Capítulo 4.
Resultados de las pruebas

4.1 Correo Spam

Fueron enviados 33255 correos de la Subdirección de Seguridad de la Información UNAM/CERT desde la cuenta spamenvia@ingecomp.seguridad.unam.mx a la cuenta spamrecibe@devsecure.seguridad.unam.mx, el correo electrónico había sido previamente clasificado como correo “spam” o “posible spam” (véase tabla 4.1).

Tabla 4.1 Estadísticas de envío de correo Spam

Hora de inicio del envío	13:23.27, Jueves 8 de Octubre 2009
Hora de finalización del envío	14:59.52, Jueves 8 de Octubre 2009
Correos enviados	33255
Correos recibidos	22771
Correos regresados	0
Correos bloqueados	10484

```
33250 FROM: <raquino@seguridad.unam.mx>
Subject:  Your order
33251 FROM: <ruben@seguridad.unam.mx>
Subject:  RE: Message
33252 FROM: "=?windows-1251?B?QWphaSBDYXJwZW50ZXI=?=" <syamu@pesa.com>
Subject:  =?windows-1251?B?U3dpc3MgQnJhbmRlZCBXYXRjaGVz?=
33253 FROM: "Mattie Odom" <burgess@viatorians.com>
Subject:  Why overpay for medications when you can save on them?
Use of uninitialized value $from in concatenation (.) or string at /home/olopez/final_spam/scriptSp
ne 7905722.
33254 FROM:
Subject: <No Subject>


Hora de inicio: 13:23:27, Jueves Octubre 8, 2009
Hora de finalizacion: 14:59:52, Jueves Octubre 8, 2009
Numero de mensajes enviados: 33255
Numero de mensajes con attachments: 1152
```

33255 Correos enviados desde la cuenta spamenvia@ingecomp.seguridad.unam.mx

4.2 Correo con Virus

Se enviaron 1516 correos de la Subdirección de Seguridad de la Información UNAM/CERT desde la cuenta virusenvia@ingecomp.seguridad.unam.mx a la cuenta virusrecibe@devsecure.seguridad.unam.mx, el correo electrónico había sido previamente clasificado como correo con “virus” (véase tabla 4.2).

Tabla 4.2 Estadísticas de envío de correo Virus

Hora de inicio del envío	15:05.49, Jueves 8 de Octubre 2009
Hora de finalización del envío	15:15.26, Jueves 8 de Octubre 2009
Correos enviados	1516
Correos recibidos	73
Correos regresados	0
Correos bloqueados	1443

```
1509 FROM: arysa_love@yahoo.com.mx
Subject:  Spam
fileName: websitelist01.zip
1510 FROM: jcld_19@hotmail.com
Subject:  approved file
fileName: file.zip
1511 FROM: barry_gotlinsky@pall.com
Subject:  Re: Its me
fileName: your_doc.txt.pif
1512 FROM: cursos@seguridad.unam.mx
Subject:  Re: text
fileName: text.pif
1513 FROM: hosting@webcom.com.mx
Subject:  Spam
fileName: websitelist01_cursos.zip
1514 FROM: 3cventas@megacom.com.mx
Subject:  improved
fileName: message_cursos.zip
1515 FROM: ilein_gonzalez@merck.com
Subject:  Re: file
fileName: file_cursos.zip


Hora de inicio: 15:5:20, Jueves Octubre 8, 2009
Hora de finalizacion: 15:15:22, Jueves Octubre 8, 2009
Numero de mensajes enviados: 1516
Numero de mensajes con_attachments: 1176
```

1516 Correos enviados desde la cuenta virusenvia@ingecomp.seguridad.unam.mx

4.3 Correo Normal

Se enviaron 6460 correos de la Subdirección de Seguridad de la Información UNAM/CERT desde la cuenta normalenvia@ingecomp.seguridad.unam.mx a la cuenta normalrecibe@devsecure.seguridad.unam.mx, el correo se había clasificado previamente como correo normal, sin embargo, entre el correo enviado también se encontraba correo spam pero en una mínima cantidad aproximadamente del 5% (véase tabla 4.3).

