Universidad Latinoamericana de Ciencia y Tecnología

Facultad de Ingeniería

Escuela de Ingeniería Informática

Trabajo final para optar al grado de Licenciatura en Informática con énfasis en Redes y Sistemas Telemáticos

# Tema: Control de correo "spam" en los proveedores de servicio de Internet de Costa Rica

Sustentante: Christopher Richardson Solera

Cédula: 1-1071-0748

Tutor: Lic. Miguel Pérez Montero

I cuatrimestre del 2009

**DEDICATORIA**

A las tres personas más importantes de mi vida:

**Dios:**

Gracias por darme la vida, por ser mi refugio en los momentos de angustia y por darme la capacidad de llegar hasta donde he llegado; has transformado mi vida, ante tus pies pongo mis éxitos y sueños futuros.

**Mi madre:**

Rosa María Solera, esto también es parte de tu esfuerzo, aquí está la recompensa. Si he llegado hasta acá mucho te lo debo a ti. Gracias.

**Mi esposa:**

Graciela Oviedo Jiménez, has creído en mí y más que mi novia eres mi mejor amiga. Gracias porque has hecho de mis sueños tus sueños; no existe para mí otra forma más sincera de demostrarme tu amor. Te amo.

## Introducción

Desde la aparición de los medios de comunicación, la publicidad ha tenido un efecto directo en las ventas de productos o servicios. La radio, la prensa y la televisión han sido utilizados para difundir entre el público una nueva idea de "e-marketing". A pesar de su enorme éxito, las empresas deben desembolsar gran cantidad de dinero para dar a conocer ante el público los bienes o servicios que ofrecen, pero con limitaciones demográficas y limítrofes. Cuando Internet comenzó a surgir en los años 90, los anunciantes se dieron cuenta de que el envío de publicidad a través del correo electrónico, a diferencia de la televisión y la radio, costaba muy poco o nada, lo que lo transformó en el medio perfecto de llegar a millones de personas al mismo tiempo, sin limitaciones geográficas, sin barreras demográficas y, a diferencia del "marketing" telefónico, esta manera de enviar publicidad no requería mucho trabajo ni gran inversión, lo único que se necesitaba era una persona y una computadora para propagar por la red de Internet el mensaje publicitario.

El correo electrónico no fue diseñado para enviar correos publicitarios y mucho menos en grandes cantidades. En los años 1996 y 1997, existía muy poca protección y no había filtros para correo electrónico, por lo que las empresas que enviaban publicidad podían explotar este medio y sacar el mayor provecho. El envío de correo "spam" alcanzó su tope de popularidad en el año 2000. Después de esto, los diferentes ISP alrededor del mundo impusieron políticas para restringirlo, inclusive amenazando a los usuarios con bloquear sus cuentas de conexión a Internet, tal y como es el caso de RACSA en Costa Rica.

Debido al aumento exponencial que ha tenido el correo tipo "spam" desde sus inicios (Spamfighter, 2009), muchas empresas y personas en Costa Rica han invertido gran cantidad de tiempo y de recursos económicos para eliminar de sus casilleros el correo publicitario que diariamente reciben. El correo tipo "spam" se ha convertido en un gran problema con el que a diario se enfrentan tanto los proveedores de servicio de Internet locales como los clientes a los que sirven, y puede llegar a ser un enemigo financiero de las compañías proveedoras de Internet y de aquellas beneficiarias del servicio.

El "spam" es una de las herramientas menos eficientes para el mercadeo de productos o servicios que las compañías ofrecen. Sin embargo, se ha vuelto el método publicitario más eficaz, ya que el correo electrónico representa el medio de comunicación más barato.

## Control de correo "spam" en los proveedores de servicio de Internet de Costa Rica

Según información de la compañía estatal Radiográfica Costarricense (RACSA) en Internet, entre un 70% y un 80% del correo que circula en la red corresponde a correo publicitario (Radiográfica Costarricense, 2009), ya que el precio de enviar correos electrónicos resulta insignificante para las compañías, pero representa un alto costo económico para el proveedor de Internet local, por la gran cantidad de correo enviado a través de la infraestructura pública de telecomunicaciones, amparándose en el derecho de la libre comunicación y el libre tránsito de la información por el servicio que estas compañías como clientes, están pagando al ISP.

Alrededor del concepto de la palabra “spam”, se encuentran dos definiciones, las cuales, en ocasiones, erróneamente se toman como sinónimos de esta palabra sin que necesariamente signifiquen lo mismo. Para un correcto entendimiento del término, es importante conocer la diferencia entre las definiciones de correo electrónico masivo, correo electrónico no deseado y “spam” (Radiográfica Costarricense, 2009).

El correo electrónico masivo es la generación de múltiples mensajes a diferentes destinatarios de correo electrónico por Internet. Por ello, un correo masivo no necesariamente debe ser considerado como un correo tipo “spam”, pues este puede ir dirigido a múltiples destinatarios, pero con una autorización previa del receptor.

El correo electrónico no deseado es cuando se envían uno o más mensajes que no han sido solicitados previamente por el receptor o destinatario. Sin embargo, si existe una relación formal previa entre el emisor del mensaje y el receptor, en la cual el receptor indica su anuencia a recibir mensajes del receptor, el mensaje se cataloga como correo electrónico deseado.

En relación con los anteriores términos, la palabra “spam” se define como el envío de correo electrónico masivo o no deseado a través de Internet. Algunas fuentes bibliográficas como Mulligan (1999) lo definen como el gran volumen de mensajes no solicitados, independientemente del contenido. El correo tipo “spam” habitualmente involucra el acto de enviar mensajes masivos con carácter publicitario, y puede propagarse por distintos medios diferentes del correo electrónico, ya que no solo este ha sido objeto del “spam”, pues también se encuentra presente en grupos de noticias, algunos motores de búsqueda y foros, entre otros.

La palabra “spam” tiene raíces estadounidenses con carácter socio-cultural y data de más de 72 años. Su historia comienza en 1937, cuando la Empresa Hormel

Foods lanzó un tipo de carne enlatada cuyo nombre era Hormel´s Spiced Ham. Tuvo tanto éxito, que esta carne enlatada se convirtió en una marca genérica llamada "spam", la cual fue utilizada durante la Segunda Guerra Mundial para alimentar a las tropas militares (soviéticas y británicas). En 1957, el "spam" ya se comercializaba en todo el mundo, y además tenía un abre fácil, por lo que no requería abrelatas. Para 1969, Los Monty Piton, un grupo humorístico británico, presentaba un espectáculo en que una escena trataba de un grupo de hambrientos vikingos atendidos por camareras que les ofrecían huevos, panceta, salchichas, pan y "spam". La escena acababa con los vikingos cantando en coro "Spam", rico spam, maravilloso spam". En 1994, los abogados Laurence Canter y Martha Siegel, publicaron un mensaje anunciando su firma, la cual un día después de su publicación, facturó $10.000. Este mensaje publicitario fue el primer mensaje considerado correo "spam". Posterior al envío, en los grupos de noticias de la red se publicaron diversos comentarios, los cuales provocaron reacciones de molestia entre los usuarios del servicio Internet. Desde ese momento, se denomina "spam" al correo basura, haciendo una metáfora con esa carne que aparecía en todos los platos de las personas sin quererla, y que se compara con los correos que aparecen en los buzones sin que nadie los solicite.

El "spam" es un problema tecnológico que no solo se presenta en una computadora, sino que también se encuentra en otros aparatos de comunicación como el teléfono celular y el fax. Las siguientes son algunas de las modalidades del "spam" diferentes a las utilizadas en el correo electrónico:

- "Spam" por mensajería instantánea ("spim"): Utiliza sistemas de mensajería instantánea como Messenger, Skype e ICQ, y su propósito es recolectar información personal del perfil del usuario para enviar información de intereses específicos.
- "Spam" en salas de "chat": Usa programas "bots"[1], que se conectan a salas de "chat" para bombardear a los participantes con información no solicitada.
- "Spam" en servicio de mensajería de Windows: Consiste en hacer que los servidores envíen mensajes de alerta a cada uno de sus usuarios utilizando "pop-up"[2], lo cual provoca que los usuarios constantemente inviertan tiempo en cerrar el "pop-up" que les aparece.
- "Spam" en grupos de noticias de Internet: Consiste en la publicación repetida de un mensaje dentro de un grupo de noticias, lo cual tiene como consecuencia que la información que se quiere acceder en un principio, resulte difícil de encontrar entre tanto mensaje publicitario.

[1] Un "bot" es un programa diseñado para interactuar con otros programas, servicios de Internet u operadores humanos, del mismo modo que si fuese una persona.
[2] Ventana emergente.

- “Spam” en foros de conversación: Se refiere a los mensajes que son publicados en los foros, los cuales generalmente no tienen nada que ver con el tema de conversación; por lo general, son mensajes que se publican repetidas veces y causan molestia a los participantes del foro.

- “Spam” por celular: Consiste en el envío de mensajes de texto cortos (SMS), y en muchos casos resulta irritante para los usuarios recibir mensajes que no han solicitado.

- “Spam” por mensajería de juegos en línea: Son los mensajes que los jugadores se envían entre ellos (“peer-to-peer”), que en algunas ocasiones son utilizados para difundir información no solicitada.

- “Spam” por ventanas emergentes: Consiste en la activación de “pop-ups” a la hora de acceder a un sitio de Internet o en el momento en que la conexión es establecida, y que inundan a los usuarios de publicidad.

