Zimbra y filtros *antispam*

En primer lugar deberá confirmar las versiones de los programas responsables del sistema *antispam* incorporados al servidor Zimbra, ya que el proceso varía entre versiones.

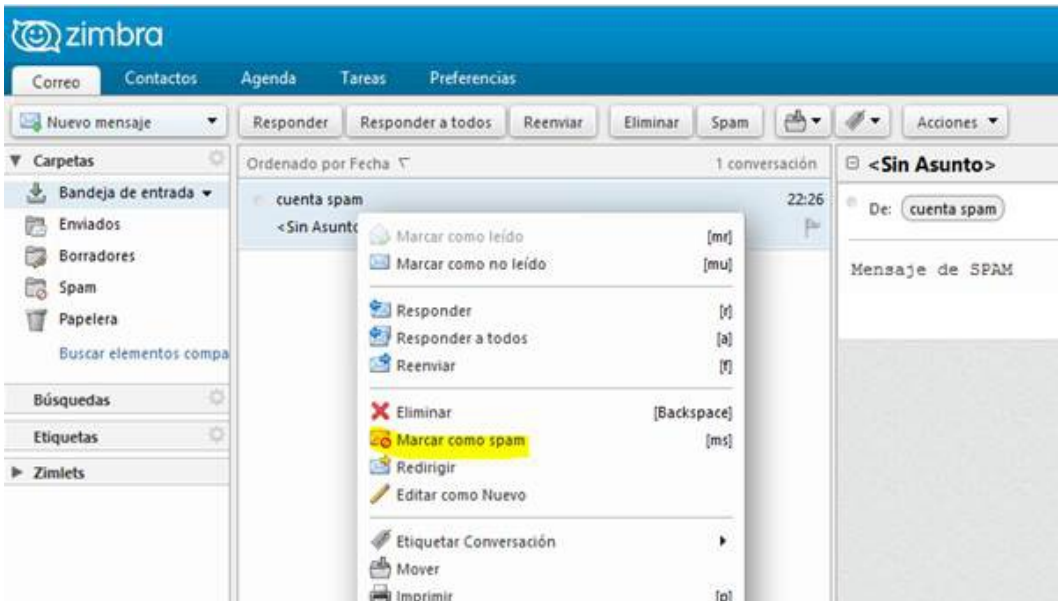
Para identificar dichas versiones, debe ejecutarse en consola los siguientes comandos:

```
/opt/zimbra/amavisd/sbin/amavisd -V

/opt/zimbra/libexec/sa-learn -V

/opt/zimbra/dspam/bin/dspam –version | head -2
```

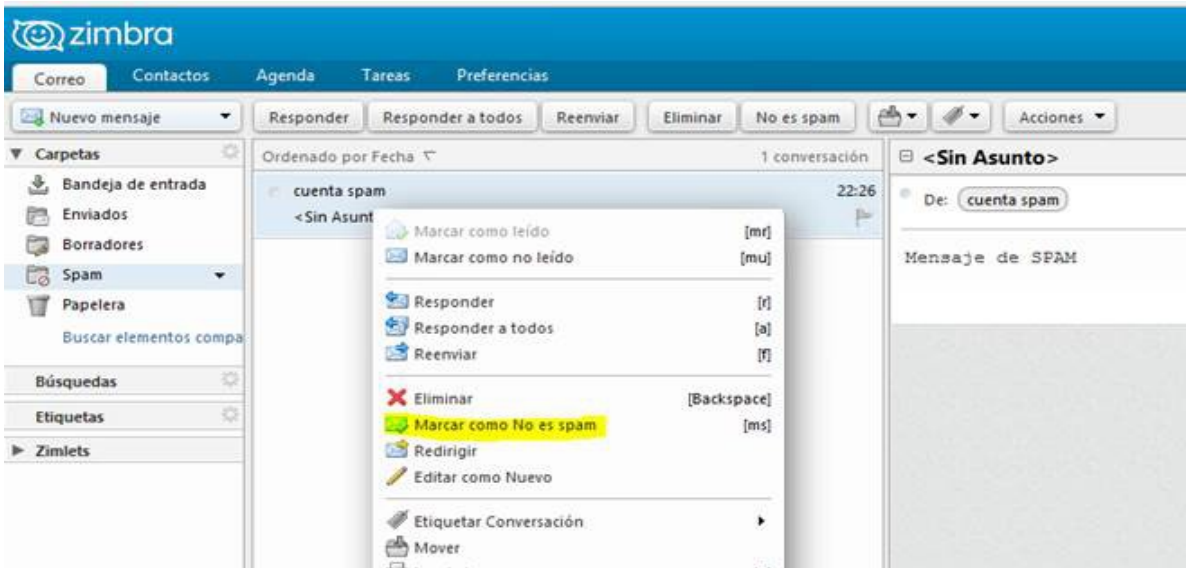
Obs.: debe ejecutarse con el usuario **zimbra**

Proceso para indicar que un correo es de tipo *spam*

El usuario final tiene la opción de marcar, desde su bandeja de entrada, el correo como *spam* utilizando un menú contextual, que se despliega con el botón derecho del ratón. Este mecanismo permite que el filtro *antispam* del servidor pueda intervenir con los nuevos correos que intenten llegar de dicha dirección.