Tabla 4.3 Estadísticas de envío de correo Normal

Hora de inicio del envío	17:16.21, Jueves 8 de Octubre 2009
Hora de finalización del envío	17: 34.34, Jueves 8 de Octubre 2009
Correos enviados	6460
Correos recibidos	5566
Correos regresados	0
Correos bloqueados	894

```
6449 FROM: "Jos Antonio Garc a Villarruel" <Protecciondelainformacion@spira.com.mx>
Subject: Contacto portal de Usuario Casero
6450 FROM: Servicio YouTube <service@youtube.com>
Subject: =?iso-8859-1?q?Tu_contrase=F1a_de_YouTube?=
6451 FROM: "cynthia" <cynthiasosaa@hotmail.com>
Subject: Contacto portal de Usuario Casero
6452 FROM: "Spiral" <spiraliamexico@gmail.com>
Subject: Contacto portal de Usuario Casero
6453 FROM: "jorge e. torres valdes" <jetpapy@prodigy.net.mx>
Subject: Contacto portal de Usuario Casero
6454 FROM: "Julio Tomas" <rbjt@proyectobsd.org>
Subject: Contacto portal de Usuario Casero
6455 FROM: "GABRIEL ALFONSO HERNANDEZ" <galfonso@correo.unam.mx>
Subject: Contacto portal de Usuario Casero
6456 FROM: Job Prieto <infoimexico@hotmail.com>
Subject: =?iso-8859-1?Q?ME_UNO_A_L?= =?iso-8859-1?Q?A_CAMPA=D1A_?= =?iso-8859-1?Q?DE_SEG
iso-8859-1?Q?TICA?=
6457 FROM: "Fernando Flores" <defectuoso7@hotmail.com>
Subject: Contacto portal de Usuario Casero
6458 FROM: "jose luis chavez gil" <jolucha2001@yahoo.com.mx>
Subject: Contacto portal de Usuario Casero
6459 FROM: "lucrecia magdalena benitez olivares" <magda_bo65@yahoo.com.mx>
Subject: Contacto portal de Usuario Casero


Hora de inicio: 17:16:21, Jueves Octubre 8, 2009
Hora de finalizacion: 17:34:34, Jueves Octubre 8, 2009
Numero de mensajes enviados: 6460
Numero de mensajes con attachments: 1120
```

6460 Correos enviados desde la cuenta normalenvia@ingecomp.seguridad.unam.mx

4.4 Prueba de carga de cpu y uso de memoria

Se realizó una prueba de carga enviando correo masivo desde cuatro diferentes cuentas para ver el comportamiento de cada una de las herramientas antispam.

El número de correos totales fue de 52980 que cada cuenta envió, entre cada inicio de envío se dejó un lapso de 2 minutos aproximadamente.

Cuentas para realizar el envío.

- mixtoenvia1@ingecomp.seguridad.unam.mx
- mixtoenvia2@ingecomp.seguridad.unam.mx
- mixtoenvia3@ingecomp.seguridad.unam.mx
- mixtoenvia4@ingecomp.seguridad.unam.mx

Cuentas para recibir el correo.

- mixtorecibe1@devsecure.seguridad.unam.mx
- mixtorecibe2@devsecure.seguridad.unam.mx
- mixtorecibe3@devsecure.seguridad.unam.mx
- mixtorecibe4@devsecure.seguridad.unam.mx

El envío de correo se realizó a las 18:02.59 hrs., del día 8 de Octubre del 2009 y finalizó a las 08:29.47 hrs., del día 9 de Octubre del 2009.

En el caso de esta herramienta no fue posible monitorear desde comandos ya que su interfaz desde la consola era limitada y solo se reducía a unas cuantas instrucciones para realizar la administración.

Como tal, la herramienta cuenta con sus propios gráficos para realizar el monitoreo de la memoria y su procesador.

En la figura 4.1 se muestra la actividad por semana, como se puede ver existe un pequeño incremento a partir del día 8 de octubre que fue cuando se realizaron las pruebas, sin embargo, según la herramienta el mayor porcentaje de carga en el procesador fue de 20%

