de correo debería tener restringido el uso de los comandos VRFY, EXPN y ETRN para evitar el acceso a información restringida del servidor.

- El servidor debe tener la posibilidad de configurarse para proporcionar diferentes códigos de retorno según distintas reglas.

Anexo 6: Normativa RFC 2554 – ESMTP

En esta RFC se describe una extensión para el protocolo de correo SMTP (Simple Mail Transfer Protocol). **Se trata de un mecanismo para autenticar la identidad del cliente que se conecta al servidor**. También permite la negociación de una capa de seguridad para hacer más segura la comunicación. El protocolo SMTP permanece inalterado en su forma, ya que los pasos que hay que seguir una vez que el usuario se haya identificado son exactamente los mismos.

Este protocolo añade nuevos comandos a los ya definidos en la RFC 2821. Estas nuevas instrucciones son:

- **EHLO**: Nuevo comando de saludo para iniciar la conversación SMTP con las instrucciones extendidas. Si el servidor responde satisfactoriamente a esta instrucción quiere decir que "sabe" hablar SMTP, y responderá con las opciones que tiene habilitadas. Si devuelve el mensaje de error éste únicamente tendrá implementado el protocolo SMTP.

- **AUTH**: Comando que sirve para negociar un protocolo de seguridad para el intercambio de datos. Los posibles protocolos, para la capa de seguridad, que se pueden negociar los da como respuesta el servidor al comando EHLO.

Anexo 7: Normativa SPF (borrador del IETF)

El protocolo SPF (Sender Policy Framework) es un sistema para **evitar el uso no autorizado del correo electrónico**. El administrador de un dominio especifica, mediante unos registros que se almacenan en el DNS (con formato TXT), cuáles son las direcciones IP de los servidores de correo que pueden mandar mensajes diciendo proceder de ese dominio.

Se trata de una extensión al protocolo SMTP (especificado en la RFC 282), de distribución libre y gratuita. Su implementación se puede dividir en dos partes:

1. Publicación de los registros TXT en el DNS con las direcciones IP de los servidores autorizados. Esto ha de ser realizado por el administrador del sistema. No requiere la instalación de ningún programa adicional. Una forma fácil de generar estos registros es utilizar un asistente, como el proporcionado en http://spf.pobox.com/wizard.html

2. Implementación de la comprobación de la identidad de los correos recibidos. Esta parte consiste en comparar la dirección de procedencia de los correos con la almacenada en los registros SPF de los servidores DNS. Esta comprobación no requiere ningún tratamiento especial, sino que una vez añadida al programa servidor de correo utilizado, no hace falta ningún tipo de mantenimiento.

Cuando un cliente SPF (en el servidor de destino) evalúa un registro SPF pude obtener siete resultados diferentes:

- **None**: El dominio de correo que se comprueba no tiene datos SPF.

- **Neutral**: El cliente SPF debe proceder como si el dominio no tuviera publicados registros SPF.

- **Pass**: Se trata de un mensaje legítimo, según el registro SPF procede de un MTA autorizado. El cliente de correo aplicará la política local específica a este mensaje.

- **Fail**: Se trata de un mensaje ilegítimo, según el registro SPF procede de un MTA no autorizado a mandar correos de ese dominio. El MTA debe rechazar el correo dando una respuesta de error (se recomienda devolver el código de error 550).

- **SoftFail**: El dominio tiene publicados registros SPF pero el mensaje no procede de un MTA autorizado, pero el administrador del dominio recomienda no rechazar el mensaje. Se pueden realizar otras comprobaciones antes de aceptar el correo.

- **Error**: Indica un error durante la comprobación SPF, el MTA debe rechazar el mensaje y responder con el código de error 450.

- **Unknown**: Indica un procesamiento incompleto, el MTA debe proceder como si el dominio no publicara registros SPF.

Ya que este protocolo basa su comprobación en el argumento del HELO/EHLO se recomienda seguir estrictamente la RFC 2821, que especifica que el argumento de HELO/EHLO debe ser bien la dirección IP o bien el nombre canónico del servidor remoto.

