

SPAM

¿Qué es y Cómo Combatirlo?

¿De qué se trata?

Todos, en mayor o menor medida, estamos cansados de recibir en nuestras casillas de correo electrónico decenas (sino cientos) de mensajes que jamás hemos solicitado y que ni siquiera nos son de utilidad. Para empeorar las cosas, nos cansamos de recibir una y otra vez los mismos mensajes, casi todos con propagandas de los más diversos artículos.

Se denomina SPAM al envío masivo de correo electrónico, aunque el nombre técnico es "CECNS" (Correo Electrónico No Solicitado).

Muchas empresas acostumbraban (y aún acostumbran) a enviar folletos de propaganda indiscriminadamente, ya sea a través del correo postal, o bien distribuyéndolas puerta a puerta. Son esos panfletos que todos los días arrojamos a la basura, sin siquiera abrir los sobres, ni mucho menos leer algo. Un bajo porcentaje de aquellos que reciben esa publicidad tal vez llega a convertirse en clientes.

Con el advenimiento de la tecnología, internet y el correo electrónico, muchas empresas volcaron sus actividades de propaganda, a través de esta nueva herramienta con un potencial casi infinito de nuevos clientes.

En efecto, el costo de envío de mails es tan barato, que con el equivalente al costo que normalmente enviarían unas pocas decenas de propagandas por correo postal, se envían (en cambio) cientos y tal vez miles de propagandas equivalentes por correo electrónico. La conveniencia es evidente, y notable.

No Todo lo que Brilla es Oro

Pero el asunto no es tan sencillo. Porque cuando un empresario enviaba por correo postal un panfleto de propaganda, él se

hacía cargo de los costos del correo, por lo tanto el destinatario podía simplemente tirarlo a la basura, sin haber tenido que pagar nada. Pero con el correo electrónico la cosa es muy diferente, porque aquí es el destinatario el que forzosamente tiene que afrontar un gasto a causa de esa propaganda que ni siquiera le interesa.

En efecto, es el usuario el que está pagando el servicio de mail (normalmente incluido en su servicio de internet), está pagando el uso de la línea (conexión) mientras descarga esos mensajes sin utilidad, está pagando electricidad y una línea telefónica (o de cable), todos ellos gastos que el comerciante inescrupuloso que utiliza estos métodos no afronta.

Primeras Legislaciones

Tan injusta y grave llega a ser la importancia del SPAM, que muchos especialistas consideran que pone en riesgo el futuro del correo electrónico.

Pero internet es un ámbito que está poco regulado, con grandes falencias de legislación, y en el que no están claramente definidos los límites del derecho público internacional. Esto complica las cosas a la hora de regular y legislar inclusive apuntando a la protección del usuario.

Seguramente el lector habrá recibido mensajes de propaganda (SPAM) con una leyenda al pie similar a esta: "bajo la ley 168 de regulación internacional, este mensaje no es considerado SPAM".

Esta leyenda es falsa, y no busca otra cosa que desorientar al receptor del mensaje. Es necesario saber que **sí** existen normativas, que en todos los casos restringen severamente o prohíben el envío de correo electrónico comercial no solicitado.

La famosa ley citada por ese párrafo, no es una ley internacional (esta figura en derecho no existe, porque no hay leyes internacionales, siempre hay una corte jurisdiccional), sino que es una Ley Federal de los Estados Unidos de Norteamérica.

Pero eso no es todo, además, los mensajes ni siquiera cumplen las exigencias de esa ley, que entre otras cosas obligan al remitente (para que el mensaje no sea considerado SPAM) a:

“El SPAM siempre obliga al usuario a una erogación, y por lo tanto en la Argentina constituye una violación de la ley 24.240.”

- ❖ Incluir en el mensaje el Nombre y Apellido del remitente.
- ❖ Incluir la dirección POSTAL (no de e-mail) del remitente responsable jurídico del mensaje.
- ❖ Incluir un método automático e inmediato para que el receptor del mensaje pueda ser borrado de la lista de destinatarios.
- ❖ Incluir un número telefónico del remitente, responsable jurídico del mensaje.