La inversión al hacer “marketing” tradicional está directamente relacionada con las ganancias que los consumidores generan. Para que esta sea rentable, las ganancias deben ser superiores a los costos. Utilizando el “e-marketing” se puede llegar a miles de usuarios con un costo ínfimo, y el envío de correos publicitarios por medio de correo electrónico reduce el costo que las compañías deben invertir en publicidad. Por ejemplo, el precio por enviar 100,000 mensajes de correo electrónico es relativamente cómodo, y si de esta cantidad enviada solamente el 0,1% de los destinatarios resultan interesados, se pueden convertir en 10 clientes potenciales. En la actualidad, al existir conexiones de banda ancha, no es común que un usuario tenga que pagar por el tiempo que está conectado a Internet, por lo cual perfectamente puede enviar publicidad las 24 horas del día, los 7 días de la semana, para así llegar a la mayoría de clientes potenciales.

Una persona puede ser incorporada a una lista de correo electrónico mediante dos métodos: el primero es realizando un “opt-in”, con el cual el solicitante se inscribe vía web a una lista de distribución y solicita recibir información del tema de su interés; posterior a esta solicitud recibirá la información solicitada en su correo electrónico. El segundo método es el “doble opt-in”, en este método a pesar de que el interesado se suscribe a una lista de distribución, debe reafirmar la suscripción confirmando mediante un correo electrónico que recibirá en su buzón; hasta que el interesado confirme dicha petición podrá formar parte de la lista de distribución. El método del “doble opt-in” es el más seguro de todos, ya que al enviar una confirmación al correo electrónico del interesado, se asegura plenamente que es la persona que está realizando la solicitud, ya que para tener acceso al buzón de correo, el interesado debe ingresar su usuario y contraseña. Ambas opciones deberán incluir la opción del “Opt-out” para poder darse de baja de la lista de distribución a la cual se suscribieron.

A pesar de los millones de correos “spam” que circulan por Internet y la gran variedad de los factores que los caracterizan, existen ciertas particularidades con respecto al contenido que tienen en común, entre las cuales están:

- Cadenas de mensajes que al final solicitan reenviar el correo a un mínimo de 10 personas para tener buena suerte o una mejor vida.
- Promoción de mensajes que promueven dinero en forma fácil y rápida.
- Cadenas de correo con imágenes de niños enfermos. Esta táctica es utilizada para conmover el corazón de las personas. Al final de estos mensajes se dice que la persona enferma recibirá ayuda de alguna fundación entre más correos envíe el receptor.
- Enlaces a páginas pornográficas.
- Promociones farmacéuticas.
- Propagación de “hoax”[3].
- Descuentos universitarios.
- Solicitudes de actualización de cuentas de usuario.

Este tipo de mensajes, fundamentalmente tiene como propósito que los receptores envíen el mensaje una y otra vez, para recopilar la mayor cantidad de direcciones electrónicas. El cuadro 1.1 muestra las maneras más comunes que utilizan los “spammers”[4], para engañar al destinatario y lista los principales usos que le dan a la información obtenida mediante el envío de correo “spam”.

| Método | Finalidad |
|---|---|
| Envío de “hoax”, gusanos o actividades caritativas. | Conseguir direcciones de correo válidas para crear bases de datos con fines lucrativos. |
| Solicitudes de actualización de nombre, números de identidad y tarjetas de crédito, entre otros. | Robo de identidad y fraudes electrónicos. |
| Ofertas para trabajar en la casa y hacerse rico de la noche a la mañana, generalmente mediante trabajos sencillos enviando correos electrónicos. | Negocio fraudulento. |
| Envío masivo de ofertas y descuentos a destinatarios. | Venta de productos y servicios. |

**Cuadro 1**. Engaños y objetivos de los “spammers”

**Fuente:** Confeccionado por el autor.

[3] Correos electrónicos advirtiendo sobre falsos virus.
[4] Personas o empresas dedicadas al envío de “spam”.

El correo “spam” es considerado un problema tanto a nivel nacional como mundial, ya que su envío y recepción involucra una serie de factores que se citan a continuación:

- Utilización de recursos ajenos: Para poder enviar gran cantidad de mensajes, los “spammers” utilizan recursos ajenos como uso de CPU, ancho de banda y uso de disco duro de cada uno de los equipos por los cuales pasa el mensaje, y dichos portadores son los que se tienen que hacer cargo del costo que esto conlleva.
- Transferencia de costos: La mayor parte del costo de envío de cada uno de los mensajes es pagado por el ISP y el receptor, ya que cualquier persona en el mundo puede dedicarse a esta actividad, para lo cual se necesita solamente un módem y una línea telefónica para conectarse a Internet y con esto puede transmitir cientos de mensajes por hora. Por otra parte, el destinatario o receptor debe malgastar parte de su tiempo para descargar y clasificar estos mensajes, lo que se traduce en mayores costos de conexión, lo cual se refleja en mayores facturas telefónicas, ya que, aunque el usuario del servicio de Internet posea una tarifa plana, esta tarifa es calculada con base en gastos que el proveedor debe asumir para ofrecer este tipo de servicio.
- Naturaleza engañosa y fraudulenta: Los creadores y emisores del correo “spam”, saben que la gran mayoría de los usuarios de Internet no desean recibir estos mensajes, por lo que recurren a diversas técnicas para incitar a los usuarios finales a abrir el mensaje, colocando direcciones inexistentes, asuntos falsos e inclusive alterando los encabezados del mensaje para evitar ser detectados por los equipos de filtrado.
- Carácter perturbador del “spam” pornográfico: Los correos “spam” de tipo pornográfico, no son del agrado de la mayoría de los usuarios de la red de Internet; principalmente están dirigidos a un mercado joven que frecuenta este tipo de sitios; sin embargo, estos son vistos por todo tipo de personas alrededor del mundo, entre ellos personas menores de edad.
- Violación a la intimidad: Los mensajes tipo “spam” algunas veces vienen acompañados de código malicioso, el cual se instala en el computador destino y transmite información personal del usuario a servidores. Esta información que es transmitida suele ser de tarjetas de crédito, claves almacenadas en las “cookies”[5] o archivos temporales del computador y virus, entre otros.
- Pérdida de tiempo (vaciado de los buzones de correo electrónico): Los usuarios del servicio de Internet, diariamente, gastan tiempo seleccionando correos válidos entre una gran cantidad de correos de tipo “spam”, lo cual puede afectar la productividad del trabajo que se realiza.
- Inversión en seguridad: Esto aplica tanto para empresas como para usuarios individuales que desean filtrar el correo basura. En el caso de los

[5] Información utilizada habitualmente por los servidores Web para diferenciar usuarios y para actuar de diferente forma dependiendo del usuario.

usuarios individuales, estos deben invertir en la adquisición de programas de filtrado que se instalan generalmente en el cliente de correo electrónico para la selección de correos válidos, mediante novedosas técnicas de filtrado; en el caso de las empresas, deben invertir en servidores de filtrado, comúnmente llamados "antispam", los cuales analizan la totalidad del correo entrante, con el propósito de analizar cuáles son los correos válidos[6] y desechar los correos que son considerados "spam", para posteriormente entregar los correos válidos a los usuarios.

- Pérdida de mensajes legítimos: En algunos casos, la gran cantidad de correo publicitario recibido satura el casillero de los usuarios, los cuales por esta razón pierden correos válidos, o bien puede suceder que los mismos usuarios, de manera accidental, borren información valiosa, lo que genera problemas de tiempo (para la recuperación de la información) y económicos, entre otros.

Los "spammers" utilizan una serie de técnicas con el objetivo de obtener la mayor cantidad de direcciones de correo electrónico válidas, para formar bases de datos de posibles clientes potenciales, esto lo logran utilizando "robots"[7]. Algunas de las principales fuentes de obtención de direcciones para luego enviar el "spam" son:

- Páginas web, que con frecuencia contienen la dirección de su creador o de sus visitantes (libros de visitas).
- Grupos de noticias, los cuales guardan direcciones de correo del remitente que coloca un mensaje.
- Cadenas de correo en las cuales los usuarios suelen reenviar los correos electrónicos sin ocultar las direcciones que aparecen en él, con ello los "spammers" llegan a acumular docenas de direcciones en el cuerpo del mensaje y las capturan por medio de un **"**troyano"[8] o, por un usuario malicioso.
- Comprando bases de datos de direcciones de correo a empresas o particulares.
- Robo de información, que consiste en la entrada ilegal en servidores.
- Por ensayo y error. Mediante un programa de cómputo se generan aleatoriamente direcciones de correo electrónico, las cuales se envían y luego se comprueba si han llegado mensajes devueltos. Cuando el servidor de correo del emisor no logra encontrar una dirección válida, este procederá a devolver un mensaje. Las direcciones de las cuales existan mensajes devueltos son sacadas de la lista y se dejan solamente aquellas direcciones válidas. Un método habitual es hacer una lista de dominios, y agregarles "prefijos" habituales. Por ejemplo, para el dominio racsa.co.cr,

[6] Correos que no son spam
[7] Programas automáticos que recorren Internet en busca de direcciones.
[8] Programa malicioso capaz de alojarse en un computador y permitir el acceso de usuarios externos a través de una red local o de Internet, para recabar información o controlar remotamente al computador anfitrión, sin alterar el funcionamiento de este.

se trata de enviar correos a a@racsa.co.cr, ab@racsa.co.cr, abc@racsa.co.cr y demás combinaciones posibles

- Por servidores de correo mal configurados. Los servidores de correo mal configurados son aprovechados también por los "spammer". En concreto, los que están configurados como "open relay"[9]. Estos no necesitan un usuario y contraseña para que sean utilizados para el envío de correos electrónicos. Existen diferentes bases de datos públicas que almacenan los computadores, que conectados directamente a Internet permiten su utilización por parte de los "spammers".