BIBLIOGRAFÍA Y DOCUMENTACIÓN UTILIZADA

1. Estudios

- "Unsolicited commercial electronic messages (SPAM) in OECD countries, Directorate for science, technology and Industry", *Committee for information, computer and communications Policy, 21-May-2003.*
- "Communication from the commission to the european parliament, the council, the european economic and social committee and the committee of the regions on unsolicited commercial communications or 'Spam'", *Commission of the European Communities. Brussels, 22-01-2004.*
- "Project Lumos: A Solution Blueprint for Solving then Spam Problem by Establishing Volume Email Sender Accountability", *Network Advertising Iniciative, Email Service Provider Coalition. Septembet 24, 2003.*
- "Anti-Spam Solutions and Security", *Dr. Neal Krawetz, 26 February 2004.*
- "Spam: A Security Issue", *CipherTrust, December 2003.*
- "Technical responses to Spam", *Taughannock Networks, November 2003.*
- "Computer Networking, A Top-Down Approach Featuring the Internet", *James F.Kurose, Keith W.Ross. Addison Wesley, 2001.*
- "4ª encuesta a Usuarios de Internet de la AIMC febrero 2001" y "5ª encuesta a Usuarios de Internet de la AIMC febrero 2002", *www.aui.es*.
- "Consumer Attitudes Regarding Unsolicited Commercial Email (Spam)", *octubre-diciembre de 2003. Realizado por TACD (Transatlantic Consumer Dialogue), www.tacd.org/docs/?id=225*.
- "Encuesta sobre el Spam", *realizada por la Asociación de Usuarios de Internet (AUI) a través de su página web (www.aui.es) entre abril y mayo de 2003.*
- "Estadísticas obtenidas del sitio web www.xtdnet.nl/paul/Spam", *Paul Wouters.*
- "False Claims in Spam, a report by the FTC's Division of Marketing Practices", *abril de 2003, Federal Trade Commission (www.ftc.gov).*
- "IV Estudio sobre el Marketing y la Publicidad Medios Interactivos 2002. AGEMDI-fecemd", *Asociación de Agencias de Marketing Directo e Interactivo-Federación Española de Comercio Electrónico y Marketing Directo; www.fecemd.es.*

- "Spam E-mail and Its Impact on IT Spending and Productivity" *(diciembre de 2003), Spira, J. B., realizado por Basex Inc., www.basex.com.*

- "Why Am I Getting All This Spam? Unsolicited Commercial E-mail Research", *marzo de 2003, Center for Democracy & Technology de la UE (www.cdt.org/speech/Spam/030319Spamreport.shtml).*

2. Legislación

- LSSI, LEY 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. BOE núm. 166.
- LGT, LEY 32/2003, de 3 de noviembre, General de Telecomunicaciones. BOE 04/11/2003.
- LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL 13-12-1999, num. 15/1999. BOE 14-12-1999, núm. 298, [pág. 43088].
- CÓDIGO PENAL ESPAÑOL, Ley Orgánica 10/1995, de 23 de Noviembre, BOE núm. 281, de 24 de noviembre de 1995.
- Directiva 2002/58/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones).

3. Normativa técnica: RFCs

Todas estas normas se pueden encontrar en:

http://www.ietf.org

- *RFC 2821, J.Klensin,* "Simple Mail Transfer Protocol", *RFC 2821, April 2001.*

- *RFC 2822, P.Rosnick,* "Internet Message Format", *RFC 2822, April 2001.*

- *RFC 2045, N. Freed, N. Borenstein,* "Multipurpose Internet Mail Extensions (MIME) Part One: Fomat of Internet Message Bodies", *RFC 2045, Nov 1996. http://www.rfc-editor.org/rfc/rfc2045.txt*

- *RFC 1939, J.Myers and M.Rose,* "Post Office Protocol – Version 3", *RFC 1939, May 1996. http://www.rfc-editor.org/rfc/rfc1932.txt*

- *RFC 2060, R.Crispin,* "Internet Message Access Protocol – Verions 4rev1", *RFC 2060, Dec. 1996. http://www.rfc-editor.org/rfc/rfc2060.txt*

- *RFC 2505, G.Lindberg,* "Anti-Spam recommendations for SMTP MTAs", *RFC 2505, February 1999.*