No escapará al lector el hecho de que estos requisitos jamás son cumplidos por el remitente:

- ❖ Nunca encontraremos un nombre de una persona responsable, y si lo hay, sin dudas será falso.
- ❖ Lo mismo vale para la dirección postal (física) del remitente.
- ❖ Los métodos de “borrado” jamás funcionan, sino que para colmo, el simple hecho de responder un mensaje, le confirma al remitente que nuestra dirección está “viva”, y seguirá enviándonos mensajes.
- ❖ ¿Número telefónico? Si de casualidad encontramos alguno, sin dudas no será el teléfono del remitente.

De modo que estos mensajes no sólo son SPAM, sino que además violan la ley norteamericana que regula la propaganda por internet a través de e-mail.

Claro... pero nosotros no vivimos en Estados Unidos de Norteamérica, y esa ley no es aplicable... ¿o sí?

Tal vez sí lo sea. Porque si el servidor a través del cual ha sido enviado el mensaje está FÍSICAMENTE en los Estados Unidos de Norteamérica, entonces el administrador del sistema de e-mails (postmaster) tiene la obligación de cumplir con esa ley, por eso los administradores de correo electrónico norteamericanos son tan exigentes y por eso las restricciones a sus clientes. Sepa el lector que puede denunciar directamente al proveedor del servicio de e-mail desde el que el remitente nos ha enviado ese SPAM.

Cómo encontrar de dónde viene ese mensaje, ya es un asunto un poco más complicado, que puede ser un poco largo de tratar en este documento. Pero sí es posible.

Aquí, en Argentina, existe una especie de vacío legal en lo que a internet específicamente se refiere. Pero sí existe legislación que protege al usuario y al consumidor en general.

Es muy importante que el usuario de correo electrónico sepa que como usuario y como consumidor o potencial consumidor existen leyes que le asisten:

- ❖ Ley de “Lealtad Comercial”
- ❖ Ley 24.240 “De Defensa del Consumidor”

En efecto, si bien la ley 24.240 no aborda específicamente el uso del correo electrónico, sí define muy claramente cuáles serán los métodos lícitos de hacer publicidad.

Específicamente, la ley 24.240 (también conocida como LDC o Ley de Defensa del Consumidor) puntualiza con toda claridad que ningún usuario puede ser obligado a recibir publicidad que le ocasione una erogación (o gasto de dinero).

¿Cómo Combatir el SPAM?

Lo primero y fundamental a la hora de luchar contra el SPAM es saber.

- ❖ Saber que el SPAM **no es** un “mal necesario”, o una “condición sine qua non” del correo electrónico.
- ❖ Saber que tiene derecho a no ser obligado a pagar por una propaganda que no le servirá para nada.
- ❖ Saber que existen normas que lo protegen aquí y en casi todo el mundo.

Ahora usted ya sabe que el Correo Electrónico Comercial No Solicitado (CECNS) también conocido como SPAM, UBM, UCE, UCM, etc. no es algo que deba simplemente aceptar como algo que está allí y contra lo que nada puede hacerse.

Si todos los usuarios del mundo conocieran sus derechos y los hicieran valer, hace ya mucho tiempo que el SPAM hubiera dejado de existir.

Y esto se debe a que además del conocimiento, debe existir decisión, y perseverancia.

La decisión de luchar contra el spam, que implicará un esfuerzo mayor al de simplemente borrarlos, pero por otra parte, implica la determinación de defender lo propio, y de no permitir que manos anónimas e inescrupulosas se metan en su bolsillo y le quiten su dinero.

Pero también la perseverancia de insistir una y otra vez, cuantas veces sea necesario, reclamando a todos los que uno puede reclamar, sin olvidar a nadie en el camino.

Una vez que se han tomado estas dos fundamentales determinaciones, es necesario tener algunos conocimientos básicos que nos permitan identificar qué método emplear para que nuestro reclamo sea más o menos efectivo.

Como el lector habrá supuesto ya, aquél que nos envía estos mensajes, generalmente **sabe que está violando la ley** y que, por lo tanto, puede tener consecuencias. Como es consciente de que lo que hace está mal, tratará por todos los medios de ocultar su identidad, para que no podamos llegar a él.

