Evaluación de alternativas para reducir el spam

Autor: Jesús Sanz de las Heras (Coordinador del servicio de correo electrónico en la comunidad académica española, **RedIRIS**), <jesus.heras@rediris.es>

> *"El correo basura es el azote del correo electrónico y los grupos de noticias en la Internet. Puede interferir seriamente con la operación de servicios públicos, por no mencionar el efecto que puede tener en los sistemas de correo electrónico de cualquier individuo... Los spammers están, de forma efectiva, sustrayendo recursos de los usuarios y proveedores de servicio sin compensación y sin autorización."*
>
> - Vint Cerf, Senior Vice President, MCI

1 Consideraciones sobre el spam

Esta sección será mas breve debido a la extensa literatura existente y los diferentes enfoques de lo que se entiende por spam. Desde mi punto de vista la definición de spam tiene varías vertientes en función de:

- **Efectos**: clásico correo basura o no deseado que se recibe en los buzones.
- **Origen**: enormes listados de direcciones de correo obtenidas de forma ilegal.
- **Distribución**: infraestructura (Estafetas de correo, proveedores de servicios y transporte) para la distribución del correo

El spam es un gran negocio que invade nuestros buzones. La mejora de los accesos a Internet ha incrementado el volumen del spam tanto por parte de los emisores como destinatarios. Los emisores porque disponen de mas posibilidades de ancho de banda y uso de servidores propios. Los receptores porque debido a las tarifa planas y la consecuente reducción del coste de recoger correo ya no es tan gravoso económicamente que la recepción de spam se asume con *resignación*.

El spam es un simple reflejo de la actual sociedad donde la publicidad inunda todos los rincones. Los contenidos del spam son variados y difíciles de clasificar, pero es cierto que los hay de carácter fraudulento e ilegal y sobre todo molestos. La naturaleza internacional de Internet y de las direcciones IP origen inhabilita cualquier medida legal para reducir el spam.

2 Métodos de captura de direcciones para spam

Las tácticas mas populares para recoger direcciones de correo de forma masiva son:

- **Compra de bases de datos** selectivas. Son bases de datos de direcciones de correo-e clasificadas por temáticas de interés. Estas bases de datos son creadas por responsables web sin escrúpulos que recogen direcciones de los usuarios que pasan por su portal.
- **Listas Opt-In**. Son servicios a los que cualquier se puede suscribir de forma voluntaria. Muchas veces marcando la casilla que dice "No me envíe ofertas", al final las recibes. Evidentemente la mayor parte de las listas opt-in son legales pero hay mucho engaño e incumplimiento de lo que ellos mismos dicen y además difícil de demostrarlo.
- **Páginas web**. Son robots capaces de hacer barridos en Internet o determinadas zonas para localizar miles de direcciones de correo-e. Los spammers los usan día y noche.
- **Servidores de correo-e**. Son robots que extraen direcciones de correo de los servidores de correo, simulando una transacción SMTP y preguntando si tal usuario es o no correcto. Hacen barridos automáticos de nombres de usuario con diccionarios.
- **Virus y códigos maliciosos**. Son virus que se propagan por correo-e consistiendo su actividad en capturar los datos de la libreta de direcciones del usuario *contaminado* y enviarlos determinadas direcciones para su procesamiento y almacenamiento.

3 Métodos de distribución de spam

Distribuir un mensaje a miles de destinatarios es una tarea sencilla y económica,. Basta con conocer el diálogo de las transacciones SMTP (Simple Mail Transfer Protocol) descritas en el RFC822 (RFC2822). Los ingredientes para la distribución son:

- **Programa** sencillo que reproduzca un diálogo SMP, colocando los campos Remite: y Destino: que le vengan en gana y falsificando algunas de las cabeceras de tránsito (*Received*:)
- **Base de datos** de direcciones de correo a los que distribuirá el mensaje de spam
- **Máquina** (Estafeta) con la que establecer el diálogo SMTP. En este caso puede ser:
    - Máquina local con un paquete de servidor de correo-e
    - Máquina remota a la que se accede por el puerto 25 (SMTP).

Entendiendo como spam todo mensaje de correo electrónico no solicitado Podríamos clasificar al spam en dos categorías en función del uso de recursos (máquina, CPU, disco, ancho de banda) por parte de terceros.

- **Spam *legal*: Uso de recursos propios.** Es el spam procedente de Empresas distribuido desde sus propias máquinas dentro de sus campañas de marketing y promoción. También el procedente de

Proveedores de servicios Internet (ISPs) que es usado por usuarios o Empresas que no disponen de recursos propios de distribución masiva.