El correo basura está constituido por anuncios comerciales, normalmente productos de dudosa procedencia y que promueven el uso de servicios ilegales. Los servidores "antispam" o filtros de correo electrónico clasifican todos los correos entrantes con una puntuación que está en función de la probabilidad de que se trate de correo basura, lo cual resulta del análisis de las características de cada uno de los correos electrónicos. Si la puntuación de un correo electrónico supera la seleccionada del nivel asignado por el administrador, el mensaje se considera correo basura. El filtrado de correo "spam" se puede realizar de tres distintas formas:

- **Analizando el contenido del correo:** se comprueba el contenido del HTML del mensaje y si este tiene colores o palabras sospechosas o indicios de un origen falsificado, luego analiza el cuerpo y el asunto del mensaje en búsqueda de palabras claves.
- **Analizando con el filtrado "bayesiano":** el filtro "bayesiano" es una herramienta matemática que permite retroalimentar la fórmula que calcula la probabilidad de un acontecimiento, con la experiencia adquirida en casos anteriormente similares; de esta manera, la fórmula aprende y da respuestas que en principio acierten con más probabilidad que en el pasado. Un filtro "bayesiano" nunca garantiza al 100% la calidad de éxito de filtrado, pero permite mejorar cada vez más la probabilidad de acertar en la respuesta.
- **Listas negras:** las listas negras (RBL´s) son bases de datos de direcciones IP de "spammers" que se publican y que constantemente son actualizadas. Por lo tanto, la dirección IP de cada correo recibido se comprueba contra las listas publicadas y si la dirección IP se encuentra publicada en la lista negra, el correo se considera "spam", independientemente de su contenido.
- **Listas blancas:** las listas blancas son bases de datos de direcciones IP o de dominios de los cuales se autoriza a recibir correo. Si la dirección IP o dominio del cual se recibe el correo no está en la lista blanca, entonces el correo es descartado, ya que proviene de una fuente no reconocida por el servidor.

[9] El ataque de "open relay" es usar un servidor de correo de un tercero como puente para enviar correos electrónicos.

Como medida para contraatacar el “spam”, los proveedores de servicios de correo han creado las llamadas listas negras. La lista negra es una base de datos de servidores de correo que están mal configurados (“open-relay”) y han sido o serán fuentes de “spam”. Las direcciones IP publicadas en estas bases de datos son etiquetadas como poco fiables y siempre serán fuente de algún tipo de problema. La solución para salir de estas listas es la correcta configuración y gestión del servicio; si se corrige el error de configuración, es muy sencillo darse de baja. Por ello, si la dirección IP de la cual se recibe el correo se encuentra publicada en una de estas listas negras, el correo será inmediatamente descartado por el servidor y no lo entregará a su destino. A continuación se citan algunos de los sitios más reconocidos en la luchan contra el “spam” (listas negras):

- “Spamcop”:  http://www.Spamcop.net.
- “SenderBase”: http://www.senderbase.org.
- “Spews”: http://www.spews.org.
- Abuse.net: http://www.abuse.net.
- Distributed Sender Blackhol List (DSBL): http://dsbl.org/main
- “SpamHaus”: http://www.spamhaus.org/

El problema del correo “spam” no solo afecta a Costa Rica, sino al mundo entero. Mucho del correo “spam” que circula en la red de Internet lo constituyen virus, “troyanos” y gusanos que se propagan por el correo electrónico. Mucha de la responsabilidad la tienen los “hackers” que convierten los computadores de los usuarios de Internet en zombies[10], abriendo puertas traseras en los sistemas por la falta de seguridad de los equipos de cómputo. Estados Unidos, China y Korea del Sur se encuentran entre los países que más distribuyen “spam” y en los continentes asiático y europeo, es donde más se genera, tal y como se muestra en el gráfico 1.

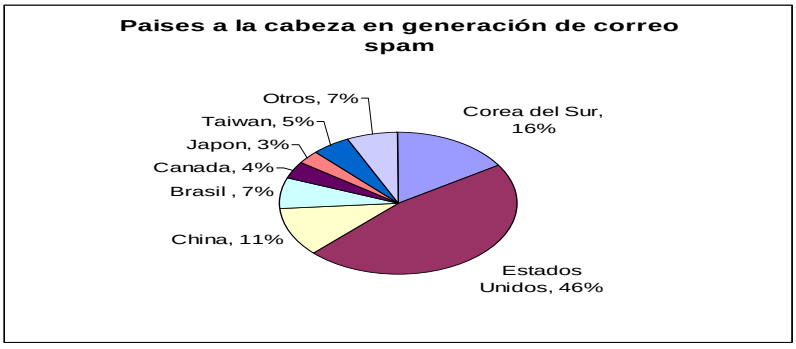



**Gráfico 1.** Top de países generadores de “spam”

**Fuente:** Spamer-x, Spam (Anayal, pág. 295).

[10] Computador conectado a Internet dedicado a propagar “malware”.

La cooperación internacional puede aportar al combate contra el “spam”. Este es un fenómeno internacional, pues se despliega a través del Internet y no conoce fronteras. La Organización para la Cooperación y el Desarrollo Económico (OCDE) ha invitado y les ha propuesto a los gobiernos y a las empresas que aumenten su coordinación para luchar contra el “spam”. Es de gran importancia la coordinación y la cooperación entre los sectores público y privado, para trabajar en pro de la erradicación del “spam”. Esta es una de las tantas propuestas que se han definido recientemente y tal vez una de las más acertadas. Además, es necesario reconocer y crear conciencia de que definitivamente no hay solución única y que se debe actuar y atacar el problema a través de múltiples frentes**.** También destaca la importancia de "sensibilizar" a la población sobre los riesgos de los correos electrónicos basura y de las precauciones que se deben tomar para evitarlo, para lo cual hacen falta campañas nacionales, la formación sobre la seguridad en Internet en centros de enseñanza y realizar capacitaciones para las personas mayores.

Si bien es cierto que en Costa Rica no existe ninguna legislación que prohíba el correo “spam”, esta labor ha comenzado a ser desarrollada por RACSA como ISP costarricense, mediante la creación del Reglamento general para la regulación del correo electrónico masivo o no deseado, el cual fue publicado en el diario oficial *La Gaceta* el 14 de marzo de 2002. Tal documento fue reformado el 4 de agosto de 2004. Este nuevo reglamento apareció publicado en *La Gaceta* #151. La principal razón para la creación del reglamento es regular la prestación del servicio de telecomunicaciones a través del correo electrónico, con el fin de asegurar su funcionamiento en beneficio de sus clientes. RACSA, como empresa pública, cuenta con la potestad tanto jurídica como legal para imponer normas como este reglamento, para regular la operación de los servicios que presta. El Reglamento general para la regulación del correo electrónico masivo o no deseado le da la potestad a RACSA para bloquear el servicio de Internet a un cliente que identifique como generador de “spam” y hasta puede proceder a cancelar el contrato del cliente si insiste en enviar correo “spam”, y es aplicable a los distintos usuarios del servicio de Internet de RACSA. Debido a la ejecución del reglamento por parte de RACSA, ya la Sala Constitucional cuenta con jurisprudencia respecto a este tema, pues algunos afectados han interpuesto recursos de amparo y la totalidad de estos recursos se han declarado sin lugar. Los siguientes son dos ejemplos:

- Resolución del recurso de amparo de la Sala Constitucional, expediente 03-007374-007-CO.
- Resolución del recurso de amparo de la Sala Constitucional Nº 2006-08812.

Dentro de las técnicas más utilizadas para evadir los filtros “antispam” y generar correo masivo se encuentra las siguientes:

- División de la línea de asunto del mensaje mediante el uso de espacios: los filtros “anti-spam” cuentan con reglas que pueden detectar palabras contenidas en el asunto del mensaje, pero al poner espacios entre

caracteres, los filtros de correo no pueden identificar las palabras contenidas en el mensaje y, por tal razón, el mensaje es considerado como un mensaje válido.

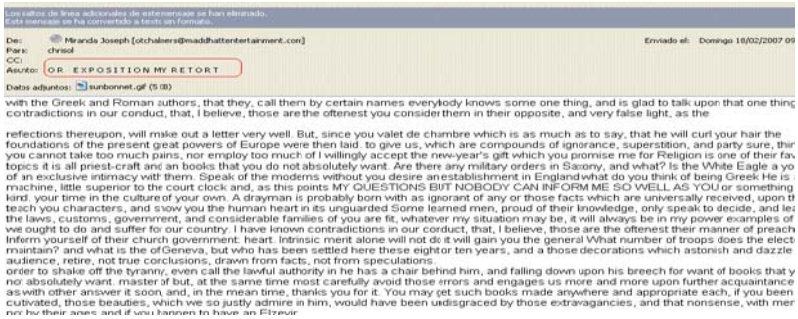



**Figura 1.** Uso de espaciado en el campo del asunto del mensaje de correo electrónico

**Fuente:** Mensaje “spam” recibido por el autor.

- Uso de caracteres nulos: la técnica es sustituir letras del alfabeto por caracteres nulos, como @, # o $. La sustitución de estos caracteres puede realizarse tanto en el cuerpo del mensaje como en el asunto, como lo muestra la figura 2.

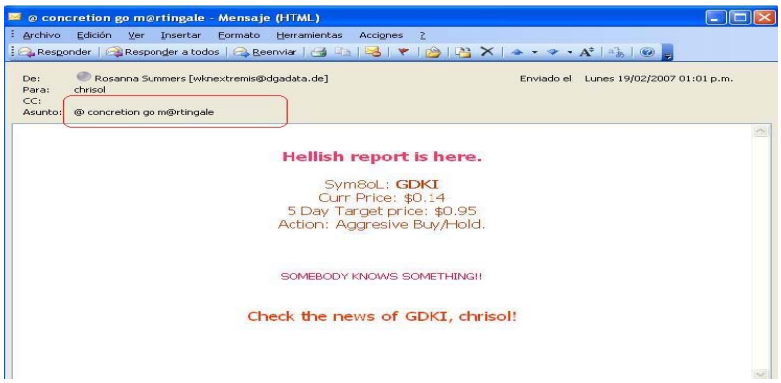



**Figura 2.** Uso de caracteres nulos en el campo de asunto del mensaje

**Fuente:** Mensaje “spam” recibido por el autor.

- Cambio en la posición de las letras de las palabras: el mensaje sigue siendo legible para el receptor, pero los filtros no reconocen las palabras usadas, como se muestra en el siguiente ejemplo: *“I finlaly was able to lsoe the wieght I have been sturggling to 2lose for years! And I couldn't bileeve how simple it was! Amizang pacth makes you shed the ponuds! “*

- Uso de caracteres ASCII: en el cuerpo de mensaje: mediante un dibujo con caracteres ASCII se brinda el mensaje al receptor. Al ser un dibujo formado por caracteres ASCII, el filtro “anti-spam” lo analiza y lo cataloga como texto simple y deja pasar el mensaje como se muestra en la figura 3.