Esto no hace sino agravar el delito cometido, porque agrega a la violación de la ley 24.240 (en Argentina) violaciones al código penal, por el uso fraudulento de un servicio público para cometer un delito, falsificación de identidad, y configura lisa y llanamente una estafa, por cuanto obliga al usuario a una erogación monetaria no autorizada y en su favor.

Comencemos por decir que el sistema de correo electrónico no es tan anónimo como parece. De hecho prácticamente siempre existe una forma de ubicar desde dónde ha sido enviado un mensaje, ya que

es virtualmente imposible que un mensaje no pase por ningún servidor intermedio para llegar a un destino, y cada servidor por donde el

mensaje fue pasando va dejando “su firma” de modo que la ruta del mensaje puede ser normalmente seguida hasta su origen.

La forma de determinar el origen de un mensaje electrónico requiere un mínimo de conocimientos, y lo dejaremos para más adelante.

En primer lugar, vamos los aspectos más importantes a tener en cuenta, para que nos orienten en nuestro accionar.

1.- Si su cuenta de correo es gratuita – Es muy importante saber qué tipo de cuenta de correo tiene. Una cuenta de correo gratuita no tiene el mismo trato que la cuenta de correo que le suministra su proveedor de internet. Y un SPAM que llega a una cuenta de correo gratuita, podría llegar a ser no considerado SPAM en algunos países, ya que el destinatario final no hace erogación alguna por el mensaje. No obstante, como las cuentas de correo gratuito suelen estar basadas en Estados Unidos de Norteamérica, si el mensaje **proviene** de una cuenta de estas, el remitente estará violando los términos del contrato. Simplemente reportando la violación al administrador de ese correo, será suficiente para que la cuenta del remitente sea definitivamente cancelada.

“La ley 24.240 puntualiza con toda claridad que ningún usuario puede ser obligado a recibir publicidad que le ocasione una erogación...”

2.- Si su cuenta de correo es paga - Si, en cambio, usted recibe SPAM en una cuenta por la que está pagando, tiene todavía varias herramientas a las que acudir.

Lea su contrato de servicio de internet. Verifique si cumple con los requisitos que fija la ley 24.240, y si contempla el caso del correo masivo no solicitado (spam). Si contempla ese caso, es probable que su proveedor disponga de filtros "anti-spam" gratuitos. Reporte los mensajes que reciba a su administrador de correo de internet.

3.- El mensaje propiamente dicho – Analizar el mensaje de **spam** que ha recibido es el siguiente paso. Lo primero que buscará, será una identificación **positiva** del remitente:

- ❖ Un nombre y apellido o razón social que identifique de quién se trata.
- ❖ Una dirección (calle y número) o número telefónico de contacto.

3.1.- Si el mensaje contiene cualquiera de estos datos, **Enhorabuena!**, porque es probable que se trate de uno de los pocos comerciantes verdaderamente honestos que es muy raro encontrar.

Si tiene estos datos, lo primero es registrarlos (por ejemplo imprimiendo el mensaje), para no olvidarlos si es necesario recurrir a la fuerza pública.

Nunca jamás utilice links en el mensaje que digan "no deseo recibir más e-mails" o enviar respuestas con el asunto "remove". Esas respuestas sólo agravarán su situación.

Lo primero será verificar a través de una guía telefónica si el número de teléfono se condice con el nombre o razón social del remitente. Si es así, llamar por teléfono al remitente y solicitar (preferentemente por fax para que quede constancia escrita) que no se le envíen más mensajes es una buena opción. El registro de esta llamada es un muy buen dato, ya sea grabándola o utilizando un fax.

Si el remitente se niega bajo el pretexto de que el sistema es automático y que para borrarse Ud. tiene que enviar un mensaje con el asunto "eliminar" o algo similar, infórmele al remitente que no lo hará, y que su comunicación será la única advertencia formal, y que de inmediato iniciará las acciones jurídicas y legales correspondientes en virtud del delito que el remitente ha cometido.



Deberá estar preparado para la segunda instancia, porque aún si el remitente acepta su requerimiento, normalmente usted no será removido de la lista de destinatarios.