- *RFC 2554, J.Myers,* "SMTP Sevice Extensions for Authentication", *RFC 2554, March 1999.*
- *SPF (Sender Policy Framework),* "A Convention to Describe Hosts Authorized to Send SMTP Traffic", *http://spf.pobox.org*

4. Referencias

[1] http://www.templetons.com/brad/Spamterm.html, "Origin of the term "Spam" to mean net abuse", *Brad Templeton, 2003.*

[2] http://www.multicians.org/thvv/mail-history.html, "The History of Electronic Mail", *Tom Van Vleck, Febrero 2001.*

[3] http://www.faqs.org/rfcs/rfc706.html, "RFC 706 - On the junk mail problem", *Jon Postel, Noviembre 1975.*

[4] http://keithlynch.net/Spamline.html, "Keith Lynch's timeline of Spam related terms and concepts", *Keith Lynch, 2002.*

[5] http://www.itu.int/Spam, "CHAIRMAN'S REPORT", ITU WSIS Thematic Meeting on Countering Spam", *Ginebra, Julio 2004.*

[6] http://www.itu.int/Spam, "CURBING SPAM VIA TECHNICAL MEASURES: AN OVERVIEW", *ITU WSIS Thematic Meeting on Countering Spam, Ginebra, Julio 2004.*

[7] http://www.oecd.org, "OECD Workshop on Spam – Report of the Workshop", *DSTI/CP/ICCP(2004)1, OECD Task Force on Spam, Bruselas, Febrero de 2004.*

[8] http://www.oecd.org/document/39/0,2340,en_2649_22555297_33680935_1_1_1_1,00.html, "2nd OECD Workshop on Spam – Report of the Workshop", *DSTI/CP/ICCP/SPAM(2004)7, OECD Task Force on Spam, Busan, Septiembre de 2004.*

[9] http://online.wsj.com/article_print/0,,SB1037138679220447148,00.html, "For Bulk E-Mailer, Pestering Millions Offers Path to Profit", *Mylene Mangalindan, The Wall Street Journal, 13 de Noviembre de 2002.*

[10] http://europa.eu.int/documents/comm/index_es.htm, "Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre las comunicaciones comerciales no solicitadas o Spam", *Bruselas, 22 de Enero de 2004.*

[11] http://ops.ietf.org/lists/namedroppers/namedroppers.2002/msg00656.html

[12] http://www.danisch.de/work/security/txt/draft-danisch-dns-rr-smtp-03.txt

[13] http://www.pan-am.ca/dmp/draft-fecyk-dmp-01.txt

[14] http://www.microsoft.com/mscorp/twc/privacy/Spam/senderid/overview.mspx, "Sender ID Framework Overview", *Microsoft Corporation, Septiembre de 2004.*

[15] http://spf.pobox.com, "Sender Policy Framework".

[16] http://www.ietf.org/internet-drafts/draft-delany-domainkeys-base-00.txt, "Draft de Internet de DomainKeys".

[17] http://www.networkmagazine.com/shared/article/showArticle.jhtml?articleId=47902587, "Sender ID In Limbo As IETF's MARID Working Group Is Disbanded", *Andrew Conry-Murray, Septiembre de 2004.*

[18] http://www.iksjena.de/mitarb/lutz/usenet/teergrube.en.html, "Teergrubing FAQ", *Lutz Donnerhacke.*

[19] http://www.rhyolite.com/anti-Spam/dcc/, "Distributed Checksum ClearingHouse", *Rhyolite Systems.*

[20] www.nuclearelephant.com, "BAYESIAN NOISE REDUCTION: PROGRESSIVE NOISE LOGIC FOR STATISTICAL LANGUAGE ANALYSIS", *Jonathan A. Zdziarski, 2004.*

[21] http://www.oecd.org, "Joint initiative between public and private sectors against mobile Spam – 2nd OECD Workshop on Spam", *Busan, Septiembre de 2004.*

