

# Configuración en Zimbra para evitar SPAM

Antes de realizar cualquier cambio se recomienda realizar un backup de la configuración de zimbra para poder volver a la configuración inicial.

## Soluciones gratuitas

### Paso 1: Bloqueo con Postscreen

El Postfix de Zimbra ahora viene con Postscreen, una especie de firewall de correo electrónico entrante.

Ejecutar como usuario zimbra

```
zmpov mcf zimbraMtaPostscreenDnsblAction enforce
zmpov mcf zimbraMtaPostscreenGreetAction enforce
zmpov mcf zimbraMtaPostscreenNonSmtptCommandAction drop
zmpov mcf zimbraMtaPostscreenPipeliningAction enforce
zmpov mcf zimbraMtaPostscreenDnsblTTL 5m
```

### Paso 2: Bloqueo con verificaciones de protocolo DNS

Ejecutar como usuario zimbra

```
zmpov mcf +zimbraMtaRestriction reject_non_fqdn_sender
zmpov mcf +zimbraMtaRestriction reject_unknown_sender_domain
```

### Paso 3: Bloqueo de IPs de envío sospechoso

```
zmpov mcf +zimbraMtaRestriction "reject_rbl_client b.barracudacentral.org"
zmpov mcf +zimbraMtaRestriction "reject_rbl_client psbl.surriel.com"
```

```
zmprov mcf +zimbraMtaRestriction "reject_rbl_client cbl.abuseat.org"
```

## Paso 4: Bloqueo de ciertos archivos adjuntos sospechosos

```
zmprov mcf +zimbraMtaBlockedExtension asd
zmprov mcf +zimbraMtaBlockedExtension bat
zmprov mcf +zimbraMtaBlockedExtension cab
zmprov mcf +zimbraMtaBlockedExtension chm
zmprov mcf +zimbraMtaBlockedExtension cmd
zmprov mcf +zimbraMtaBlockedExtension com
zmprov mcf +zimbraMtaBlockedExtension dll
zmprov mcf +zimbraMtaBlockedExtension do
zmprov mcf +zimbraMtaBlockedExtension exe
zmprov mcf +zimbraMtaBlockedExtension hlp
zmprov mcf +zimbraMtaBlockedExtension hta
zmprov mcf +zimbraMtaBlockedExtension js
zmprov mcf +zimbraMtaBlockedExtension jse
zmprov mcf +zimbraMtaBlockedExtension lnk
zmprov mcf +zimbraMtaBlockedExtension ocx
zmprov mcf +zimbraMtaBlockedExtension pif
zmprov mcf +zimbraMtaBlockedExtension reg
zmprov mcf +zimbraMtaBlockedExtension scr
zmprov mcf +zimbraMtaBlockedExtension shb
zmprov mcf +zimbraMtaBlockedExtension shm
zmprov mcf +zimbraMtaBlockedExtension shs
zmprov mcf +zimbraMtaBlockedExtension vbe
zmprov mcf +zimbraMtaBlockedExtension vbs
zmprov mcf +zimbraMtaBlockedExtension vbx
zmprov mcf +zimbraMtaBlockedExtension vxd
zmprov mcf +zimbraMtaBlockedExtension wsf
zmprov mcf +zimbraMtaBlockedExtension wsh
zmprov mcf +zimbraMtaBlockedExtension xl
zmprov mcf +zimbraMtaBlockedExtensionWarnAdmin TRUE
zmprov mcf +zimbraMtaBlockedExtensionWarnRecipient TRUE
zmprov mcf zimbraVirusBlockEncryptedArchive FALSE
```

## Paso 5: Verificación de contenido de correo electrónico

```
zmprov mcf zimbraSpamKillPercent 75
zmprov mcf zimbraSpamTagPercent 20
zmprov mcf zimbraSpamSubjectTag "*** CUIDADO CORREO SOSPECHOSO**"
```

## Paso 6: Habilitar mayor información de logs

```
zmprov mcf zimbraAmavisLogLevel 2
```

## Paso 7: Personalizar SpamAssassin

```
nano ~/data/spamassassin/localrules/zsuser.cf
```

```
score DOS_OUTLOOK_TO_MX 0
score TO_EQ_FM_DIRECT_MX 0
score RCVD_IN_PBL 0.1
score RDNS_NONE 0.1
score FREEMAIL_FORGED_REPLYTO 4.0
score RCVD_IN_RP_RNBL 4.0
score FROM_FMBLA_NEWDOM 2.5
score FROM_NEWDOM_BTC 3.0
score __RCVD_IN_DNSWL 0.001
use_bayes 1
score BAYES_00 0
score BAYES_05 0
use_razor2 1
use_pyzor 1
pyzor_path /usr/bin/pyzor
pyzor_timeout 10
score RAZOR2_CHECK 2.0
score PYZOR_CHECK 2.0
```