En segunda instancia, lo ideal sería proceder a través de una **carta-documento** del siguiente tenor:

"De mi mayor consideración:

En relación al correo electrónico comercial no solicitado que Ud. me remite, y considerando que Ud. ha hecho caso omiso a las comunicaciones telefónicas y fax recibidas por usted los días xx, yy, y zz de las que obran en mi poder las grabaciones y copias correspondientes, cúmpleme informarle que de no cesar de inmediato en su actitud dolosa, daré inmediato traslado de la documentación que acredita su violación del artículo xx de la ley 24.240 de defensa del consumidor, y los artículos xx, yy, y zz del código penal de la nación, a las autoridades correspondientes. Por lo tanto intimole a que elimine inmediatamente de su lista de destinatarios de e-mail de su SPAM mi dirección de correo electrónico (sumail@suservidor.com), prohibiéndole además cualquier uso de la misma en el futuro.

Queda Ud. formal y debidamente notificado.

Firma y Documento de Identidad".

Probablemente este paso sea suficiente. Pero no siempre es así. En caso que aún así el remitente persista en sus envíos, diríjase con copia impresa de todos los mails que ha recibido de ese remitente, más copia de sus requerimientos de eliminación, más las grabaciones telefónicas que tuviera, más una copia de los artículos pertinentes de la LDC y del CPN, a la **Oficina de Defensa del Consumidor** más próxima a su domicilio (generalmente en los municipios locales). Allí radicará Ud. la denuncia respectiva contra el comerciante que le envía esas propagandas, con todos los antecedentes de que Ud. dispone.

Sepa también el lector que ya existe jurisprudencia sentada, con un fallo de la Justicia de la Provincia de Buenos Aires que obliga a un vendedor de "bases de datos" a

- ❖ Resultan mucho más difíciles de individualizar.
- ❖ Obligan a recurrir a un proveedor de internet en lugar del remitente en forma directa.
- ❖ La responsabilidad jurídica está más diluida y el usuario promedio no sabe que el administrador del servidor desde el que sale el mensaje es "responsable solidario" del delito que se comete.
- ❖ Exigen más conocimientos para encontrar a alguien a quién reclamar.

Pues bien, entramos entonces en la fase más difícil de la lucha contra el spamming.

A este punto llegamos generalmente por dos motivos:

- ❖ No hay una dirección o teléfono adonde podamos recurrir, ni una persona a quién denunciar con nombre y apellido.
- ❖ Sí hay datos, pero estos son falsos.



Esta incómoda situación nos obliga a buscar en el historial del mensaje (oculto al que lo recibe) para encontrar de dónde viene, y en consecuencia a quién efectuar el reclamo.

Debemos saber de antemano que en estos casos, el que recibirá nuestros reclamos no es la persona que los está enviando, sino la empresa que le brinda a esa persona el servicio de internet.

Así como aquel que alquila un vehículo que luego se utiliza para cometer un crimen es responsable del uso que se haga del mismo por parte de aquella persona que lo alquiló, en el caso de internet, el servicio de internet representa jurídicamente algo similar a la figura de ese vehículo alquilado que se usó para cometer un crimen.

Pero llegar a saber quién es el proveedor de internet de la persona que nos envía el spam no es cosa muy fácil.

eliminar ciertas direcciones de correo electrónico por violación a la ley de protección de datos haciendo lugar a un pedido de "habeas data" de un usuario.

3.2.- Si el mensaje no tiene datos del remitente que permitan individualizarlo, lo que lamentablemente resulta ser la mayoría de los casos, las posibilidades de acción son muy diferentes, y bastante menos efectivas.

Aquí explicaremos sólo la utilización de Outlook Express 6 (por ser uno de los clientes de correo electrónico más difundidos), el lector deberá encargarse de averiguar en el manual de uso de su cliente de correo la forma de acceder a la información de los "encabezados" o "headers" del mensaje.


Esto está explicado en el Anexo de este documento.

Una vez que identificamos al proveedor de internet, buscaremos la forma de contactarlo.