5. Artículos

- "¿Es nuestro buzón de correo más libre tras un año de LSSI?", *Juan Carlos Plaza Soler, Mundo Internet 2004, Febrero 2004.*
- "Métodos efectivos contra el correo basura", *Jaime Fernández Gómez, responsable de sistemas de acens technologies, Mundo Internet 2004, Febrero 2004.*
- "Bruselas contra el 'Spam'", *Reuters, www.elmundo.es/navegante.*
- "Diez recomendaciones de Symantec para luchar contra el Spam" (6 de junio de 2003), *www.noticiasdot.com*.
- "Dos de cada tres correos basura son un fraude, según un informe de la Comisión Federal de Comercio de EEUU", *30 de mayo de 2003, www.efe.com*.
- "Dos tercios del 'Spam' que recibimos es fraudulento", *30 de abril de 2003, www.iblnews.com.*

- "EEUU limita el Spam", *24 de noviembre de 2003, www.vunet.com.*
- "El 55,1% de los mensajes de correo electrónico de EEUU son 'Spam'", *3 de junio de 2003, www.iblnews.com.*
- "El Congreso de USA aprueba ley 'anti-Spam'", *24 de noviembre del 2003, www.conocimientosweb.net/dt.*
- "El correo basura colapsará los 'e-mails' durante un tiempo", *3 diciembre 2002, www.iblnews.com.*
- "El Spam a los clientes será legal en España", *www.noticiasdot.com*.
- "El 'Spam' cuesta 20.000 millones de dólares a las empresas en todo el mundo", *30 de diciembre de 2003, www.elmundo.es/navegante.*
- "El 'Spam' supera por primera vez la mitad del total de correos electrónicos", *AFP, www.elmundo.es/navegante.*
- "El volumen del correo masivo amenaza el futuro del 'e-mail'", *1 de mayo de 2003, Iblnews, Agencias. www.iblnews.com.*
- "Email Address Harvesting: How Spammers Reap What You Sow", *noviembre de 2002, www.ftc.org.*
- "En Gran Bretaña el envío de SPAM es un delito", *19 de septiembre del 2003, www.conocimientosweb.net/dt.*
- "Estados Unidos aprueba ley de regulación del Spam", *2 de diciembre de 2003, Guillem Alsina, www.diariored.com.*
- "Europa prohibirá el Spam a partir de otoño", *Sánchez, Y., www.diarioenred.com.*
- "Evaluación de Alternativas para Reducir el Spam", *Sanz de las Heras, J., mayo de 2000, www.rediris.es.*
- "FAQ: Is there a Bayesian filter for Outlook?", *Graham, P. (2003).*
- "Filters vs. black list", *septiembre de 2002, Graham, P., www.paulgraham.com.*
- "For Bulk E-Mailer, Pestering Millions Offers Path to Profit", *13 de noviembre de 2002, Mangalindan, M. del Wall Street Journal, www.alanluber.com.*
- "Frequently asked questions about Spam", *Hazen Mueller, S., Panitz A. R., www.Spamabuse.net.*
- "¡Guerra al Spam!", *5 de febrero de 2004, Guillem Alsina, www.diariored.com.*
- "Inside the Spammer's world", *29 de junio de 2001, Livingston, B., http://news.com.com.*

- "Internautas, empresas y legisladores se unen contra la plaga del correo basura", *22 de mayo de 2003, www.iblnews.com.*
- "La Comisión Europea declara la guerra al Spam", *23 de enero de 2004, www.vunet.com.*
- "La Fecemd advierte sobre la legislación de e-mails publicitarios", *9 de diciembre de 2003, www.fecemd.org.*
- "La Lucha contra el Envío Masivo de Correos no solicitados (Spams)", *Burgess, T., www.aui.es.*
- "La mayoría de los cibernautas son víctimas del correo indeseado", *Tortello M. A., www.aui.es.*
- "La UE anuncia medidas contra el 'Spam' por la desconfianza que causa", *27 de enero de 2004, Europa Press, www.elmundo.es/navegante.*
- "Las cifras del correo basura", *A. B. F., www.elmundo.es/navegante.*
- "Legisladores británicos planean extraditar a quienes envíen Spam", *30 de octubre del 2003, www.conocimientosweb.net/dt.*
- "Legisladores de Estados Unidos legaliza el Spam", *27 de noviembre del 2003, http://www.conocimientosweb.net/dt.*
- "Los internautas esconden sus direcciones email por miedo al "Spam"", *www.noticiasdot.com*.
- "Los productos de consumo y de salud son los que más utilizan el Spam", *www.noticiasdot.com*.
- "Luchando contra la publicidad no deseada (o Spam) en el correo", *1 de febrero de 2003, Katja y Guido Socher, LinuxFocus.org, http://www.linuxfocus.org/Castellano /January2003/article279.shtml.*
- "Make'em pay", *12 de febrero de 2004, www.economist.com.*
- "¡Muerte al Spam!", *30 de abril de 2003, Rodríguez, G., www.libertaddigital.com.*
- "Multan a un 'Spammer' con 93.000 euros tras aceptar los cargos", *14 de mayo de 2003, www.iblnews.com.*
- "Riesgos del Spam", *Van der Reis,J., www.vanderreis.com/Glosario/riesgosSPAM.htm.*
- "Rompe las Cadenas", *Campaña contra el Correo Basura, www.aui.es/contraelSpam.*
- "Sobre la Realidad de Hacer E-commerce V (o El Spam, ¿Violencia contra el Usuario?)", *diciembre 2003, Iriarte Ahon, E., www.diariored.com.*