- **Spam *ilegal*: Uso de recursos ajenos.** Es el spam que para sus distribución se aprovecha de Estafetas ajenas mal configuradas (open-relay [1]). Existe entre los spammers bases de datos de máquinas (IP) mal configuradas para poder ser usadas.

El spam ilegal es uno de los mas extendidos y suele ser el que viene en idioma inglés. Generalmente procede de USA pero utilizan para su distribución máquinas open-relay de cualquier parte del mundo con el objeto de evitar la legislación de dicho país. El spam en idioma castellano suele ser spam legal procedente de ISPs o empresas.

El protocolo SMTP que regula todas las transacciones de correo de Internet se creó allá por 1981 de forma insegura para ser usado por científicos sin pensar en ningún uso comercial. Ya existían listas de distribución (LISTSERV-1984) que era usadas para distribuir información de uno a muchos. La explosión de Internet en 1994 a nivel social y comercial hizo que se "descubrieran" los agujeros de SMTP para ser utilizado como el mejor y mas barato mecanismos para distribuir y hacer llegar directamente a miles de buzones cualquier tipo de información.

La gran explosión del spam empezó en 1995-1996 donde cualquier máquina con un servidor de correo podía ser usada por los indeseables spammers para distribuir su información. En esos años el spam que se recibía en el buzón era muy inferior al actual del 2002. El gran problema eran los ataques que sufría el puerto SMTP (25) para distribuir spam. En dicha época el servidor de correo mas extendido era Sendmail, el cual solucionó las deficiencias de SMTP con sus reglas de configuración y se empezaron a solucionar muchos de los problemas, los de servidores con otro tipo de sistema operativo llegaron mas tarde. Aún así estos problemas de configuración no están erradicados en el 100% de las máquinas de Internet por lo que siguen existiendo máquinas open-relay.

4 Efectos del spam

Algunos los efectos negativos y problemas del spam:

1 Inunda los **buzones** saturando la capacidad máxima de los mismos y por tanto provocando la pérdida de correo deseado y útil.
2 Reduce la **efectividad** del correo-e al ser molesto u ofensivo al receptor.
3 Afecta a los **recursos** de la Estafeta de correo-e ya que mientras está procesando spam ralentiza el procesamiento del correo normal.

[1] **Estafeta open-relay:** Son Servidores de correo mal configurados que permiten encaminar correo desde cualquier dirección IP. Esto permite un uso indebido de recursos de la empresa por parte de personas ajena a la misma. Estas Estafetas son las preferidas por los spammers para inyectar mensajes de spam y destinado a miles o millones de destinatarios.

4 Afecta al ancho de banda congestionando las **infraestructuras** de comunicaciones
5 Afecta al **tiempo** de los usuarios empleado en borrar, denunciar, filtrar etc y al de los responsables del correo
6 Afecta a la **imagen** de la Empresa que distribuye spam

Por poner un ejemplo un servicio clásico en Internet como las News de Usenet está siendo bastante afectado en su funcionalidad por el incesante uso que se le está dando para distribuir spam a través de muchos de sus grupos. Otros ejemplos graves de efectos del spam en cualquier empresa son:

- **Tamaño del mensaje**. La distribución masiva de spam incluyendo ficheros grandes puede perjudicar gravemente a las Estafetas de una empresa o inhabilitar el correo de algún usuario. De aquí la necesidad de limitar el tamaño del correo entrante.
- **Direcciones falsificadas**. Este es un efecto difícil de explicar en pocas líneas. Básicamente consiste en atacar una Estafeta open-relay (E1) para ser la distribuidora del correo. El truco está en que el mensaje de spam lleva como dirección de correo emisora la de cualquier dominio. La Estafeta de este dominio (E2) será la atacada. ¿cómo? Dicho dominio es quien recibirá los mensajes de error de las miles de direcciones inyectadas en la Estafeta (E1). Estos errores serán los producidos en las transacciones SMTP desde la máquina open-relay a los diferentes destinos.

  La máquina atacada (E2) recibirá miles de mensajes destinados a direcciones de su dominio con el agravante que la parte local de la dirección no existe generándose un nuevo error y una nueva transacción SMTP produciendo el colapso de los servidores de correo.