En primer término, lo haremos a la dirección de correo electrónico que el proveedor haya establecido para casos de abusos. Adonde enviaremos la información completa sobre los mensajes abusivos que el remitente le envía; se deberá adjuntar los mensajes que ha recibido en forma completa (incluyendo los encabezados), para que el administrador pueda

individualizar al usuario. Se tendrá la precaución de conservar copia de toda la documentación cursada al respecto.

Si este medio no fuera efectivo (no sería raro que suceda), se debería proceder a través de un instrumento público de validez oficial, es decir, a través de una carta documento similar a la citada previamente, haciendo expresa mención de que un usuario de ese proveedor está utilizando su servicio como herramienta para cometer un delito (que consiste en las violaciones a la ley 24.240 y de los artículos que correspondiere del CPN), y que en caso de que el administrador no arbitre los medios para impedir que esa actitud continúe, la denuncia que corresponda a las autoridades será cursada contra el proveedor del servicio.

El paso siguiente será efectivizar la denuncia ante la Dirección de Defensa del Consumidor más próxima a su domicilio, suministrando ante esa repartición toda la información de que dispone, incluyendo copia impresa de los datos que utilizó para llegar hasta el proveedor. 

Anexo

Cómo Interpretar los Encabezados de un Mensaje Electrónico

Explicaremos a realizar la maniobra a con la herramienta de MicroSoft ® Outlook Express ®.

En primer lugar identificaremos el mensaje sobre el que queremos saber información. Lo seleccionaremos con el puntero del mouse, y haremos click sobre el mismo con botón derecho. Se desplegará un menú emergente como se observa en la **figura 1**.

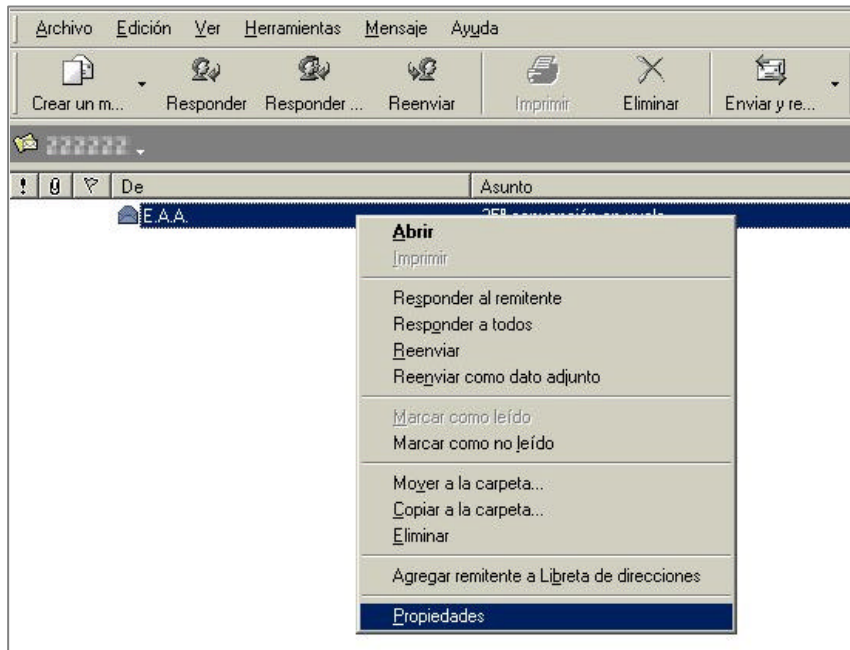


Fig. 1 – Menú emergente en la carpeta de mensajes, se activa con botón derecho del mouse.

Haremos click (esta vez con el botón izquierdo) en la opción **“propiedades”**, y se abrirá una nueva ventana, con los datos exclusivamente del encabezado del mensaje, en ella seleccionaremos la segunda oreja (“Detalles”), que nos revelará los encabezados ocultos, tal como se aprecia en la **figura 2**.