## Paso 8: Instalar herramientas anti-spam (Pyzor and Razor)

### a) Instalar

```
nano /etc/yum.repos.d/epel.repo
```

```
[epel]
name=EPEL repository
baseurl=http://mirrors.kernel.org/fedora-epel/7/x86_64
enabled=1
gpgcheck=0
```

```
yum update
yum install pyzor perl-Razor-Agent
razor-admin -home=/opt/zimbra/data/amavisd/.razor -create
razor-admin -home=/opt/zimbra/data/amavisd/.razor -discover
razor-admin -home=/opt/zimbra/data/amavisd/.razor -register
```

## b) Configurando Pyzor

```
pyzor --homedir /opt/zimbra/data/amavisd/.pyzor discover

nano /opt/zimbra/data/spamassassin/localrules/sauser.cf
```

```
# pyzor
use_pyzor 1
pyzor_path /usr/bin/pyzor
pyzor_options -homedir /opt/zimbra/data/amavisd/.pyzor
# DNS lookups for pyzor can time out easily. Set the following line IF you want to give pyzor up to 20 seconds to
respond
# may slow down email delivery
pyzor_timeout 20

# razor
use_razor2 1

ok_languages en es
ok_locales en es
trusted_networks 127. 192.168.
use_bayes 1
skip_rbl_checks 0

# pyzor
```

```
use_pyzor 1
pyzor_path /usr/bin/pyzor

# DNS lookups for pyzor can time out easily. Set the following line IF you want to give pyzor up to 20 seconds to
respond
# may slow down email delivery
pyzor_timeout 20

# razor
use_razor2 1

score URIBL_BLACK 4.250
score RAZOR2_CHECK 3.250
score PYZOR_CHECK 3.250
score RP_MATCHES_RCVD -0.000
score BAYES_00 -1.000
score BAYES_20 1.000
score BAYES_50 1.500
score BAYES_60 1.800
score BAYES_80 2.100
score BAYES_90 2.500
score BAYES_99 2.900
score BAYES_999 3.800
```

```
chown -Rf zimbra:zimbra /opt/zimbra/data/spamassassin/localrules/sauser.cf
```

## c) Configurando Razor

```
mkdir /opt/zimbra/data/amavisd/.razor
chown -Rf zimbra:zimbra /opt/zimbra/data/amavisd/.razor
razor-admin -home=/opt/zimbra/data/amavisd/.razor -create
razor-admin -home=/opt/zimbra/data/amavisd/.razor -discover
razor-admin -home=/opt/zimbra/data/amavisd/.razor -register -user postmaster@dominio.gob.bo

su zimbra
cd /opt/zimbra/data/spamassassin/localrules
wget -N https://www.pccc.com/downloads/SpamAssassin/contrib/KAM.cf
```

# Soluciones de pago

## Invaluement

Subscribirse con una cuenta institucional : <https://www.invaluement.com/subscribe>, despues de 2 dias llegara a su correo el código de la licencia de prueba (valida para 7 dias)

Adicionar esta lista de bloqueo como usuario zimbra:

```
zmprov mcf zimbraMtaPostscreenDnsblSites 'b.barracudacentral.org=127.0.0.2*7' zimbraMtaPostscreenDnsblSites  
'sip-sip24.<licencia-enviada>.invaluement.com=127.0.0.2*6'  
zmprov mcf +zimbraMtaRestriction "reject_rbl_client sip-sip24.<licencia-enviada>.invaluement.com"
```

## Uribl

Subscribirse con una cuenta institucional y solicitar una cuenta de prueba: <https://admin.uribl.com/?section=datafeed;method=request> , (Elegir “Datafeed over DNS”) despues de un dia llegara a su correo el código de la licencia de prueba (valida para 30 dias).

Adicionar la IP del servidor de correos en [https://admin.uribl.com/?section=datafeed\\_acl](https://admin.uribl.com/?section=datafeed_acl)

Adicionar esta lista de bloqueo como usuario zimbra:

```
zmprov mcf +zimbraMtaRestriction "reject_rhsbl_client <licencia-enviada>.df.uribl.com"  
zmprov mcf +zimbraMtaRestriction "reject_rhsbl_reverse_client <licencia-enviada>.df.uribl.com"  
zmprov mcf +zimbraMtaRestriction "reject_rhsbl_sender <licencia-enviada>.df.uribl.com"
```

## Posibles errores

Un posible error encontrado es que MTA se encuentra en estado STOP en Zimbra, esto se puede deber a que el sistema operativo inicializó de forma previa postfix, para corregir esto se puede seguir los siguientes pasos:

```
$ systemctl stop postfix  
$ su zimbra  
$ postfix start
```

\$ zmcontrol start

---

Revision #3

Created 2 marzo 2023 17:33:10 by Vladimir Urquiola

Updated 10 abril 2024 11:05:56 by Franz Rojas