Todos estos problemas nos pueden llevar a pensar en la fragilidad del correo-e en Internet y la pérdida de confianza en este útil servicio. Si al spam habitual, se le añaden sus efectos colaterales mas allá de la simple recepción de correo no deseado, los virus y la generación mensajes y confusión producida por los Antivirus en las Estafetas, la falsificación de mensajes etc podemos llegar a la conclusión que el Servicio de Correo electrónico en Internet es inútil. Actualmente los **virus** es el problema mas grave del correo-e pero éstos tienen su patrones y por tanto son interceptables con los actuales Antivirus. El **spam** es un problema del correo-e por la dificultad de evitarlo.

Un problema colateral del incesante aumento del spam es la regulación legislativa que puede llegar a encubrir la regulación de otros aspectos de Internet. Es claro que la legislación en Internet ya comenzó y mucha de ella está relacionada con la protección de datos, el correo-e y el spam.

5 Medidas contra el spam

5.1. Introducción

¿Qué es lo que se quiere solucionar: el correo basura en los buzones de los usuarios o reducir el impacto en los servidores de correo y líneas de comunicaciones? O por el contrario se quiere combatir el spam en general por ser una lacra en Internet.

En función de cuales sean nuestros objetivos debemos enfocar las posibles alternativas al problema. No son iguales las soluciones o medidas a adoptar para una Empresa que para un Proveedor de servicios Internet que para un comunidad amplia como puede ser la Comunidad científica española, RedIRIS.

En función de cómo queremos reducir los efectos del spam podemos clasificar las soluciones en:

- **Precavidas**: Medidas que **colaboran** a evitar recibir o distribuir spam en o desde Empresa o Proveedores. En este bloque se englobaría: eliminación del *tag html* "malito:" en las páginas web, Políticas de Uso Aceptable en Empresas y Proveedores, Formación, cumplimiento de la LOPD y registro de ficheros etc.

- **Reactivas**: Medidas que se toman **después** que el correo (spam) haya llegado a los servidores y buzones. Son medidas del tipo Filtros de contenidos (Content-Filter) tanto para servidores como clientes de correo.

- **Proactivas**: Medidas que se toman **antes** que el correo (spam) llegue a los servidores. Son medidas del tipo *listas negras* , denuncias y Legislación.

Es necesario dejar claro que no hay solución ni exacta ni infalible ni global, la aplicación de todas si reducirá el impacto del spam. Esto no implica que no se deban tomar medidas porque las que se tomen siempre reducirán en mayor o menor grado el impacto del spam. Las técnicas de los *spammers* cambian continuamente a medida que aparecen nuevas técnicas para evitarlo.

5.2. Medidas Precavidas

Estas medidas son necesarias para prevenir la captura de nuestras direcciones de correo. La distribución de spam sólo es posible si se dispone de muchas de estas direcciones. La captura de direcciones escaneando páginas web es una técnica habitual para la distribución de spam. Existen numerosos programas de manejo sencillo y distribución pública que permiten este tipo de técnicas. Un diseño de

páginas donde se tenga en cuenta evitar utilizar el *tag* **mailto:** será un primer paso para evitar capturar direcciones que acaben alimentando estas bases de datos y reducir el spam. La mejor alternativa al uso de estos *tag* es la implementación de formularios web cuya información sea enviada por correo al buzón correspondiente para lectura.

Otra de las medidas preventivas que debería ser adoptadas es la disponibilidad de un documento que defina la **Política de Uso Aceptable** del correo-e en la Empresa o en Proveedores. Básicamente este tipo de documentos deben definir los derechos y obligaciones del uso del servicio con recursos de la empresa o Proveedor. El uso del correo electrónico e Internet en las empresas ha abierto un nuevo capítulo en el debate sobre los límites de la privacidad y el control. Es claro que se minimizan los conflictos en un empresa por aspectos relacionados con el correo-e cuando las empresas disponen de Políticas de Uso sencillas, claras y conocidas por todos. En dicho documento la Empresa debería aceptar que las técnicas de spam no forma parte de sus mecanismo de marketing y publicidad.

Un tema muy importante a tener en cuenta es la labor de **formación** e **información** continua de los empleados en todos los aspectos relacionados con el correo: lo qué es, uso correcto, tipos de abuso, legislación relacionada y descripción del spam.