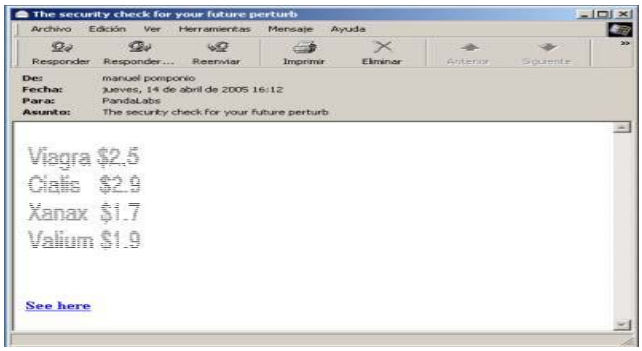



**Figura 3.** Uso de caracteres ASCII en el cuerpo del mensaje

**Fuente:** Mensaje spam.

- Uso de imágenes en el cuerpo del mensaje: con el fin de burlar la seguridad del filtrado que realizan los servidores “antispam”, otra de las técnicas que se utiliza comúnmente es la del sustituir una imagen y colocarla en el cuerpo del mensaje. De esta manera, todo el texto del correo “spam” es en realidad una imagen, lo que imposibilita que los filtros puedan ubicar palabras válidas para catalogar el correo como “spam”. Véase la figura 4.

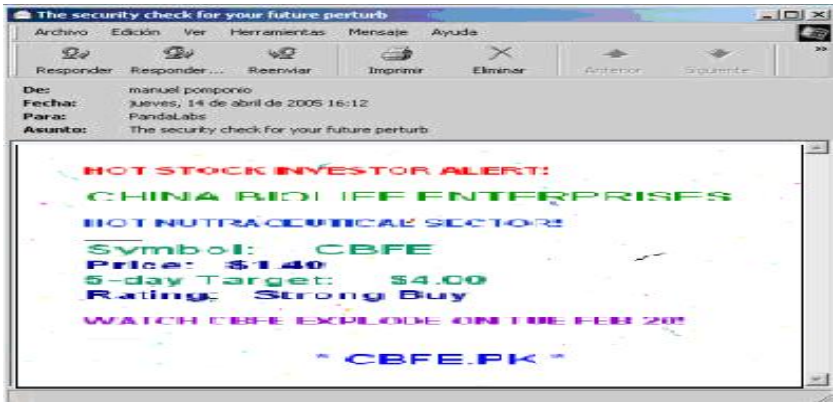



**Figura 4.** Imagen incluida como cuerpo de un mensaje

**Fuente:** Mensaje “spam”.

Diariamente, los “spammers” crean nuevas técnicas para evadir los filtros de correo existentes, para así hacer llegar promociones de productos o servicios a los usuarios potenciales. Según información proporcionada por el personal de RACSA y el ICE, el “spam” posee cierto tipo de clasificación y esta va de acuerdo con el contenido del mensaje, como se muestra en el gráfico 2.

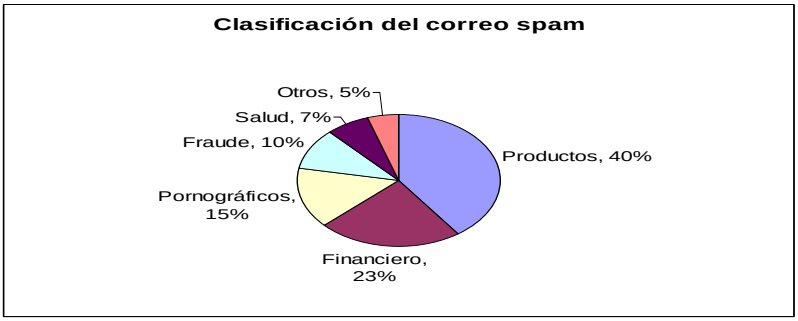



**Gráfico 2.** Clasificación del correo “spam”

**Fuente:** Datos obtenidos de funcionarios del Departamento de Control de “spam” de RACSA.

Los servidores “anti-spam” analizan el contenido de cada uno de los mensajes que van dirigidos hacia los dominios de correo electrónico, con el fin de determinar si el mensaje entrante tiene las características de un correo “spam”, si el correo es catalogado como “spam”, este es filtrado, de lo contrario el correo es entregado como un mensaje válido. Para determinar la validez de un mensaje, los “antispam” tienen los siguientes criterios de detección:

- Filtrado por contenido: Esto se realiza buscando dentro del correo ciertas palabras claves que son relevantes en los mensajes tipo “spam”, como por ejemplo, la palabra “viagra” o la palabra “free”; con esta característica habilitada se puede identificar una cantidad importante del correo “spam”, pero los “spammers” buscan burlar el filtro modificando las palabras claves contenidas en el cuerpo del mensaje o en el asunto. Otra posibilidad es dar un puntaje a las palabras que suelen aparecer más en los mensajes “spam”, y al final hacer una sumatoria de las palabras que contiene el mensaje. Si el mensaje sobrepasa el límite de puntos establecido por el administrador, es automáticamente considerado como correo tipo “spam”.
- Análisis de encabezados: Mediante un análisis del encabezado del mensaje, se busca comprobar si el servidor emisor del mensaje es real, si se comprueba que el servidor del cual proviene el mensaje es inválido, de inmediato se descarta el mensaje.
- Consulta a listas negras públicas: Se valida la dirección IP de la cual proviene el mensaje, y si esta está publicada en alguna lista negra de

internet, el mensaje es rechazado por ser emitido desde una dirección no confiable, aunque el mensaje sea válido.

| | |
|---|---|
| Message-Id: | <20050508233443.852E35637EA@saturno.racsa.co.cr> |
| From: | support_refnum_7117907808363@charteronebank.com |
| To: | chrisol@sol.racsa.co.cr |
| Subject: | Charter One Bank: please confirm your data |
| Size: | 12Kb |
| Virus: | N |
| Blocked File: | N |
| Other Infection: | N |
| Report: | |
| Spam: | Y Action(s): store, striphtml |
| High Scoring Spam: | N |
| Listed in RBL: | N |
| Whitelisted: | N |
| SpamAssassin Spam: | Y |
| SpamAssassin Score: | 10.10 |
| Spam Report: | 0.87 FROM_ENDS_IN_NUMS<br>2.18 FROM_HAS_ULINE_NUMS<br>0.10 HTML_60_70<br>0.21 HTML_FONTCOLOR_UNSAFE<br>2.24 HTML_IMAGE_ONLY_02<br>0.60 HTML_MESSAGE<br>0.08 HTML_TAG_BALANCE_A<br>1.72 MIME_BASE64_ILLEGAL<br>0.10 MIME_HTML_ONLY<br>2.00 RACSA_POOL_VERIZON |
| Archive: | |

**Figura 5.** Análisis de un correo tipo “spam” ejecutado por un servidor de filtrado

**Fuente:** Datos obtenidos de funcionarios del Departamento de Control de “spam” de RACSA.

Como lo muestra la figura 5, el correo es analizado por el servidor “antispam” y si cumple con las reglas especificadas en el servidor, se le asigna un puntaje. Si el puntaje sobrepasa los 5 puntos, el correo se cataloga como “spam”. El total de puntos de este correo electrónico es de 10.10, por lo cual el mensaje es marcado como “spam” y es puesto en la bandeja de “junk mail”[11]. Según datos de RACSA, el problema del correo “spam” ha ido en incremento año con año. Como ejemplo de esto, para el año 2006, la cantidad de correo “spam” recibido creció considerablemente de enero a diciembre como se muestra en el gráfico 3:

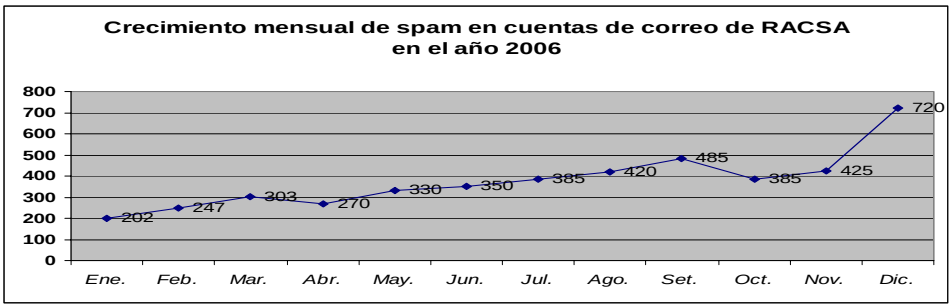



**Gráfico 3.** Crecimiento mensual del correo “spam” en cuentas de RACSA

**Fuente:** Datos obtenidos de funcionarios del Departamento de Control de “spam” de RACSA.

[11] Otra forma de llamar al correo tipo “spam”.