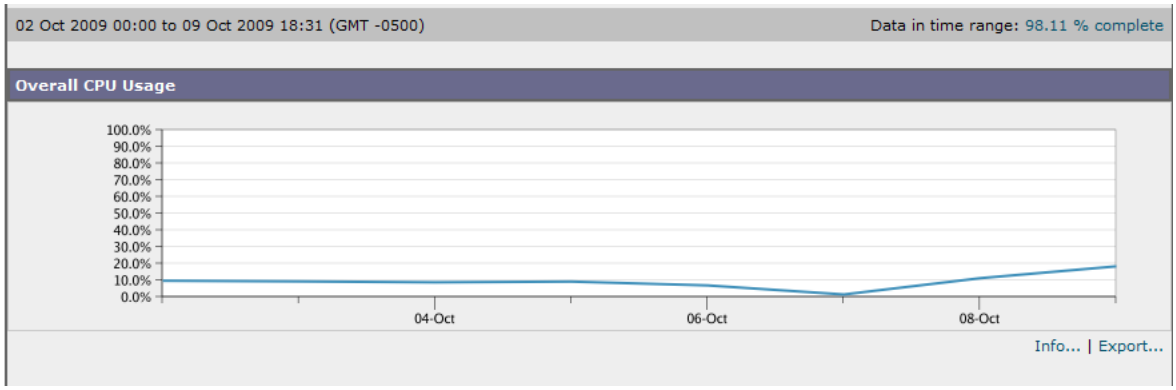

Figura 4.1 Actividad y carga de CPU de la herramienta Antispam analizada

La figura 4.2 muestra la carga de CPU por tarea, anti – spam, anti – virus, procesamiento de correos, reportes y cuarentena.

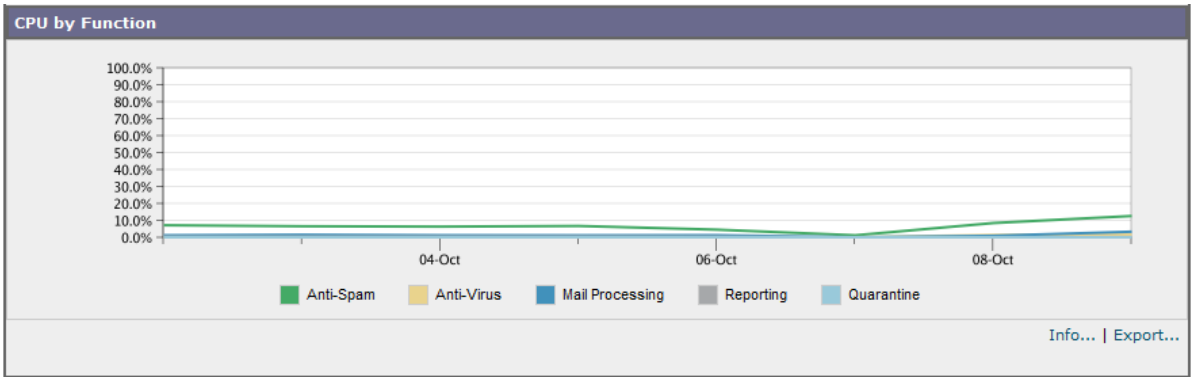

Figura 4.2 Carga de CPU por tarea realizada en la herramienta antispam

Estadísticas de envío de correo desde la cuenta mixtoenvia1@ingecomp.seguridad.unam.mx hacia la cuenta mixtorecibe1@devsecure.seguridad.unam.mx (véase tabla 4.4).

Tabla 4.4 Estadísticas de envío de correo mixto 1

Hora de inicio del envío	18:02.59, Jueves 8 de Octubre 2009
Hora de finalización del envío	08:24.35, Viernes 9 de Septiembre 2009
Correos enviados	52980
Correos recibidos	36570
Correos regresados	6

```
Subject:  Don't reject my calls!
52971 FROM: <webmaster@asc.unam.mx>
Subject:  Don't disappear now!
52972 FROM: "Linda F., Bellevue WA" <luculent@tpg.com.au>
Subject:  Attack your lady harder  S6LR
52973 FROM: "Beau Walker" <dandoviueltas@hotmail.com>
Subject:  NO SE QUEDE ATRAS EN LA INFORMACION
52974 FROM: "Thora Keri" <thorag_keribe@alden-smith.co.uk>
Subject:  _LoseWeight Natural SuperFood endorsed by Oprah Winfrey, FREE TRIAL 1 bottle,
l5
52975 FROM: <raquino@seguridad.unam.mx>
Subject:  Your order
52976 FROM: <ruben@seguridad.unam.mx>
Subject:  RE: Message
52977 FROM: "=?windows-1251?B?QWphaSBDYXJwZW50ZXI=?=" <syamu@pesa.com>
Subject:  =?windows-1251?B?U3dpc3MgQnJhbmRlZCBXYXRjaGVz?=
52978 FROM: "Mattie Odom" <burgess@viatorians.com>
Subject:  Why overpay for medications when you can save on them?
Use of uninitialized value $from in concatenation (.) or string at /home/olopez/final_s
ne 22357052.
52979 FROM:
Subject: <No Subject>


Hora de inicio: 18:2:59, Jueves Octubre 8, 2009
Hora de finalizacion: 8:24:35, Viernes Octubre 9, 2009
Numero de mensajes enviados: 52980
Numero de mensajes con attachments: 3462
```