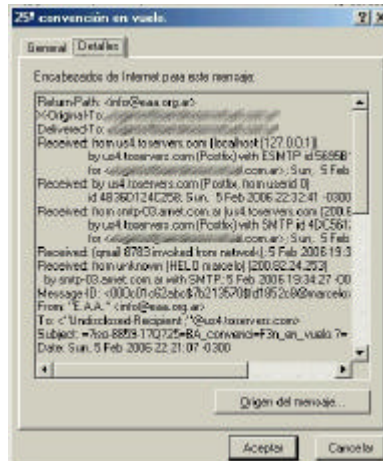
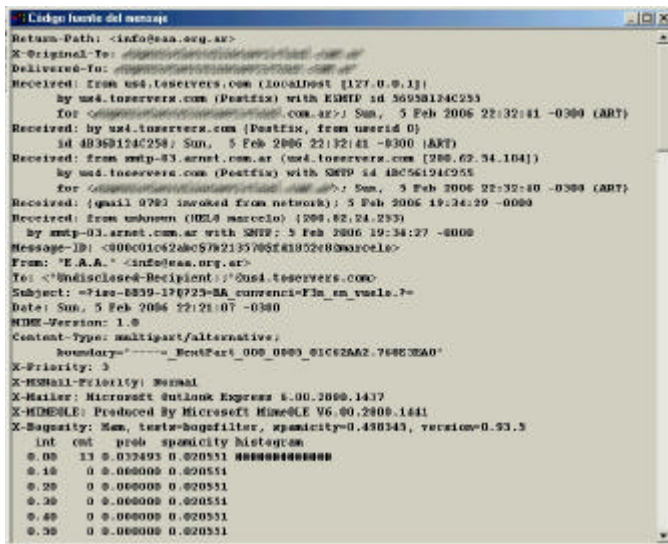


Fig. 2 – Ventana con los datos del mensaje, seleccionando la ventana “detalles”, accederemos a los encabezados ocultos.

SISTENET.COM.AR

Sin embargo, los datos en esta ventana suelen no ser lo suficientemente claros como para poder analizarlos en detalle, bastará con presionar el botón "Origen del mensaje...". Esto abrirá una nueva ventana en la que podremos observar el "mensaje crudo" como llega al servidor, con todos los encabezados completos, y el contenido del mensaje tal como luego lo descodificará el programa cliente de correo (en este caso Outlook Express), tal como se observa en la figura 3.



```
Return-Path: <info@xxx.org.ar>
X-Original-To: info@sistenet.com.ar
Delivered-To: info@sistenet.com.ar
Received: from us4.toservers.com (localhost [127.0.0.1])
  by us4.toservers.com (Postfix) with ESMTP id 5695B124C255
  for <info@sistenet.com.ar>; Sun, 5 Feb 2006 22:32:41 -0300 (ART)
Received: by us4.toservers.com (Postfix, from userid 0)
  id 4B36D124C258; Sun, 5 Feb 2006 22:32:41 -0300 (ART)
Received: from smtp-03.arnet.com.ar (us4.toservers.com [204.13.12.120])
  by us4.toservers.com (Postfix) with SMTP id 4DC56124C255
  for <info@sistenet.com.ar>; Sun, 5 Feb 2006 22:32:40 -0300 (ART)
Received: (qmail 8783 invoked from network); 5 Feb 2006 19:34:29 -0000
Received: from unknown (HELO marcelo) (200.12.24.30)
  by smtp-03.arnet.com.ar with SMTP; 5 Feb 2006 19:34:27 -0000
Message-ID: <000c01c62abc57b213570$fd1852c8@marcelo>
From: "E.A.A." <info@xxx.org.ar>
To: <"Undisclosed-Recipient;"@us4.toservers.com>
Subject: =?iso-8859-1?Q?25=BA_convenci=F3n_en_vuelo.?
Date: Sun, 5 Feb 2006 22:21:07 -0300
MIME-Version: 1.0
Content-Type: multipart/alternative;
  boundary="-----_NextPart_000_0005_01C62AA2.768E3EA0"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2800.1437
X-MIMEOLE: Produced By Microsoft MimeOLE V6.00.2800.1441
X-Spammy: Sun, text=bugfilter, spamcity=0.430343, version=0.33.5
Int  cnt  prob  spamicity  histogram
0.00  13  0.032493  0.020551  #####
0.10  0  0.000000  0.020551
0.20  0  0.000000  0.020551
0.30  0  0.000000  0.020551
0.40  0  0.000000  0.020551
0.50  0  0.000000  0.020551
```

Fig. 3 – Código fuente del mensaje.