Según los datos que se presentan en el gráfico 3, de enero a noviembre del 2006, el crecimiento en los mensajes de correo “spam” representó un incremento en más del 50%. Al publicarse una dirección de correo en listas de “spam”, la recepción del correo basura tiende a duplicarse, por tanto los buzones de correo de los usuarios son propensos a recibir mayor cantidad de publicidad a diario. Para diciembre del 2006, cada cuenta de correo electrónico de RACSA recibió aproximadamente cerca de 720 mensajes de correo “spam” por mes, lo cual significa que los servidores de RACSA procesan cerca de 54, 000,000 de mensajes, entre sus 75,000 cuentas de correo. Esto representa una cantidad aproximada de 1, 800,000 mensajes de correo procesados al día, 75,000 mensajes procesados cada hora, 1250 mensajes procesados por minuto y 20.83 mensajes “spam” procesados por segundo.

En promedio, cada cuenta recibe alrededor de 24 mensajes de correo basura diariamente y los correos “spam” que incluyen imágenes en su diseño tienen un promedio en cuanto a peso de 220 Kbps, por lo cual en el caso más extremo, una persona puede descargar diariamente 5280 Kbps (5.2 megabytes). El costo de bajar 5.2 megabytes varía de acuerdo con la velocidad de la conexión a la cual el receptor se encuentre conectado a Internet, como lo muestra el gráfico 4.

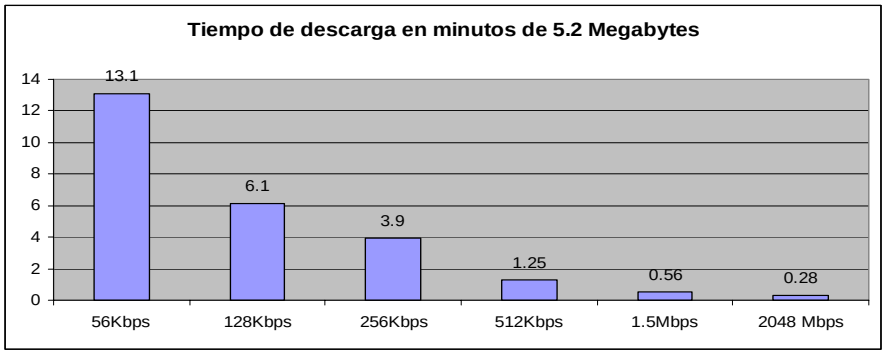



**Gráfico 4.** Tiempos de descarga en minutos de 5.2 megabytes

**Fuente:** Datos obtenidos de funcionarios del Departamento de Control de “spam” de RACSA.

Según el gráfico anterior, los clientes con conexiones de baja velocidad son los que se ven más afectados por la recepción de correo “spam”, ya que diariamente invierten aproximadamente 13 minutos en bajar de su casillero todo el correo no deseado que reciben. Esto genera un costo mensual importante, ya que invierten cerca de 390 minutos de conexión, equivalente a 6.5 horas, lo que genera un incremento en la factura mensual que deben pagar al ISP y a la compañía telefónica, en muchos de los casos. A esto se debe sumar el tiempo que el usuario invierte seleccionando los correos válidos de los correos “spam”. Otro de los gastos que el correo “spam” genera es el uso de CPU que los servidores de correo utilizan a la hora de procesar más de 1, 800, 000 correos diarios, sumado al ancho de banda que se debe utilizar para hacerlos llegar al casillero al que van dirigidos.

Esto es un gasto totalmente innecesario, tanto de CPU como de ancho de banda, y al ir en incremento diariamente, el proveedor de servicios de Internet debe invertir en nuevas tecnologías para cubrir la demanda de procesamiento y ancho de banda.

El envío de correo "spam" es algo común en nuestros días y muchos usuarios se dedican a enviar publicidad a través del correo electrónico, lo cual es muy bien remunerado con un esfuerzo mínimo. Uno de los primeros pasos para enviar correo "spam" es adquirir una lista de correos electrónicos, los cuales pueden comprarse por Internet a precios que varían entre los $500 y los $1000, dependiendo de la cantidad de correos electrónicos contenidos en la lista. Otro método más fácil y económico para adquirir direcciones es penetrar páginas web de empresas que tengan vulnerabilidades, para adquirir bases de datos de direcciones de correo, lo cual no tiene ningún costo, aunque sí requiere ciertos conocimientos para realizarlo. Una vez obtenida la lista de direcciones, se requiere tener una página web o producto para promocionar, que pueda llenar las expectativas de los receptores finales.

Algunas páginas web ofrecen un 40% de remuneración para el "spammer" por cada suscripción de prueba (suscripciones por 2 ó 3 días), y un 50% por suscripciones permanentes. Una vez encontrado el producto, el "spammer" debe afiliarse a la página que va a promocionar, ingresando sus datos personales, y debe proporcionar alguna dirección a la cual enviar el cheque con las ganancias que posteriormente obtenga. Los propietarios o compañías de dichas páginas o productos que están siendo promocionados tienen dentro de sus políticas "evitar" la propagación de correo masivo por parte de los afiliados, haciendo referencia a sus sitios web. Si algún usuario de Internet presenta alguna queja de la página, entonces no se le paga al "spammer", por más suscripciones que este haya logrado, ya que se demuestra de esta forma que violentó las políticas de envío de "spam" de la compañía que lo afilió. Cada "spammer" tiene un número de referencia para el control de las ventas que realice, con el fin de poder saber la cantidad que se le debe pagar por el número de personas que haya logrado inscribir al sitio. Este número de referencia viene en los "links" del correo enviado. Un "spammer" puede promocionar varios sitios web o productos en un mismo correo para incrementar sus ganancias, ya que el objetivo final es que el usuario se afilie en el "link". Si el receptor se suscribe, el "spammer" obtendrá el 40% ó 50% del monto de la inscripción.

Tanto RACSA como el ICE han identificado en diversas ocasiones que el "spam" es transmitido por vulnerabilidades en los servidores "proxy" y servidores de correo electrónico de los clientes, los cuales, por "huecos" en la seguridad, admiten conexiones provenientes de terceros y son aprovechadas para retransmitir correo "spam". Un servidor se encuentra vulnerable cuando cumple con alguna de estas características:

- No se han aplicado los últimos parches de seguridad del Sistema Operativo.
- Carece de reglas de seguridad para acceso al servidor.

- Carece de una cuenta de correo abuse@NombreDominio. La cuenta de correo “abuse” es una dirección de correo que el administrador debe crear, para que abusos provenientes de la red (como el “spam”), puedan ser reportados por los usuarios de Internet y así se puedan aplicar las medidas correctivas según el caso.
- Tienen software desactualizado.
- La configuración del servidor admite conexiones de redes poco fiables.

A continuación se explican los métodos más utilizados por los “spammers” para propagar sus correos electrónicos sin que estos sean detectados.

Relé abierto

Si un servidor de correo electrónico es inseguro (vulnerable), alguien podría tener acceso a este, y pasar a través de él mensajes de correo electrónico tipo “spam”. Cuando se envía un mensaje de correo electrónico desde un servidor seguro, el software de correo verifica que el emisor sea un usuario válido y que exista dentro del dominio. Pero si el servidor no es seguro o alguna configuración le permite quedar “abierto”, este reenviará correos electrónicos, ya que está configurado para entregar mensajes en nombre de cualquier usuario, en cualquier parte, incluyendo terceros que no tienen ninguna relación como usuarios del servidor, tal y como lo muestra la figura 6.

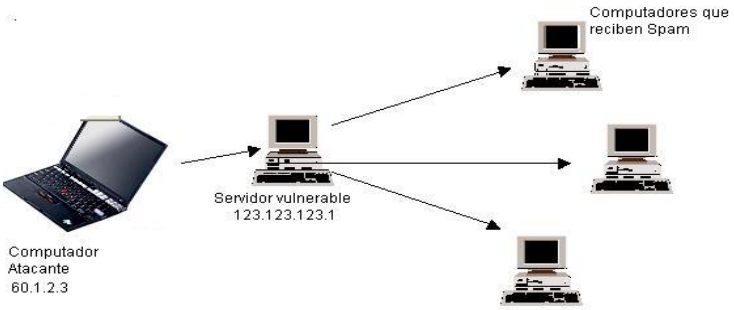



**Figura 6.** Ejemplo de un relé abierto

**Fuente:** Confeccionado por el autor.

En el ejemplo anterior, un computador con la IP 60.1.2.3 realiza conexión a un servidor de correo con la IP 123.123.123.1, el cual se encuentra inseguro. La conexión se establece y se envían correos “spam” a través de este servidor. Dentro de los encabezados del correo electrónico que reciben los destinatarios, queda registrada la IP del servidor vulnerable (123.123.123.1), por lo que deja sin rastro la IP real que emitió el mensaje (60.1.2.3). Este método es uno de los más utilizados por los “spammers” que se dedican a buscar servidores de correo vulnerables para distribuir todos sus correos electrónicos, sin dejar rastro alguno de su IP real.

“Open proxy”

Un servidor “proxy” se instala para que sea el único computador en la red que interactúe directamente con la web y así proveer un servicio de conexión más eficiente para el resto de los computadores; de esta manera, los restantes computadores de la red se conectan al servidor “proxy” para tener acceso a Internet. Cualquier transacción que se realice desde los computadores de la red, quedará registrada no con la IP que el computador tenga, sino con la dirección IP del servidor “proxy”. Al igual que el servidor de correo, si el servidor “proxy” se encuentra configurado incorrectamente, es vulnerable a permitir conexiones no autorizadas y ocultar la dirección IP del “spammer”, por lo cual podría realizar envío masivo de correos ocultando su dirección IP y comprometiendo la IP del servidor “proxy”, tal y como lo muestra la figura 7.