Evidentemente estas políticas de uso en un proveedor de servicios Internet (ISP) tendrían enfoques diferentes ya que no hay empleados sino usuarios/clientes que usarán los servicios. Los Servicios de los ISP son los que usan las empresas para distribuir spam por lo que deberían de disponer de una reglamentación contundente especificando claramente los tipos de abuso en el correo-e como la distribución masiva de correo así como sus penalizaciones. Este es un buen ejemplo de un extracto de la Política de Uso de Aceptable de un proveedor:

Por esta razón, se entenderá que los clientes han infringido la política de usos aceptables de VERIO y el Contrato de servicios cuando los clientes realicen las siguientes acciones consideradas como prohibidas:

Spamming - Enviar correo no solicitado y/o mensajes comerciales no solicitados a través de Internet (llamado "spamming"). No es solamente por el impacto negativo que pueda crear en el consumidor hacia VERIO, además puede sobrecargar la red de VERIO haciendo que el servicio que se ofrece al cliente no pueda ofrecerse en condiciones plenas de calidad. De la misma forma, el mantener una pasarela SMTP abierta está prohibido. Cuando una queja es recibida VERIO tiene la potestad de determinar si cumple o no las características que infringen las normas o determinan que se ha realizado Spamming.

Los ISP que ofrecen servicios de conectividad también deberían especificar en los contratos las condiciones de uso dejando claro que como responsables de las direcciones IP no se acepta la distribución de spam por sus líneas y por tanto cualquier denuncia recibida será canalizada convenientemente

5.3. Medidas Reactivas

Las medidas reactivas implican que la transacción SMTP entre el servidor origen y el destino **ha concluido** con éxito y el mensaje ha sido depositado en la Estafeta local para su posterior aplicación de filtros. Estos filtros son filtros de contenidos y son definidos por el usuario final o por el administrador del sistema por lo que las medidas reactivas puede ser:

- **Filtros clientes**: Filtros de contenido en el cliente de correo. Cadenas de datos que puedan encajar con el campo Remite:, Tema:, cuerpo del mensaje etc. Las palabras clave las pone el usuario y por lo tanto es él quien decide lo que le gusta o lo que no.
- **Filtros Estafeta**: Filtros de contenido en el servidor de correo. Cadenas de datos que puedan encajar con el campo Remite:, Tema:, cuerpo etc. El que decide lo que le gusta o lo que no es el responsable del servidor, es decir, la Empresa.

Actualmente ambos tipos de filtros disponen muchas alternativas teniendo como objetivo común el generar y compartir ficheros con patrones de cadenas que puedan filtrar e interceptar el spam. Existen un amplio abanico de desarrollos públicos y comerciales de iniciativas de análisis estadístico de contenidos de spam para ser instalados en clientes (filtros clientes) o Servidores de correo (filtros estafeta).

Las medidas reactivas realmente lo que hacen es ocultar al usuario lo que ya ha llegado a la Estafeta de correo. Los filtros de cliente suele tomar acciones como borrar o generalmente mover a alguna carpeta por si algún mensaje bueno ha sido interceptado. Los filtros de Estafeta lo mismo, suelen tomar como acción la conservación de los mensajes interceptados en directorios de *cuarentena* para su posterior revisión.

Las medidas reactivas tipo **Filtros cliente** solucionan algunos de los problemas ocasionados por el spam (Ver **4. Efectos del spam**) como son reducir sus efectos en la gestión del correo de los usuarios. Pero no solucionan la recepción vía POP o IMAP del spam que sigue llegando al buzón aunque gracias a los filtros no se ve y por tanto no molesta al usuario. Es decir soluciona con efectividad lo que mas interesa al usuario final que es no ver el maldito spam. Por lo que desde este punto de vista las soluciones reactivas son bastante eficientes. Además y muy importante es que permiten trasladas al usuario la decisión de configurar sus propios filtros y la decisión de lo que quiere y lo que no.

Las medidas reactivas de **Filtros en Estafeta** solucionan los mismos problemas que los de cliente pero además evita que el spam llegue al buzón de los usuarios. Tiene el inconveniente que se deja en manos de los responsables del Servicio la creación de las bbdd de patrones de palabras (contenidos) para filtrar el spam.

Debemos de recordar que las Medidas Reactivas no solucionan los efectos del spam en el ancho de banda de las líneas de la Empresa ni en los recursos de la Estafeta que por el contrario los aumenta para poder usar los Filtros de Estafeta.

Los Filtros de contenidos en Estafetas son una buena solución corporativa contra el spam. Están apareciendo productos de Empresas Antivirus (TrendMicro-Emanager-, McAfee –SpamKiller-...) que acompañando a los productos para evitar los virus también intentan evitar el spam. La filosofía es similar a los de los antivirus, ya que se escanean los correos en busca de patrones de virus se escanean en busca de patrones de contenidos de spam. Estas Empresas igual que mantienen y actualizan continuamente sus ficheros *pattern* de virus lo están haciendo también del *pattern* de patrones de contenido para el spam. ¿de donde sacan dichos patrones de palabras? Recogiendo spam por Internet de:

- De portales que ofrecen como servicio el envío de denuncias a los lugares adecuados. Los usuarios dejan su spam, se analiza y se envía la correspondiente denuncia. El spam que deja el usuario es reutilizado

- De proveedores o Empresa que interceptan spam y lo intercambian o ceden a otras.