Todos los mensajes que hemos marcado como *spam* llegan a una carpeta personal que se denomina **Spam**, sin embargo se puede deshacer la marcación (en caso de que nos hayamos equivocado) haciendo el proceso idéntico pero en dicha carpeta: esta opción es **Marcar como No es spam.**

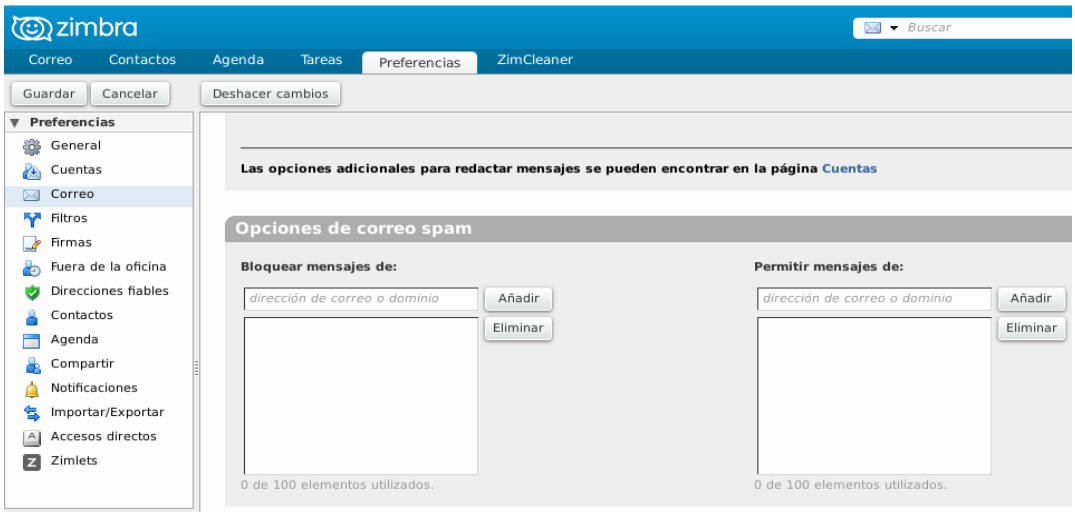


Al terminar este proceso el correo vuelve a la **Bandeja de entrada**.

Administración de listas blancas (*whitelist*) y negras (*blackList*)

Existe la posilidad de administrar las listas blancas y negras desde las preferencias del usuario. Dicha opción se encuentra ubicado bajo el menú:

Preferencias->Correo->Opciones de correo spam



Sistema de *Realtime Blackhole List* (RBL)

Las RBL's son listados de IPs que son detectados como posibles amenazas de spam, o que han sido detectados enviando spam.

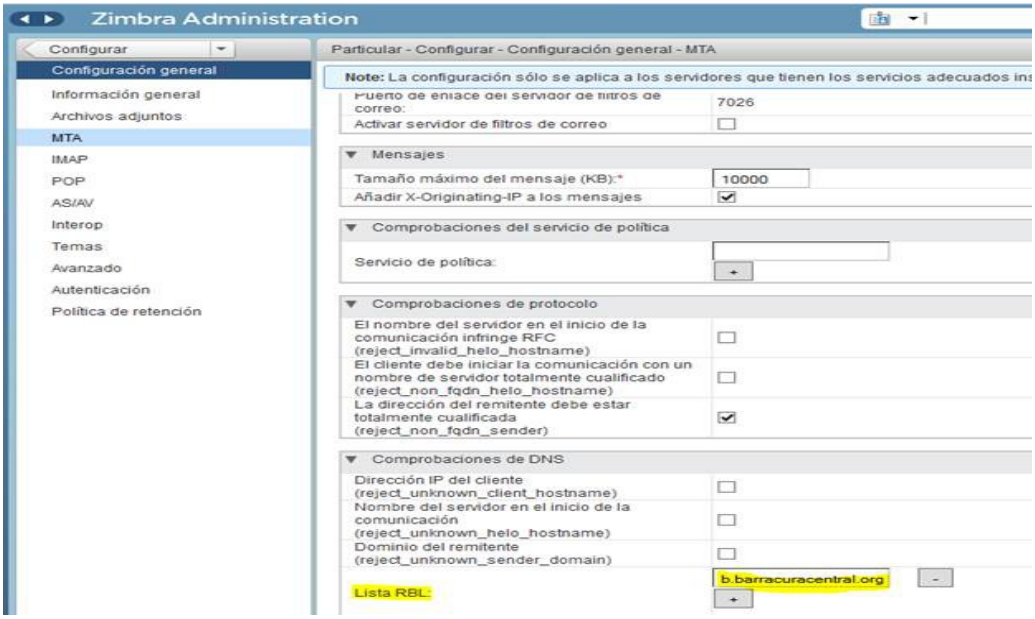
Con este sistema es posible evitar la recepción del correo electrónico desde un servidor que está registrado como *spammer*. Nuestro servidor -al inicio de la interacción- consulta una o varias listas en tiempo real, antes de decidir continuar con la recepción del mismo.

Las RBL's gratuitas más conocidas y usadas, son SpamHaus y Barracuda. Por ejemplo: para activar desde una consola la lista provista por "barracuda" se debe ejecutar:

```
zmprov mcf +zimbraMtaRestriction "reject_rbl_client b.barracuracentral.org"
```

Obs.: debe ejecutarse con el usuario **zimbra**

Una vez realizado lo anterior se puede utilizar la interfaz gráfica para agregar otras listas (p.ej.: la de spamhaus).



Enlaces de interés:

http://wiki.zimbra.com/wiki/SpamAssassin_Customizations

http://www.zimbra.com/support/support-offerings/product-lifecycle