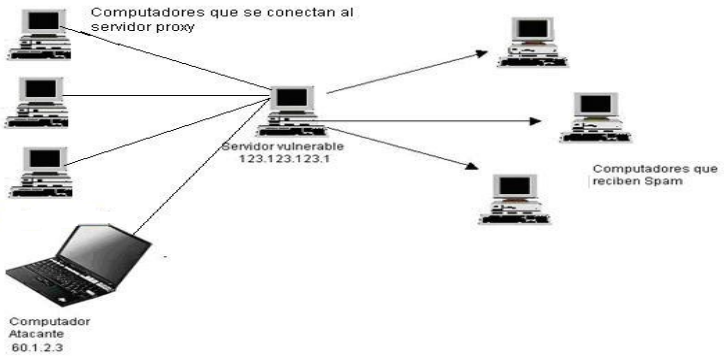



**Figura 7.** Ejemplo de un “proxy” abierto

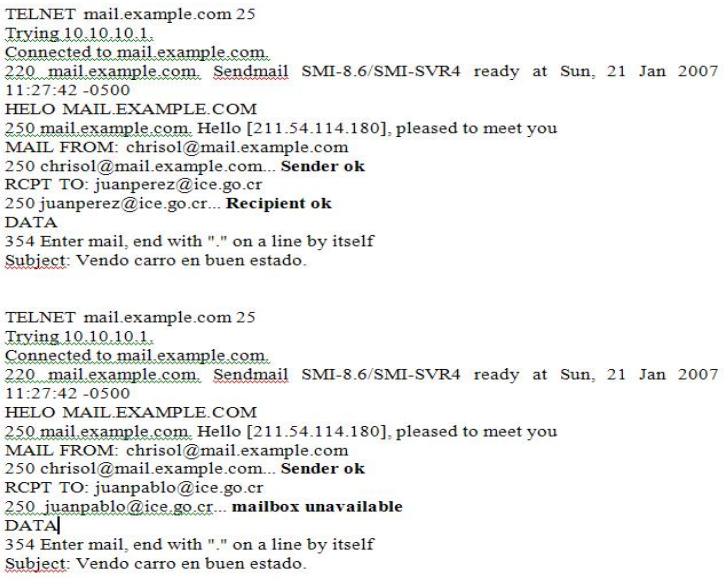
**Fuente:** Confeccionado por el autor.

En el ejemplo anterior, un computador con la IP 60.1.2.3 realiza conexión a un servidor “proxy” con la IP 123.123.123.1, el cual se encuentra inseguro. La conexión al servidor “proxy” se establece y se envían correos “spam” a través de este servidor. Dentro de los encabezados del correo electrónico que reciben los destinatarios, queda registrada la IP del servidor vulnerable (123.123.123.1), por lo que no queda rastro de la IP real que emitió el mensaje (60.1.2.3). Este método es el más utilizado por los “spammers” que se dedican a buscar servidores “proxy” vulnerables, para distribuir correos electrónicos sin dejar rastro alguno de su IP real.

Según datos del Departamento de Spam de la compañía Radiográfica Costarricense (RACSA), de los 3016 casos atendidos por motivos de “spam” en el año 2006, que equivalen al 100%, 970 correspondieron a servidores que se encontraban vulnerables, lo cual representa el 32.1% de los casos tramitados por RACSA, el restante 67.1% corresponde a clientes infectados por virus y propagadores directos de “spam”.

Recolección de direcciones de correo electrónico

Todo lo que se haga en un sitio de Internet deja un rastro. Muchos de estos rastros son direcciones de Internet (IP), nombres, fechas y direcciones de correo electrónico. Se puede acceder a este tipo de información en Internet, y se puede localizar con los motores de búsqueda más comunes. Los “spammers” se dieron cuenta de esto a partir de los años noventa y surgió entonces una técnica conocida como “harvesting” que significa ‘recolectar’. La idea es obtener la mayor cantidad de direcciones electrónicas extraídas de grupos de noticias, páginas web y anuncios de mensajes de correo electrónico, que contengan direcciones electrónicas. Con el tiempo comenzaron a desarrollarse programas para sacar el máximo provecho de esta información presente en Internet, y hoy existen decenas de aplicaciones “localizadoras”, no solamente dedicadas a extraer información de páginas web o grupos de noticias, sino también a buscar en programas de mensajería instantánea. A menudo, los “spammers” desarrollan sus propios programas “localizadores” para saquear nuevas aplicaciones como libretas de direcciones en línea, servidores de juegos y otros. Cuando se intenta entregar un mensaje de correo electrónico, es posible determinar si la cuenta de correo electrónico es válida mediante los mensajes que son devueltos por el servidor. El siguiente ejemplo revela que juanperez@ice.go.cr es una cuenta de correo válida, mientras que juanpablo@ice.go.cr no lo es. Utilizar un diccionario de nombres de direcciones comunes permitirá descubrir la mayoría de las cuentas en unas pocas horas realizando consultas a los servidores de correo electrónico como lo muestra la figura 8.


TELNET mail.example.com 25
Trying 10.10.10.1.
Connected to mail.example.com.
220 mail.example.com. Sendmail SMI-8.6/SMI-SVR4 ready at Sun, 21 Jan 2007 11:27:42 -0500
HELO MAIL.EXAMPLE.COM
250 mail.example.com. Hello [211.54.114.180], pleased to meet you
MAIL FROM: chrisol@mail.example.com
250 chrisol@mail.example.com... **Sender ok**
RCPT TO: juanperez@ice.go.cr
250 juanperez@ice.go.cr... **Recipient ok**
DATA
354 Enter mail, end with "." on a line by itself
Subject: Vendo carro en buen estado.

TELNET mail.example.com 25
Trying 10.10.10.1.
Connected to mail.example.com.
220 mail.example.com. Sendmail SMI-8.6/SMI-SVR4 ready at Sun, 21 Jan 2007 11:27:42 -0500
HELO MAIL.EXAMPLE.COM
250 mail.example.com. Hello [211.54.114.180], pleased to meet you
MAIL FROM: chrisol@mail.example.com
250 chrisol@mail.example.com... **Sender ok**
RCPT TO: juanpablo@ice.go.cr
250 juanpablo@ice.go.cr... **mailbox unavailable**
DATA
354 Enter mail, end with "." on a line by itself
Subject: Vendo carro en buen estado.

**Figura 8.** Respuestas del servidor de correo que verifica la existencia de una cuenta en el dominio

**Fuente:** Obtenido por el autor de un diálogo real.

Otra técnica muy eficiente es encontrar cuentas de correo “aleatorias”, lo que a menudo se utiliza para localizar las direcciones de un dominio específico. Para estos casos, se inicia un proceso extenso de verificación de cada combinación posible de números y letras en una dirección de correo electrónico, como lo muestra el siguiente ejemplo de la figura 9.

a@racsa.co.cr

b@racsa.co.cr

c@racsa.co.cr

..

..

..

abea@racsa.co.cr

abeb@racsa.co.cr

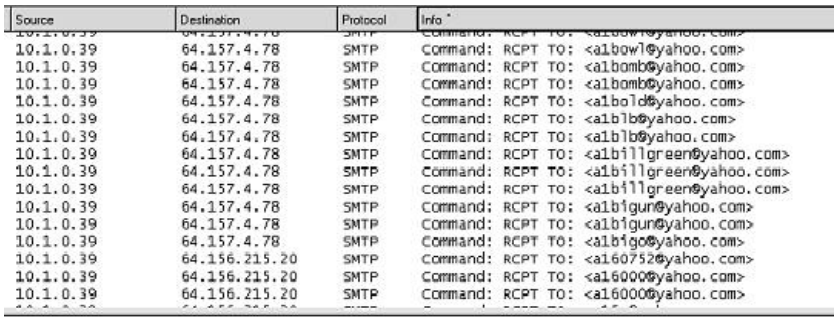
abec@racsa.co.cr

**Figura 9**. Generación aleatoria de direcciones de correo electrónico

**Fuente:** Confeccionado por el autor.

Está técnica encontrará cada cuenta de correo del servidor atacado, si este no está configurado para negar este tipo de conexiones, después de cierta cantidad de intentos con receptores no válidos.

Existen aplicaciones diseñadas para generar este tipo de combinaciones automáticamente para un determinado dominio o varios, como se muestra en la figura 10, la cual fue tomada de un analizador de protocolos proveniente de uno de los clientes de ADSL del ICE, quien envía correos deliberadamente a direcciones de yahoo.com.



| Source | Destination | Protocol | Info |
|---|---|---|---|
| 10.1.0.39 | 64.157.4.78 | SMTP | Command: RCPT TO: <a1bowl@yahoo.com> |
| 10.1.0.39 | 64.157.4.78 | SMTP | Command: RCPT TO: <a1bomb@yahoo.com> |
| 10.1.0.39 | 64.157.4.78 | SMTP | Command: RCPT TO: <a1bomb@yahoo.com> |
| 10.1.0.39 | 64.157.4.78 | SMTP | Command: RCPT TO: <a1bold@yahoo.com> |
| 10.1.0.39 | 64.157.4.78 | SMTP | Command: RCPT TO: <a1blb@yahoo.com> |
| 10.1.0.39 | 64.157.4.78 | SMTP | Command: RCPT TO: <a1blb@yahoo.com> |
| 10.1.0.39 | 64.157.4.78 | SMTP | Command: RCPT TO: <a1billgreen@yahoo.com> |
| 10.1.0.39 | 64.157.4.78 | SMTP | Command: RCPT TO: <a1billgreen@yahoo.com> |
| 10.1.0.39 | 64.157.4.78 | SMTP | Command: RCPT TO: <a1billgreen@yahoo.com> |
| 10.1.0.39 | 64.157.4.78 | SMTP | Command: RCPT TO: <a1bigun@yahoo.com> |
| 10.1.0.39 | 64.157.4.78 | SMTP | Command: RCPT TO: <a1bigun@yahoo.com> |
| 10.1.0.39 | 64.157.4.78 | SMTP | Command: RCPT TO: <a1bigo@yahoo.com> |
| 10.1.0.39 | 64.156.215.20 | SMTP | Command: RCPT TO: <a160752@yahoo.com> |
| 10.1.0.39 | 64.156.215.20 | SMTP | Command: RCPT TO: <a160000@yahoo.com> |
| 10.1.0.39 | 64.156.215.20 | SMTP | Command: RCPT TO: <a160000@yahoo.com> |