Todo el spam es procesado para extraer las palabras mas comunes usadas en el spam para generar estos directorios de firmas o *pattern* que luego serán descargados por las clientes para interceptar correo en las Estafetas o clientes.

Las medidas reactivas suele ser **bastante efectivas** siendo además una de las pocas soluciones accesible a cualquier Empresa.

Aspectos **positivos** de las Medidas reactivas:

- Elimina (esconde) el spam de los buzones
- Si los filtros eliminan algún mensaje correcto, siempre es posible buscarlo en las carpetas de cuarentena
- Filtros cliente: La decisión de lo que es spam recae en el usuario que lo sufre ya que es él quien define los filtros
- Filtros Servidor: La decisión de lo que es spam definido en la Política Aceptable de Uso de la Empresa recae en los responsables de la misma quien define los filtros

Aspectos **negativos** de las Medidas reactivas:

- Esconde el spam en carpetas (Filtros cliente) o directorio (Filtros servidor) de cuarentena
- El spam es encaminado por nuestras líneas de comunicaciones y procesado como mínimo por las Estafetas de correo-e.
- No **elimina** realmente el spam simplemente lo *esconden* a los ojos de los destinatarios finales
- No **avisan** al emisor o proveedor del envío de spam

- Los filtros pueden eliminar mensajes *correctos* (deseados)
- No son técnicas que tengan efectos en la **erradicación** del spam. Ni emisores ni proveedores responsables reciben ningún tipo de información que les indique que su actividad o del cliente es incorrecta.
- La gestión de la base de datos de palabras usada para los filtros es compleja, pues depende del idioma y del tipo de spam que se reciba.

5.4. Medidas Proactivas

Las medidas proactivas implican que la transacción SMTP entre el servidor origen y el destino **no finaliza** con éxito y es rechazado en función del perfil del servidor origen que pretende enviar el correo. Las medidas proactivas intentan evitar tanto la entrada de spam en nuestro dominio como presionar al origen para no volver ha intentarlo. Digamos que las diferentes medidas proactivas son mas comprometidas para luchar contra el problema del spam que las reactivas.

5.4.1. Legislación

La legislación es una de estas medidas proactivas. La legislación intenta regular e intimidar con sanciones las actividades del spam. La legislación española contempla, regula y penaliza las actividades de spam en el contexto de la LSSI (*LEY DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN Y DE COMERCIO ELECTRÓNICO***),** en el "*Título III de Comunicaciones Comerciales por vía electrónica*" . El gran problema de esta Ley es la ausencia de canales de puesta en marcha de la Ley, es decir, no se contempla la definición de mecanismos de denuncia que coordinados con el poder judicial permita emitir denuncias de una forma sencilla, ágil y dinámica. A día de hoy no existe ningún mecanismo de este ni ningún tipo.

El carácter internacional del spam hace que la legislación nacional tengan poco sentido. La legislación nacional es necesaria, pero no útil, ya que sólo puede regular las emisiones de spam con origen en máquina ubicadas en territorio nacional.

5.4.2. Listas Negras

Otra de las medidas proactivas mas ampliamente conocidas y útiles son las llamadas **listas negras** de las que hablaremos en este apartado. Haremos un breve repaso a sus orígenes.

La existencia a partir de mediados de los años 90 cuando el spam empezó a despertar el método mas habitual de distribuirlo era usando Estafetas open-relay. El uso de Estafetas o servidores open-relay ajenos para la distribución de spam no sólo consumía los recursos de la máquina (disco, CPU y líneas de

comunicaciones) sino que evitaban cualquier posible medida legal del país de origen. Muchas Estafetas empezaron a actualizar sus paquetes que hacían las labores de Estafeta para evitar el uso de sus recursos de forma ilegal.