En este ejemplo, el código fuente del mensaje nos muestra los siguientes encabezados (headers):

```
Return-Path: <info@xxx.org.ar>
X-Original-To: info@sistenet.com.ar
Delivered-To: info@sistenet.com.ar
Received: from us4.toservers.com (localhost [127.0.0.1])
  by us4.toservers.com (Postfix) with ESMTP id 5695B124C255
  for <info@sistenet.com.ar>; Sun, 5 Feb 2006 22:32:41 -0300 (ART)
Received: by us4.toservers.com (Postfix, from userid 0)
  id 4B36D124C258; Sun, 5 Feb 2006 22:32:41 -0300 (ART)
Received: from smtp-03.arnet.com.ar (us4.toservers.com [204.13.12.120])
  by us4.toservers.com (Postfix) with SMTP id 4DC56124C255
  for <info@sistenet.com.ar>; Sun, 5 Feb 2006 22:32:40 -0300 (ART)
Received: (qmail 8783 invoked from network); 5 Feb 2006 19:34:29 -0000
Received: from unknown (HELO marcelo) (200.12.24.30)
  by smtp-03.arnet.com.ar with SMTP; 5 Feb 2006 19:34:27 -0000
Message-ID: <000c01c62abc57b213570$fd1852c8@marcelo>
From: "Infobusiness" <info@xxx.org.ar>
To: <"Undisclosed-Recipient;"@us4.toservers.com>
Subject: =?iso-8859-1?Q?25=BA_convenci=F3n_en_vuelo.?
Date: Sun, 5 Feb 2006 22:21:07 -0300
MIME-Version: 1.0
Content-Type: multipart/alternative;
  boundary="-----_NextPart_000_0005_01C62AA2.768E3EA0"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2800.1437
X-MIMEOLE: Produced By Microsoft MimeOLE V6.00.2800.1441
(...)
```

De esta información, seleccionaremos los datos que están marcados, que es lo único que será de utilidad. Obviamente variarán de un caso a otro, pero en líneas generales siguen casi siempre la misma secuencia y con similares registros en el encabezado.

Buscaremos en primer lugar la información marcada con color rojo, que en este caso es la siguiente:

SISTENET.COM.AR

From: "InfoBussiness" <info@xxx.org.ar>
To: <"Undisclosed-Recipient:;@us4.toservers.com">
(...)
X-Mailer: Microsoft Outlook Express 6.00.2800.1437

Esta parte de los headers nos indica lo siguiente:

- ❖ El mensaje ha sido enviado utilizando la opción de "copia oculta" que permite el envío masivo sin revelar la lista de destinatarios (esta es una práctica recomendable, y que debería ser obligatoria para no violar el derecho a la privacidad de la información personal de los usuarios).
- ❖ La dirección de correo electrónico que el remitente "declara" como remitente es info@xxx.org.ar, aunque esto no quiere decir que realmente esta dirección sea la que utilizó para enviar el mensaje, puede ser "forzada" si se utilizaron programas de envío masivo.
- ❖ Más abajo, los headers nos indican que el mail fue enviado utilizando Outlook Express version 6.00.2800.1437.

Esta información nos orienta sobre quién nos envía el mensaje, y tendremos en cuenta estos datos cuando determinemos a través de qué proveedor de internet ha sido enviado el mensaje, que cotejaremos con los resultados.

La ruta de cada mensaje hasta llegar a su destino se va canalizando automáticamente a través de una secuencia de servidores que a modo de "postas" que se van retransmitiendo el mensaje sucesivamente.

Cada vez que un servidor recibe un mensaje, registra en el encabezado del mensaje esa recepción, agregando un campo "Received" en el que indica:

Desde qué servidor recibe el mensaje.
Identificador del mensaje (biunívoco).
Fecha y hora de recepción del mensaje.
Para qué recibe el mensaje (a quién está dirigido).