52980 correos enviados desde mixtoenvia1@ingecomp.seguridad.unam.mx

Estadísticas de envío de correo desde la cuenta mixtoenvia2@ingecomp.seguridad.unam.mx hacia la cuenta mixtorecibe2@devsecure.seguridad.unam.mx (véase tabla 4.5).

Tabla 4.5 Estadísticas de envío de correo mixto 2

Hora de inicio del envío	18:04.49, Jueves 8 de Octubre 2009
Hora de finalización del envío	08:33.43, Viernes 9 de Octubre 2009
Correos enviados	52980
Correos recibidos	3561
Correos regresados	7

```
Subject:  Don't disappear now!
52972 FROM: "Linda F., Bellevue WA" <luculent@tpg.com.au>
Subject:  Attack your lady harder  S6LR
52973 FROM: "Beau Walker" <dandoviueltas@hotmail.com>
Subject:  NO SE QUEDE ATRAS EN LA INFORMACION
52974 FROM: "Thora Keri" <thorag_keribe@alden-smith.co.uk>
Subject:  _LoseWeight Natural SuperFood endorsed by Oprah Winfrey, FREE
l5
52975 FROM: <raquino@seguridad.unam.mx>
Subject:  Your order
52976 FROM: <ruben@seguridad.unam.mx>
Subject:  RE: Message
52977 FROM: "=?windows-1251?B?QWphaSBDYXJwZW50ZXI=?=" <syamu@pesa.com>
Subject:  =?windows-1251?B?U3dpc3MgQnJhbmRlZCBXYXRjaGVz?=
52978 FROM: "Mattie Odom" <burgess@viatorians.com>
Subject:  Why overpay for medications when you can save on them?
Use of uninitialized value $from in concatenation (.) or string at /home
ne 22357052.
52979 FROM:
Subject: <No Subject>


Hora de inicio: 18:4:49, Jueves Octubre 8, 2009
Hora de finalizacion: 8:33:43, Viernes Octubre 9, 2009
Numero de mensajes enviados: 52980
Numero de mensajes con attachments: 3462
```

52980 correos enviados desde mixtoenvia2@ingecomp.seguridad.unam.mx

Estadísticas de envío de correo desde la cuenta mixtoenvia3@ingecomp.seguridad.unam.mx hacia la cuenta mixtorecibe3@devsecure.seguridad.unam.mx (véase tabla 4.6).

Tabla 4.6 Estadísticas de envío de correo mixto 3

Hora de inicio del envío	18:07.29, Jueves 8 de Octubre 2009
Hora de finalización del envío	08:31.16, Viernes 9 de Octubre 2009
Correos enviados	52980
Correos recibidos	36554
Correos regresados	9

```
Subject:  NO SE QUEDE ATRAS EN LA INFORMACION
52974 FROM: "Thora Keri" <thorag_keribe@alden-smith.co.uk>
Subject:  _LoseWeight Natural SuperFood endorsed by Oprah Winfrey, FREE
l5
52975 FROM: <raquino@seguridad.unam.mx>
Subject:  Your order
52976 FROM: <ruben@seguridad.unam.mx>
Subject:  RE: Message
52977 FROM: "=?windows-1251?B?QWphaSBDYXJwZW50ZXI=?=" <syamu@pesa.com>
Subject:  =?windows-1251?B?U3dpc3MgQnJhbmRlZCBXYXRjaGVz?=
52978 FROM: "Mattie Odom" <burgess@viatorians.com>
Subject:  Why overpay for medications when you can save on them?
Use of uninitialized value $from in concatenation (.) or string at /home
ne 22357052.
52979 FROM:
Subject: <No Subject>


Hora de inicio: 18:7:29, Jueves Octubre 8, 2009
Hora de finalizacion: 8:31:16, Viernes Octubre 9, 2009
Numero de mensajes enviados: 52980
Numero de mensajes con attachments: 3462
```

52980 correos enviados desde mixtoenvia3@ingecomp.seguridad.unam.mx

Estadísticas de envío de correo desde la cuenta mixtoenvia4@ingecomp.seguridad.unam.mx hacia la cuenta mixtorecibe4@devsecure.seguridad.unam.mx (véase tabla 4.7).