Esta excesiva cantidad de máquinas open-relay provocó la aparición de múltiples de iniciativas con diferentes técnica para generar listas o bases de datos de Estafetas open-relay. Las máquinas listadas eran máquinas poco fiables para que se conectaran a la nuestra para enviar correo porque con mucha probabilidad fuera spam. Las listas negras empezaron a aparecer como el único mecanismo que disponible para reducir los efectos del spam. Estas bases de datos de máquinas *indeseables* sólo eran accesible en local. Allá por el 1997 la iniciativa MAPS/RBL ideó un mecanismo para acceder a dichas listas negras en remoto en concreto vía DNS (Domain Name System) . Es decir un mecanismo que permite a los servidores de correo-e *preguntar* vía DNS a dichas bases de datos si la IP (servidor de correo) que se que va a conectar a mi máquina para comenzar una transacción SMTP está o no está incluida. En caso que estuviera la conexión se cierra, en caso que no estuviera continúa la transacción.

Evidentemente estas listas negras disponían de mecanismos para chequear periódicamente las máquinas y comprobar si seguían siendo open-relay o había corregido el problema. La gran labor de las listas negra fue: a) obligar a todos los servidor de correo-e a actualizarse y b) dio a conocer el problema del spam.

A partir de este momento empieza a producirse un gran movimiento y a aparecer muchas iniciativas de listas negras cada una con su propia peculiaridad para diferenciarse de las demás. Empiezan a aparecer listas negras con otros criterios y como no... empiezan a comercializarse (ver Tabla 1.). No sólo existen listas negras con Estafetas open-relays sino con criterios como: que cumplan estrictamente algunos RFCs, listas manuales mantenidas con coordinación internacional etc. Estas bases de datos de listas negras con miles de open-relays serán muy similares a las que los spammers usan para distribuir su basura.

¿ De dónde obtenían la información estas iniciativas de listas negras? De las denuncias de spam que introducían los usuarios que las recibían y de mecanismos vía web para comprobar si una máquina era o no era open-relay . Incluso había iniciativas que escaneaban los puertos SMTP de toda Internet en busca de open-relays.

Nombre	Zona DNS	Descripción
MAPS / RBL / DUL / RSS www.mail-abuse.org	blackholes.mail-abuse.org dialups.mail-abuse.org relays.mail-abuse.org rbl-plus.mail-abuse.org	Almacena open-relays, rangos de dial-up. Los primeros y una de las mejores iniciativas. En 2000 empezó a comercializarse (MAPS RBL+)
ORDB (www.ordb.org)	relays.ordb.org	Sólo almacena open-relays. Actualmente es una de las mas sólidas.

ORBZ	orbz.gst-group.co.uk	Una de las mas agresivas. Nació en 1998 y murió en 2001 por problemas jurídicos. Una de las históricas
FIVETEN (www.five-ten-sg.com/blackhole.php)	blackholes.five-ten-sg.com	Almacenan diversas fuentes de spam: direcciones de grupos de News, organizaciones con formails inseguros etc
SPAMHAUS (SBL**)** (www.spamhaus.org/sbl)	spamhaus.relays.osirusoft.com	Lista **manual** de Bloques IP de distribuidores masivos de spam y/o Empresas colaboradores de spam.
DSBL (dsbl.org)	list.dsbl.org multihop.dsbl.org	Desde Abril2002.Almacenan open-relays que ellos mismos chequean. ¿Herederos de ORBZ?
RFC-Ignorant (RFC-Ignorans.org)	**dsn**.rfc-ignorant.org	Detecta MTas que incumplen RFCs básicos del correo-e: RFC821, 2821[2], 1123[3], 2142[4], 954[5]. En continuo crecimiento.
OSIRUS (relays.osirusoft.com)	Relays.osirusoft.com	Almacenan IP con diferentes criterios open-relays, usuarios, empresas colaboran con el spam, MTAs con servidores de listas que no solicitan confirmación etc. Actualmente también funciona como agregador de varias listas negras
Spamcop (spamcop.net)	Bl.spamcop.net	Una de las mejores. Almacena de forma temporal MTAs que simplemente han distribuido spam
Spamhaus (sbl.spamhaus.org)	**sbl.spamhaus.org**	Almacena open-relays, spammers etc. Disponen de una amplia red de zonas DNS repartida por Europa y USA

Tabla 1 Relación simplificada de algunas de las iniciativas de listas negras.

Por tanto las listas negras son bases de datos que direcciones IP que se reflejan en un una zona inversa de DNS de la organización que lleva la iniciativa y que son consultadas en tiempo real por los Servidores de correo-e en cada transacción SMTP al entrar correo. Cada una de estas listas disponen de su propia política propia de criterios y mecanismo para ingresas y/o salir. Uno de los aspectos mas importantes de las listas negras es la disponibilidad y accesibilidad de un buen soporte rápido de Zonas de DNS a ser posible con mirrors en varias partes de mundo. Un acceso lento o una caída de estas Zona supondría un cuello de botella en la entra de correo.