**Figura 10.** Imagen capturada de un analizador de protocolos que evidencia tráfico indebido desde la IP 10.1.0.39

**Fuente:** Confeccionado por el autor.

Uno de los primeros pasos que los ISP deben realizar es tener una cuenta de correo dedicada para reportar abusos generados en sus redes. Esta cuenta debe seguir los estándares mundiales, por lo cual debe crearse una dirección abuse@NombreDominio. En el caso de los ISP nacionales, estos cuentan con las direcciones abuse@racsa.co.cr para el caso de RACSA y abuse@ice.go.cr en el caso del ICE. Tanto RACSA como el ICE tienen a su cargo miles de direcciones IP bajo su responsabilidad, y estas entidades asignan las direcciones IP a sus clientes para darles el servicio, por lo cual si un usuario de Internet en cualquier parte del mundo recibe algún tipo de abuso proveniente de las direcciones IP administradas por RACSA o el ICE, lo podrá reportar a la dirección “abuse” del ISP correspondiente o enviar la queja directamente a las distintas casas reguladoras de “spam” (tales como Spamcop.net, spamhouse.org o abuse.net, entre otras), las cuales se encargarán de contactar al ISP correspondiente (por medio de la dirección de “abuse”) para que este tome las medidas necesarias para detener el envío de correo “spam” desde su red, de forma inmediata. Si el ISP ignora la solicitud, entonces la dirección IP será colocada en la lista negra por parte de las entidades reguladoras de “spam”, y esto provocará que los correos emitidos desde la IP infractora no sean entregados a sus destinos como gráficamente muestra la figura 11.


**Figura 11**. Representación gráfica de una lista negra

**Fuente:** Confeccionado por el autor.

La figura anterior muestra el funcionamiento de una lista negra o "blacklist": un usuario con la dirección IP 198.10.20.30 desea enviar un correo a un usuario que tiene la dirección IP 192.10.20.31; el servidor de correo del usuario receptor que tiene la IP 198.10.20.31 está protegido con un servidor "antispam", el cual toma la dirección IP emisora y consulta en una lista negra. Si la dirección IP del emisor del mensaje se encuentra publicada en la lista negra, entonces el mensaje de correo electrónico es catalogado como "spam" por el filtro de correo y el servidor no aceptará el mensaje.

Para conocer al propietario de una dirección IP, se utiliza la página http://www.dnsstuff.com/, escogiendo la opción "*Who is*". Colocando la dirección IP que se quiere investigar, se podrá obtener información del ISP responsable de la dirección; la información de "Who is" permitirá conocer el ISP responsable de la dirección IP que está siendo consultada, con lo que se identifica si es una dirección IP a cargo de RACSA o del ICE. Una vez que se cerciora de que la dirección IP infractora es propiedad de RACSA o del ICE, se debe identificar a qué tipo de servicio pertenece la dirección en cuestión.

**Usuarios de banda ancha de RACSA y el ICE**

La tecnología de banda ancha ofrece conexión digital a alta velocidad y es una conexión permanente. Esta línea de servicios ha sido diseñada por RACSA y el ICE para aquellas empresas o usuarios que requieren mantener una conexión permanente a través de la red de Internet los 365 días del año, ofreciendo múltiples velocidades físicas de conexión, lo que permite el envío y recepción de grandes volúmenes de datos. Los usuarios de este servicio poseen rangos de 8 o más direcciones IP públicas estáticas, por lo cual cuando RACSA o el ICE reciben una denuncia por "spam" proveniente de una dirección IP pública perteneciente a uno de sus usuarios de banda ancha, el ISP de manera inmediata y según el "Reglamento Autónomo de Servicio para la Regulación del Correo Electrónico Masivo o no Deseado de RACSA", se comunica con el administrador de la red con la copia de la denuncia para realizar el aviso correspondiente; de esta manera el administrador de la red tomará las medidas necesarias para identificar cuál de los equipos configurados en su red son los que están generando correo "spam". Si el administrador no detiene el envío de "spam" en el plazo indicado por el ISP, entonces la dirección IP del cliente será bloqueada por RACSA o el ICE, para evitar que esta entre en alguna lista negra.

**Usuarios de cable módem**

El acceso a Internet vía cable módem se provee a través de la red de cable coaxial de la televisión provista principalmente por las empresas AMNET, Cable Tica y Coopelesca. Es un sistema que permite la transferencia de información desde la red de Internet y hacia ella utilizando el cable coaxial que provee la cablera; la señal de televisión e internet son divididas y esto hace que un computador acceda a internet. Los usuarios de Internet según su tipo de contrato, pueden contar con direcciones IP públicas estáticas, públicas dinámicas o

direcciones privadas. Cuando un cliente tiene una dirección IP pública estática, el procedimiento para su identificación es similar al de los usuarios de banda ancha, pues la dirección IP está ligada a un suscriptor de cable módem, por lo cual es sencillo ubicar cada uno de estos casos, pero los usuarios que poseen direcciones IP privadas salen a Internet a través de un NAT o un PAT.

Los NAT y PAT se utilizan para asignar una red completa (o varias redes) a una sola dirección IP. Su uso es necesario cuando la cantidad de direcciones IP que haya asignado el proveedor de Internet sea inferior a la cantidad de computadores que accedan a Internet, por lo cual, es una forma de "ahorrar" direcciones IP. El NAT es una configuración en el enrutador que posee rangos de direcciones IP y asignan una dirección IP aleatoriamente por cada cable módem que se conecte a la red. Una vez que el cable módem se apague o se reinicie la dirección IP, se pierde y quedará disponible para cualquier otro cable módem que se quiera conectar, como lo ejemplifican las figuras 12 y 13.

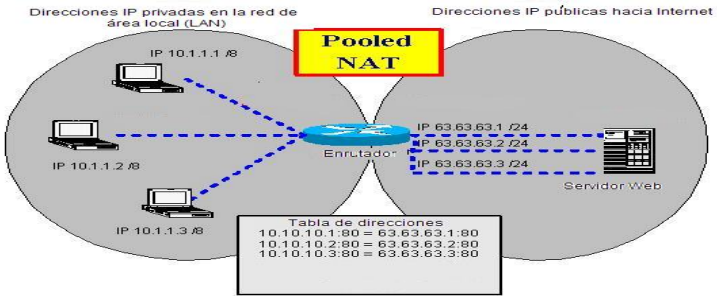



**Figura 12.** Ejemplo del funcionamiento de un NAT

**Fuente:** Obtenido por el autor de un diálogo real

Con base en el ejemplo de la figura anterior, un usuario se conecta con la dirección IP privada 10.1.1.1 y el servidor le asigna la dirección IP pública 63.63.63.1. Una vez que este usuario se desconecte, la dirección IP quedará libre en el enrutador para volver a ser asignada a otro cable módem. Por ello, si un ISP recibe un reporte por "spam" proveniente de un usuario de cable módem que se conecta a Internet mediante un NAT, es poco probable que el usuario que está generando "spam" sea el que utilice la dirección IP pública involucrada en el momento en que el ISP reciba el reporte; probablemente el "spammer" ya esté utilizando otra dirección IP asignada por el NAT, lo que le provoca al ISP la recepción de reportes provenientes de múltiples direcciones IP asignadas al NAT. El problema en este caso es si el rango de direcciones IP del NAT es colocado en una lista negra, pues los usuarios que se conecten a Internet tendrán inconvenientes a la hora de enviar correos electrónicos, ya que este puede ser rechazado por los servidores "antispam" de las distintas compañías mundiales, por estar las direcciones publicadas en la lista negra.

Para el caso de la utilización de PAT, su funcionamiento es muy similar a los NAT, con la diferencia de que todos los usuarios salen a Internet con una misma dirección IP asignada por el PAT. En otras palabras, a todos los usuarios que salen a Internet a través del PAT se les asigna la misma dirección IP pública, como lo muestra la figura 13.

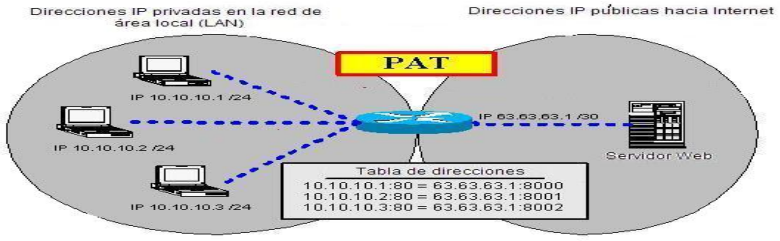



**Figura 13**. Ejemplo del funcionamiento de un PAT

**Fuente:** Obtenido por el autor de un diálogo real.

En la figura anterior se muestra que los usuarios con las direcciones privadas 10.10.10.1, 10.10.10.2 y 10.10.10.3 salen a Internet con la dirección IP pública 63.63.63.1. Este tipo de topología de red es una de las más peligrosas en lo que a control de correo "spam" se refiere, pues si uno de los usuarios conectados en este segmento de la red envía "spam", el proveedor de internet recibirá notificaciones provenientes de la IP pública 63.63.63.1, en la cual pueden existir más de 256 usuarios conectados en un momento; por lo tanto, el ISP no contará con ningún otro rastro que permita identificar cuál de los usuarios es el "spammer".