Tabla 4.7 Estadísticas de envío de correo mixto 4

Hora de inicio del envío	18:10.11, Jueves 8 de Octubre 2009
Hora de finalización del envío	08:29.47, Viernes 9 de Octubre 2009
Correos enviados	52980
Correos recibidos	36555
Correos regresados	9

```
Subject:  NO SE QUEDE ATRAS EN LA INFORMACION
52974 FROM: "Thora Keri" <thorag_keribe@alden-smith.co.uk>
Subject:  _LoseWeight Natural SuperFood endorsed by Oprah Winfrey, FREE
l5
52975 FROM: <raquino@seguridad.unam.mx>
Subject:  Your order
52976 FROM: <ruben@seguridad.unam.mx>
Subject:  RE: Message
52977 FROM: "=?windows-1251?B?QWphaSBDYXJwZW50ZXI=?=" <syamu@pesa.com>
Subject:  =?windows-1251?B?U3dpc3MgQnJhbmRlZCBXYXRjaGVz?=
52978 FROM: "Mattie Odom" <burgess@viatorians.com>
Subject:  Why overpay for medications when you can save on them?
Use of uninitialized value $from in concatenation (.) or string at /home
ne 22357052.
52979 FROM:
Subject: <No Subject>


Hora de inicio: 18:10:11, Jueves Octubre 8, 2009
Hora de finalizacion: 8:29:47, Viernes Octubre 9, 2009
Numero de mensajes enviados: 52980
Numero de mensajes con attachments: 3462
```

52980 correos enviados desde mixtoenvia4@ingecomp.seguridad.unam.mx

4.5 Comparativa entre Herramientas

4.5.1 Envío de correo spam

Se realizó un envío de 33255 correos spam, el comportamiento fue el siguiente.

Tabla 4.8 Comparativa de envío de correo Spam

	Fecha/ hora de inicio	Fecha/hora de finalización	Tiempo de procesamiento	Correos enviados	Correos recibidos	Correos regresados	Correos bloqueados
Herramienta 1	27 Agosto 2009 15:57.39	27 Agosto 2009 16:31.41	33 minutos	33255	3286	1	29968
Herramienta 2	8 Septiembre 2009 13:34.06	8 Septiembre 2009 14:45.1	71 minutos	33255	21937	82	11235
Herramienta 3	8 Octubre 2009 13:23.27	8 Octubre 2009 14:59.52	96 minutos	33255	22771	0	10484

La herramienta 1 fue la que más correo spam bloqueó.

4.5.2 Envío de correo con virus

Se enviaron 1516 correos que contenían virus adjuntos, el comportamiento fue el siguiente (véase tabla 4.9).

Tabla 4.9 Comparativa de envío de correo con virus

	Fecha/ hora de inicio	Fecha/hora de finalización	Tiempo de procesamiento	Correos enviados	Correos recibidos	Correos regresados	Correos bloqueados
Herramienta 1	27 Agosto 2009 16:47.54	27 Agosto 2009 16:51.22	4 minutos	1516	230	3	1283
Herramienta 2	8 Septiembre 2009 13:44.49	8 Septiembre 2009 13:54.26	10 minutos	1516	54	97	1365
Herramienta 3	8 Octubre 2009 15:05.49	8 Octubre 2009 15:15.26	10 minutos	1516	73	0	1443

En la parte de virus la que tuvo mejor rendimiento fue herramienta 3, pues aunque la herramienta 2 recibió menos correo con spam (54) regresó 97 correos. Herramienta 3 no regresó ningún correo y por lo tanto bloqueó un número mayor de correos con virus.