Observando los denominados "timestamp" (o marcas de hora) en que fueron recibidos los mensajes, el lector podrá observar que el primer "Received" es el que está más abajo en la lista de headers.

El primer "Received" normalmente lo registra el servidor en el que el remitente tiene su cuenta de correo, aunque a veces (si el remitente está en una red local que tiene un servidor de correo, puede ser que exista una recepción previa por el servidor local de correo, y recién luego será enviado al verdadero proveedor de e-mail).

En este caso observaremos el primer "Received" marcado en azul:

```
Received: from unknown (HELO marcelo) (200.12.24.30)
  by smtp-03.arnet.com.ar with SMTP; 5 Feb 2006 19:34:27 -0000
Message-ID: <000c01c62abc$7b213570$fd1852c8@marcelo>
```

Este registro nos permitirá determinar lo siguiente:

- ❖ El mensaje fue recibido de un servidor "desconocido" (unknown).
- ❖ Observamos un mensaje (HELO marcelo) que nos indica ni más ni menos que la identificación del ordenador del remitente.
- ❖ Luego observamos un URL o "dirección IP". La dirección IP es el primer dato importante que obtenemos de los headers, porque nos permitirán ubicar al proveedor de internet del remitente, a quien podremos reclamar. En este caso: 200.12.24.30 (obviamente esta dirección IP ha sido inventada para este ejemplo).
- ❖ Observamos inmediatamente la "firma" del servidor que recibió el mensaje (smtp-03.arnet.com.ar) y el protocolo empleado (SMTP).
- ❖ Luego el timestamp (5 de febrero de 2006 a las 19:34:27). "-0000" indica que la diferencia entre la hora GMT y la que está seteada en el servidor es 0.

SISTENET.COM.AR

- ❖ Finalmente, el identificador biunívoco del mensaje, que el administrador puede usar para ubicarlo en su sistema.

Tenemos pues, los primeros datos concretos en relación al origen del mensaje. Tenemos una dirección IP del mismísimo remitente (200.12.24.30) que el proveedor de internet del mismo podrá utilizar para identificarlo, y llegado el caso para sancionarlo por el delito cometido. (Generalmente esto sucederá recién después que el proveedor sea sancionado por Defensa del Consumidor o por una acción judicial).

Observemos ahora el siguiente registro importante, marcado en **verde**:

```
Received: from smtp-03.arnet.com.ar (us4.toservers.com [204.13.12.120])  
by us4.toservers.com (Postfix) with SMTP id 4DC56124C255  
for <info@sistenet.com.ar>; Sun, 5 Feb 2006 22:32:40 -0300 (ART)
```

Tal como ya lo indicamos antes, este registro lo ha agregado el segundo servidor por el que ha pasado el mensaje. La información concreta que aquí obtenemos es la siguiente:

- ❖ El mensaje fue recibido proveniente del servidor smtp-03.arnet.com.ar por el servidor us4.toservers.com con protocolo SMTP.
- ❖ El IP del servidor (no del usuario) que envía el mensaje sería 204.13.12.120 (este IP está modificado para el ejemplo por supuesto).
- ❖ Luego el servidor que recibe agrega una identificación.
- ❖ Finalmente indica para qué lo recibe (para ser entregado a info@sistenet.com.ar, y el timestamp (5 de febrero de 2006 a las 22:32:40 -300 tiempo de Argentina).

Con esta información procederemos al siguiente paso, que es ubicar los datos del proveedor de internet del remitente, que para toda latinoamérica obtendremos en www.lacnic.com, buscaremos en ese sitio de internet (NIC significa Network Information Center, es decir, Centro de Información de la Red) y LACNIC es el Centro de Información de la Red para Latino América y el Caribe.

Allí buscaremos el servicio "**whois**" y allí escribiremos el IP que encontramos en el encabezado. El sitio nos devolverá la información sobre la entidad administradora de ese IP (el responsable final), incluyendo una dirección postal, número de teléfono y también dirección de e-mail.

Buscaremos el registro "abuse" o similar, que será la dirección específicamente designada por el administrador para manejar casos de abuso como este.

Una vez establecido esto, ya sabemos adónde iniciar nuestro contacto.