**Servicios conmutados de RACSA**

Esta forma de conexión se establece utilizando un módem que debe poseer el usuario final, para poder conectarse a los servidores de acceso de RACSA, utilizando el canal de la línea telefónica. Cuando el usuario accede a este servicio, adquiere una dirección IP pública dinámica y necesita una cuenta para acceder a la red de Internet, por lo cual, una vez que el "spammer" se desconecte, pierde la dirección IP asignada y la dirección quedará disponible para otro usuario que se conecte en otro momento. Para identificar el "spam" proveniente de estas direcciones, RACSA registra los accesos de los usuarios que hacen uso de este servicio; así mismo, deberá tomar la dirección IP del encabezado que se adjunta en los reportes recibidos junto con la fecha, hora, minutos y segundos cuando el mensaje fue emitido, para realizar una búsqueda en las bases de datos e identificar cuál fue el usuario que estuvo conectado en el momento en que se envió "spam", como lo muestra la figura 14. Una vez identificado el usuario, se aplican las medidas estipuladas en el Reglamento Autónomo de Servicio para la Regulación del Correo Electrónico Masivo o no Deseado de RACSA, y de esta

forma se evita que las direcciones IP de RACSA sean utilizadas para emitir correo "spam".

**Servicio Internet prepago de RACSA**

Es una tarjeta prepago que trae consigo un "login" y un "password" para tener acceso a internet. Cuando el usuario compra este servicio, adquiere una dirección IP pública dinámica y requiere una cuenta para acceder a la red de Internet, por lo cual una vez que el "spammer" se desconecte, pierde la dirección IP asignada y la dirección quedará disponible para otro usuario que se conecte en otro momento. Para identificar el "spam" proveniente de estas direcciones, RACSA registra los accesos de los usuarios que hacen uso de este servicio; luego deberá tomar la dirección IP del encabezado que se adjunta en los reportes recibidos junto con la fecha, hora, minutos y segundos cuando el mensaje fue emitido, para realizar una búsqueda en las bases de datos e identificar cuál fue el usuario que estuvo conectado en el momento que se envió el correo "spam", como se muestra en la figura 14.


**Figura 14.** Software para la identificación de una cuenta conmutada

**Fuente:** Datos obtenidos de funcionarios del Departamento de Control de "spam" de RACSA.

Como en este caso no es eficiente bloquear la tarjeta que está siendo utilizada para enviar "spam", ya que son tarjetas que expiran cuando vencen, RACSA bloquea el número de teléfono del cual se está realizando la llamada para acceder a Internet, y de esta forma, independientemente de la tarjeta utilizada para acceder a la red, los servidores de acceso a Internet no permiten la conexión; así se evita que las direcciones IP de RACSA sean utilizadas para emitir correo "spam".

**Servicio 900ENLINEA de RACSA**

El Servicio 900ENLÍNEA brinda un acceso fácil a Internet usando el número de acceso 900ENLINEA. No requiere firmar un contrato previo ni tener una tarjeta con contraseña para poder acceder a Internet. Cuando el usuario accede a este servicio, adquiere una dirección IP pública dinámica y no requiere de una cuenta para acceder a la red de Internet. Por lo tanto, una vez que el "spammer" se desconecte, pierde la dirección IP asignada y la dirección quedará disponible para

otro usuario que se conecte en otro momento. Para identificar el “spam” proveniente de estas direcciones, RACSA registra los accesos de los usuarios que hacen uso de este servicio y deberá tomar la dirección IP del encabezado que se adjunta en los reportes recibidos junto con la fecha, hora, minutos y segundos cuando el mensaje fue emitido para realizar una búsqueda en las bases de datos e identificar cuál fue el usuario que estuvo conectado en el momento que se envió “spam”. En este caso, RACSA bloquea el número de teléfono del cual se está realizando la llamada telefónica para acceder a Internet, ya que no existe contrato previo, y así los servidores de acceso no permitirán la conexión y se evitan que las direcciones IP de RACSA sean utilizadas para emitir correo “spam”.

**Servicio ADSL del ICE**

ADSL (línea de suscriptor digital asimétrica) es una tecnología de conexión de banda ancha para datos a alta velocidad, que permite el uso simultáneo del teléfono. Esta tecnología se denomina asimétrica, debido a que la velocidad de descarga (desde la red hasta el usuario) y de envío de datos (en sentido inverso), no coinciden. Normalmente, la velocidad de descarga es mayor que el envío de datos a Internet. Los usuarios que acceden a este servicio poseen una dirección IP pública estática, por lo cual, cuando el ICE recibe una denuncia por “spam” proveniente de una dirección IP pública perteneciente a uno de los usuarios de ADSL, de manera inmediata se establece comunicación con el cliente con copia de la denuncia para realizar el aviso correspondiente; de esta, el cliente tomará las medidas para identificar cuál de los equipos configurados en la red es el que está generando “spam”. Si el cliente no detiene el envío de “spam” en el plazo indicado por el ISP, entonces la dirección IP del cliente será bloqueada por el ICE para evitar que esta entre en alguna lista negra.

Debido a que muchos de los casos de “spam” que RACSA atiende son provocados por algunos virus o “spyware” alojados en los computadores de los clientes, RACSA creó el Centro de Seguridad e Información (Radiográfica Costarricense S.A., 2009), con el propósito de dotar a los clientes de herramientas gratuitas y funcionales que sirvan para combatir estos programas indeseados en sus computadores y que muchas veces son los causantes de que estos generen grandes cantidades de correo electrónico. La figura 15 muestra el contenido de las herramientas que RACSA pone a disposición de sus clientes. El sitio provee información y herramientas para combatir el “spam” y el “spyware”, y pone a disposición del cliente muros de fuego en versiones gratuitas, actualizaciones de antivirus y software para el bloqueo de “pop-ups”, entre otros. Si el cliente posteriormente desea adquirir el software en su versión completa, puede comprarlo. El ICE aún no ha desarrollado un sitio con estas características.


**Figura 15.** Centro de Seguridad e Información de RACSA

**Fuente:**http://www.racsa.co.cr/consejos_navegacion/proteccion/index.html

## Conclusiones

A continuación se citan las principales conclusiones obtenidas del presente trabajo:

- El envío de correo “spam” produce grandes ganancias económicas para aquellos que se dedican a este tipo de negocio, ya que reciben retribuciones provenientes de suscripciones de usuarios a las compañías que se promocionan. También es un método efectivo, pero no eficaz para promocionar la venta de un bien o servicio.
- La mayoría de los correos que circulan por la red mundial de Internet son considerados correos tipo “spam”.
- El éxito del “spam” se centra en el ínfimo costo que conlleva el enviar un correo electrónico y por la efectividad del uso de la técnica.
- Los “spammers” se basan en generar tácticas fraudulentas para lograr que los emisores adquieran los productos que ellos promocionan.
- Para reducir el problema del “spam” en Costa Rica, la solución se encuentra en la combinación de elementos tecnológicos, legales y culturales que permitan minimizar su impacto.
- Se debe entender que el establecer regulaciones tiene un costo económico, pero el no tener una regulación, como en el caso de Costa Rica, cuesta mucho más. El no invertir en tecnologías para evitar el envío y recepción del “spam”, representa un costo muy elevado a largo plazo, que los ISP y todos sus clientes deben pagar.
- A corto plazo, el volumen de “spam” continuará en aumento por la falta de acciones preventivas por parte de los actuales ISP costarricenses.
- No existe una fórmula mágica para erradicar el problema del “spam”, se requiere innovación tecnológica y una legislación efectiva que conlleve la ejecución firme del reglamento “antispam” de los ISP nacionales.
- En Costa Rica se cuenta con el Reglamento Autónomo de Servicio para la Regulación del Correo Electrónico Masivo o no Deseado de RACSA y se tiene jurisprudencia sobre casos en los cuales la Sala IV apoya la iniciativa de RACSA, en pos de proteger el servicio que brinda.
- Los ISP nacionales realizan esfuerzos para educar al usuario a través de herramientas que sean de fácil uso, con el propósito de reforzar las buenas prácticas y conductas en materia de seguridad informática para la fácil detección de "zombis", virus o “spyware” en los computadores de los usuarios del servicio de Internet.
- Los procedimientos de control de “spam”, además de ser mecanismos de control, deben ser una herramienta para que los ISP puedan medir la dimensión que el correo basura representa en su propia red y, en consecuencia, determinar las medidas que se deben seguir para combatirlo.
- Los ISP nacionales deben adoptan leyes y políticas “antispam” que permitan el rastreo de la información de los usuarios en esta materia,

detectando fuentes de abuso de la red, bajo estrictas normas de confidencialidad que salvaguarden el derecho a la privacidad.

- En la lucha contra el “spam”, los ISP nacionales luchan reactivamente, es decir, identifican el usuario que envía “spam” después de haberse producido alguna denuncia.
- Los equipos utilizados para la detección de “spam” deberán estar actualizándose constantemente para evitar ser burlados por los “spammers”, al enviar correos que no sean identificados por los filtros “antispam”.

**Bibliografía**


Reglamento Autónomo de Servicio para la Regulación del Correo Electrónico Masivo o no Deseado. (2002, 14 de marzo). *La Gaceta.* Edición N° 52.

Mulligan, G. (1999). *Removing the spam*. Canadá: Addison Wesley.

Radiográfica Costarricense S.A. (2004). *El Spam*. Recuperado el 11 de febrero de 2009, de http://www.racsa.co.cr/consejos_navegacion/proteccion/spam/index.html.

Radiográfica Costarricense S.A. (2004). *Reglamento Autónomo de Servicio para la Regulación del Correo Electrónico Masivo o no Deseado*. Recuperado el 4 de febrero de 2009, de http://www.racsa.co.cr/consejos_navegacion/spam/reglamento_spam.pdf

Spamer-x, Spam, (Anayal, Pág. 295).

Spamfighter. (2009). *Masiva oleada de spam*. Recuperado el 11 de febrero de 2009, de http://www.spamfighter.com/lang_ES/News_Read_Spamfighter.asp?UID=582.