4.5.3 Envío de correo normal

Se enviaron 6460 correos que se habían clasificado como correo normal, sin embargo, al realizar las pruebas se observó que existían correos spam, aunque en una mínima porción. La cantidad aproximada de spam que se encuentró dentro de esta prueba es de alrededor del 5% (véase tabla 4.10).

Tabla 4.10 Comparativa de envío de correo Normal

	Fecha/ hora de inicio	Fecha/hora de finalización	Tiempo de procesamiento	Correos enviados	Correos recibidos	Correos regresados	Correos bloqueados
Herramienta 1	27 Agosto 2009 17:12.58	27 Agosto 2009 17:24.55	12 minutos	6460	4042	9	2409
Herramienta 2	8 Septiembre 2009 15:51.05	8 Septiembre 2009 14:15.41	24 minutos	6460	5465	0	995
Herramienta 3	8 Octubre 2009 17:16.21	8 Octubre 2009 17: 34.34	18 minutos	6460	5566	0	894

La Herramienta 1 fue la que bloqueó más correo, sin embargo, al revisar en la cuarentena se observó que tenía más falsos positivos. La Herramienta 2, aunque bloqueó menos correos, igualmente contenía falsos positivos. La Herramienta 3 fue la que menos correo bloqueó y menos falsos positivos tuvo.

4.5.4 Envío de correo mixto

La última prueba que se realizó fueron envíos de correo con virus, spam y normal desde cuatro cuentas diferentes, con el fin de verificar el tiempo de procesamiento, el desempeño de cada herramienta con respecto al bloqueo de correos y la carga en el equipo antispam. Se enviaron 52980 correos por cada cuenta (véase tabla 4.11).

Tabla 4.11 Comparativa de envío de correo Mixto

	Fecha/ hora de inicio	Fecha/hora de finalización	Tiempo de procesamiento	Correos enviados	Correos recibidos	Correos regresados	Correos bloqueados
Herramienta 1	4 Septiembre 2009 12:59.47	4 Septiembre 2009 20:02.57	7 horas 4 minutos	52980	9767	290	42923
	4 Septiembre 2009 13:02.00	4 Septiembre 2009 20:19.40	7 horas 17 minutos	52980	9786	154	43040
	4 Septiembre	4 Septiembre	7 horas	52980	9755	154	43071

	2009 13:04.00	2009 20:21.20	17 minutos				
	4 Septiembre 2009 13:06.02	4 Septiembre 2009 20:22.6	7 horas 16 minutos	52980	9807	421	42752
Herramienta 2	9 Septiembre 2009 14:38.49	9 Septiembre 2009 22:44.22	8 horas 6 minutos	52980	36184	412	16384
	9 Septiembre 2009 14:42.01	9 Septiembre 2009 23:01.38	8 horas 19 minutos	52980	36295	439	16246
	9 Septiembre 2009 14:45.02	9 Septiembre 2009 23:05.25	8 horas 20 minutos	52980	36213	477	16290
	9 Septiembre 2009 14:48.06	9 Septiembre 2009 23:06.08	8 horas 18 minutos	52980	36023	474	16483
Herramienta 3	8 Octubre 2009 18:02.59	9 Octubre 2009 08:24.35	14 horas 22 minutos	52980	36570	6	16404
	8 Octubre 2009 18:04.49	9 Octubre 2009 08:33.43	14 horas 29 minutos	52980	36561	7	16412
	8 Octubre 2009 18:07.29	9 Octubre 2009 08:31.16	14 horas 24 minutos	52980	36554	9	16417
	8 Octubre 2009 18:10.11	9 Octubre 2009 08:29.47	14 horas 19 minutos	52980	36555	9	16416

La Herramienta 1 tuvo un mejor rendimiento en cuanto a tiempo ya que el promedio fue de 7 horas con 12 minutos aproximadamente, sin embargo, existieron algunas inconsistencias ya que se usó el mismo script, el mismo buzón de correos y los resultados aparecieron disparados pues en alguna ocasión los correos regresados fueron 154 y en otra 421, además fue la herramienta que bloqueó más correos, La Herramienta 2 igualmente tuvo un procesamiento de 8 horas con 15 minutos en promedio y tuvo un mejor rendimiento en cuanto a los correos bloqueados y los correos recibidos. La Herramienta 3 fue la que más tiempo se llevó en procesar los correos, sin embargo, fue la que tuvo más consistencias entre los correos recibidos y los correos bloqueados.