- "¡Socorro! ¡Me ahogo en E-Mails basura!", *30 de junio de 2003, Fleming, P., www.fecemd.es.*
- "Spam king lives large off others' e-mail troubles", *22 de noviembre de 2002, Wendland, M., www.freep.com/money/tech/mwend22_20021122.htm.*
- "¿Spam sí o Spam no? Legalidad", *26 de agosto de 2003, Hernández, J., www.baquia.com.*
- "Técnicos y gobiernos sacan la artillería pesada contra el "Spam"", *Molist, M. ((c) 2003), www.aui.es.*
- "The Email Abuse FAQ", *http://members.aol.com/emailfaq/emailfaq.html*.
- "The Great Spam Supply Chain", *15 de marzo de 2003, Scalet, S. D., www.cio.com/archive/031503/tl_email.html.*
- "Winning the War on Spam: Comparison of Bayesian Spam filters", *Graham, P., agosto de 2003, www.paulgraham.com.*
- *Documentación de la conferencia* "Internet Level Spam Detection and SpamAssassin 2.50", *Sergeant, M. (Senior Anti-Spam Technologist, 2003), MessageLabs, obtenido de www.Spamconference.com.*
- *Documentación de la conferencia* "The Spammer's compendium", *Graham-Cumming (2003), http://popfile.souceforge.net, obtenido de www.Spamconference.com.*
- *Documentación de la conferencia* "Spam Filtering. From the Lab to the Real World", *Goodman, J., Microsoft Research. Obtenido de www.Spamconference.com.*
- "Tutorial sobre Postfix", *2004-02-02, http://hal9000.eui.upm.es/halwiki/Postfix).*
- "Tutorial sobre Sendmail", *www.seguridad.unam.mx/Tutoriales/Tutoriales/sendmail/sendmail.html.*

6. Otras páginas web de interés

- http://www.abuse.net
- http://www.PePi-II.com
- http://www.aui.es
- http://www.rediris.es/mail/abuso
- http://www.cauce.org y www.euro.cauce.org
- http://www.dnsstuff.com
- http://www.europa.eu.int/comm
- http://www.europa.eu.int/pol/infso/index_es.htm
- http://www.exim.org
- http://www.ftc.gov
- http://www.ftc.gov/bcp/conline/edcams/Spam/index.html
- http://www.ftc.gov/openrelay
- http://www.internautas.org
- http://www.mail-abuse.org
- http://www.messagewall.org
- http://www.ordb.org
- http://www.postfix.org
- http://www.procmail.org
- http://www.razor.sf.net
- http://www.rediris.es
- http://www.rompecadenas.com
- http://www.samspade.org
- http://www.sendmail.org/antiSpam.html
- http://www.Spamassassin.org
- http://www.Spambouncer.org
- http://www.Spamcop.net
- http://www.Spamhaus.org

- http://www.Spamlaws.com
- http://www.tuxedo.org/~esr/bogofilter
- http://www.unicom.com/sw/blq
- http://www.vanderreis.com