[2] RFC2821: Indica que cualquier servidor de correo debe disponer de una dirección de correo tipo <postmaster@...>. "*SMTP servers MUST NOT send notification messages about problems transporting notification messages. One way to prevent loops in error reporting is to specify a null reverse-path MAIL FROM:<>* ")"

[3] RFC1123: Se refiere a MTAs mal configurados que no soportan Mail From:<> que lo usan, falsamente, como medida anti-spam (e.g. Terra) . "The syntax shown in RFC-821 for the MAIL FROM: command omits the case of an empty path: "MAIL FROM: <>" (see RFC-821 Page 15). An empty reverse path MUST be supported"

[4] RFC2142: Indica que cualquier servidor de correo debe disponer de una dirección de correo tipo <abuse@..>

[5] RFC954: Básicamente se refiere a IP que no disponen de datos correcto o desactualizados en el Whois.

La implementación de listas negras en servidores de correo de cualquier plataforma es muy sencilla y está ampliamente documentada. Los criterios de decisión de qué listas negra instalar serían:

- Política propia sobre el correo-e
- Política de las diferentes iniciativas que evaluemos
- Dinamismo y mecanismos de altas y bajas de las iniciativas
- Disponibilidad y accesibilidad de las Zonas DNS de consulta

Hay que recordar que es posible instalar varias listas en cascada en un servidor de correo, es decir, si una de ellas no tiene la IP se lo pasa a otra y así hasta la última, evidentemente no es un técnica muy aconsejable por las consultas necesarios a DNS por cada mensaje. Es por este motivo que hay listas negras como Osirusoft que son integradores que contienen mirrors de varias listas negras lo que facilita la labor de la configuración en cascada.

Aspectos **positivos** de las Medidas reactivas:

- Presionan y ayudan a proveedores y responsables de correo-e a mejorar sus configuraciones y eliminar clientes indeseables que usan técnicas de spam
- Avisan a los responsables y usuarios que su Estafeta tiene problemas.
- Eliminan y reduce el impacto del spam.
- Ayudan a los proveedores a mejorar sus configuraciones y eliminar clientes indeseables que usan técnicas de spam,

Aspectos **negativos** de las Medidas reactivas:

- Todo el correo procedente de una Estafeta es rechazado. Es decir, podrían ser rechazados mensajes *correctos* provenientes de una MTA, sin posibilidad de rescatarlos.
- Solo chequean la IP del MTA y desprecian el cuerpo y origen del mensaje
- El filtrado de mensajes *buenos* procedentes de MTAs *malos* debe ser considerado como un efecto colateral.

5.5. Plataforma Unificada AntiSpam (PUAS). Comunidad RedIRIS

El éxito de las listas negras está en la posibilidad de consultar las bases de datos vía DNS lo que permite que aplicaciones de red como los que llevan a cabo los servidores de correo-e (MTAs o Estafetas) puedan chequearlas y decidir si aceptan o no una conexión SMTP desde una IP incluida en estas listas

RedIRIS es la Red Académica española y consideramos que entre sus funciones es fomentar el buen uso del correo en la Red, con PUAS se fomenta a través de la presión y rechazando toda la Comunidad correo procedente de un servidor . Las

prácticas de spam desde hace tiempo son duramente penalizadas en las instituciones de RedIRIS. Se ofrecen canales especializados de distribución masiva (congresos, cursos, ofertas de trabajo y becas, avisos etc) como alternativa a las prácticas de spam . PUAS intentará fomentar las buenas prácticas entre los proveedores de la Red impidiendo que envíen correo a la comunidad académica.

En base a estos conceptos, RedIRIS pone en marcha un sistema anti-spam basado en listas negras pero con ciertas peculiaridades concretadas en una **política propia, única, común y consensuada** por todos los responsables de correo de la Comunidad RedIRIS. De ahí el nombre de Plataforma Unificada AntiSpam (PUAS). Una de las principales características de PÚAS es su carácter comunitario que permitirá a todas las Estafetas de la Comunidad RedIRIS, a través del uso de listas negras, rechazar tráfico procedente de las mismas Estafetas (IP). PUAS ofrece resultados sorprendentemente **ágiles** y **exactos**

Peculiaridades de PUAS:

- La entrada y salida en la base de datos de PUAS de direcciones IP origen de spam es: **dinámica** y **temporal.**
- En PUAS sólo se **entra** por ser denunciado
- De PUAS sólo se **sale** por dejar de ser denunciado
- PUAS juzga a cada IP de forma independiente y penaliza sólo por méritos estadísticos
- El tiempo de **permanencia** en PUAs depende:
    - Número de sensores que lo ha denunciado
    - Número de denuncias
    - Configuración open-relay
    - Reincidencia
    - Frescura de la denuncia (mas valor las denuncias mas recientes).
    - Si se corregido el problema de open-relay

Coordenadas de PUAS:

- Detectar origen (IP) de mismo spam con destino a varias instituciones de las Comunidad. Es decir capturar un mismo mensaje de spam que ha entrado en varias universidades.
- Penalizar a las Estafetas que han distribuido dicho spam, rechazando su correo en todo a la Comunidad.

Objetivos de PUAS:

- Hacer **frente común** en la Comunidad académica RedIRIS al problema del spam
- Rechazar el tráfico de correo desde máquinas que han sido usadas como distribuidoras de spam a la Comunidad académica RedIRIS

- Fomentar con la presión de toda la comunidad académica española el buen **uso del correo** en los proveedores y reducir las técnicas de spam
- Exclusivamente se tendrá en cuenta el **spam** que entre en varias universidades (sensores de spam)
- **Capturar** direcciones IP de Estafetas que hayan distribuido spam a mas de 5% de instituciones.
- Disponer de una **política propia y común** independientemente de iniciativas similares extrajeras.
- Ajustar las **necesidades** propias de la Comunidad RedIRIS frente al spam.
- Crear dos **Zonas secundarias** DNS (*puashard.rediris.es* y *puassoft.rediris.es*) con las IPs de MTAs emisores de spam:
    - *puashard.rediris.es*": bases de datos con penalizaciones **bajas** y **fácil** entrada
    - puassoft.rediris.es": bases de datos con penalizaciones altas y **difícil** entrada

Características de PUAS:

- PUAS será dirigido y gestionado por los ***postmasters*** de la Comunidad académica RedIRIS
- Las denuncias de spam se envían por **correo electrónico** de dos posibles formas
    - **Directo**: a través de RedIRIS
    - **Indirecto**: a través de la universidad que previo análisis se redirige a RedIRIS
- Las denuncias son analizadas y procesadas en RedIRIS

6 Conclusiones

Para reducir el impacto del spam es necesario conocer los detalles tanto de los mecanismos como sus efectos o daños y las posibles soluciones. En la evaluación de las posibles soluciones habrá que tener en cuenta: las necesidades de nuestra empresa, la posible ralentización del sistema de correo, la política de la Empresa o las necesidades de los clientes a los que damos servicio etc.

La solución mas accesible son los filtros de contenidos en el servidor de correo- de acuerdo con la Política de Uso del servicio en la Empresa. Estos filtros escanean todo el tráfico entrante de correo (SMTP) en busca de patrones de palabras almacenadas en una base de datos (pattern) actualizada periódicamente. Estos filtros suelen actuar después del escaneo del tráfico SMTP en busca de virus. En el mercado existe un amplio abanico de ofertas de productos para llevar a cabo estas funciones. Una aspecto muy importante de esta solución es la gestión de la bases de datos o pattern que deberá ser alimentada continuamente

con patrones propios. Los pattern de las Empresas suelen estar en idioma inglés, es decir, preparadas para interceptar el spam en dicha lengua.

Las medias reactivas son también perfectamente viables, son consideradas soluciones agresivas porque puede llegar a rechazar correo *bueno* procedente de Estafetas etiquetadas como indeseables. Éste debe ser considerado como un efecto colateral habitual de medidas de este estilo

Las medidas reactivas son las mas efectivas en la lucha contra el spam. Estas medidas son muy útiles cuando se aplican en un comunidades amplias de carácter académico, gubernamental o empresarial . Este es el caso de la iniciativa PUAS (Plataforma Unificada AntiSpam) aplicada en mas la comunidad académica española RedIRIS formada por mas de 300 instituciones.

Una aspecto que no abordado en este artículo es la evaluación de las diferentes tecnologías que disponen para evitar la distribución de spam, es decir, las alternativas a los métodos de spam. Actualmente existen multitud de técnicas que sirven de alternativa a la distribución de correo no deseado (spam) . A estas alturas se conocen perfectamente los efectos negativos del spam en las Empresas que lo usen, pero la tentación de disponer y utilizar de bases de datos de clientes clasificados es muy grande por su sencillez y rapidez. Es necesario disponer de alternativas que aunque lleven mas tiempo son mas correctas.