Cuánto conocen los usuarios sobre el Phishing

*Durante dos meses **Segu-Info** ha llevado adelante una encuesta para conocer cómo reaccionan los usuarios ante un caso de Phishing, si saben reconocerlo y, sobre todo, como proceden luego de hacerlo ya que de esa decisión depende el bloqueo y la baja del engaño llevado adelante cada vez más frecuentemente por los delincuente en América Latina.*

Autor: Lic. Cristian Borghello CISSP-MVP
Versión: 1.0 (20110402)

Procedimiento

La encuesta fue realizada por **Segu-Info** en los meses de febrero y marzo de 2011 y fue respondida de manera anónima y opcional por 1.314 usuarios cuyos perfiles son aquellos que habitualmente se interesan por temas de Seguridad de la Información y son visitantes asiduos de Segu-Info y su Blog de noticias.

Este último dato es importante ya que no debe considerarse que quienes respondieron son usuarios normales de correo electrónico y ello también se verá reflejado en las respuestas analizadas.

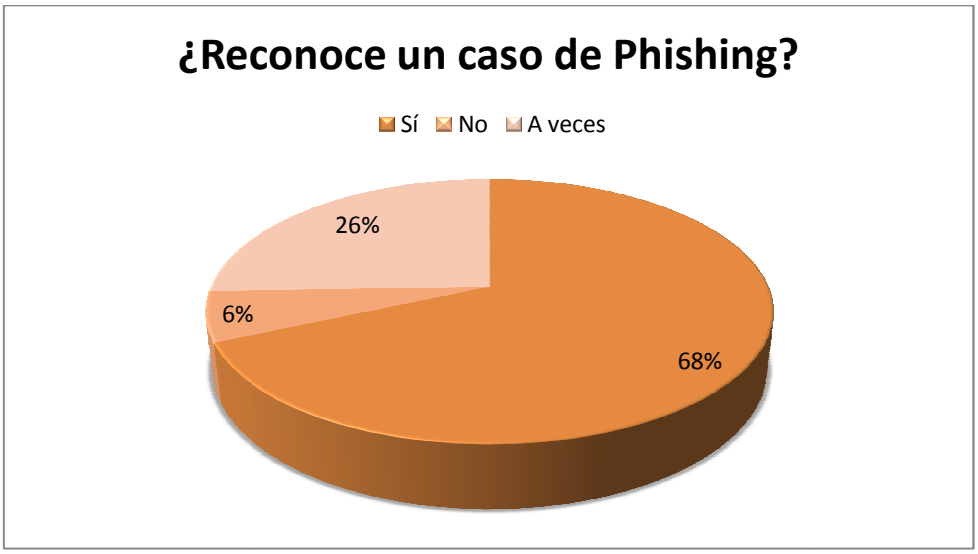
La encuesta completa de opciones múltiples para cada pregunta puede encontrarse en el Anexo, así como los datos crudos recolectados al finalizar la misma.

Análisis de datos

A continuación se analizan cada una de las preguntas y las respuestas dadas por los usuarios.

Pregunta 1

Inicialmente se preguntó a los usuarios si creían saber reconocer un caso de Phishing cuando el mismo arribaba a sus correos electrónicos. Como era de esperarse, considerando el perfil de usuarios que respondieron la encuesta, el 68% dijo conocer positivamente un correo que pretende engañarlo para robar sus datos sensibles.



Es curioso notar que el 6% de los usuarios dice no saber reconocer un correo electrónico fraudulento.

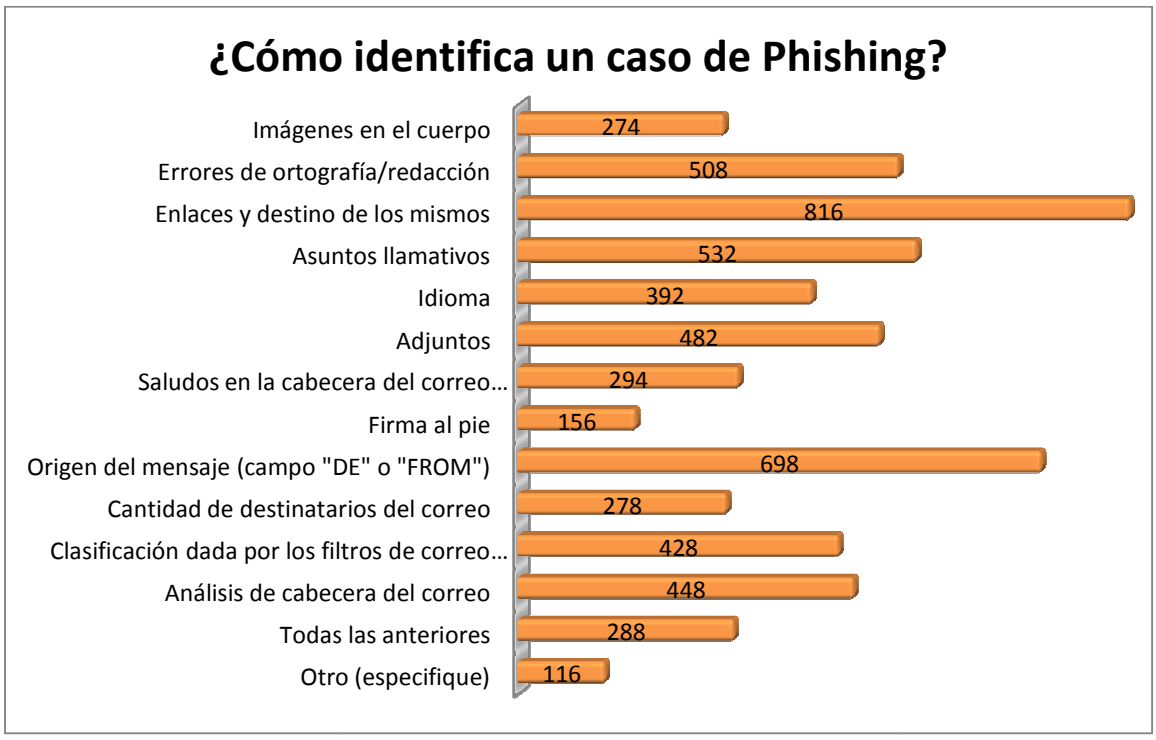
Si bien la mayoría manifiesta que puede reconocer un mensaje falso, a medida que se avance sobre el análisis de los resultados, se comprobará que esto no es del todo acertado ya que suele confundirse al Spam o al Scam con el Phishing.

Esta situación genera una **falsa sensación de seguridad** en los usuarios porque efectivamente ellos "creen" que pueden identificar un caso de Phishing, lo que los vuelve más propensos a caer en la trampa cuando el correo recibido esté correctamente manipulado y sus autores hayan puesto mayor esfuerzo en hacerlo pasar por verdadero.

Pregunta 2

Con el objetivo de conocer cuáles son las principales características que se observan en un correo para identificarlo como Phishing, esta pregunta brinda las distintas opciones que pueden considerarse al momento de evaluar un mensaje como falso. En este caso cada usuario podía marcar todas las opciones que considerara adecuadas.

Aquí comienza a observarse lo planteado en la pregunta anterior ya que la mayoría de los usuarios, 816 de ellos, dice observar si el correo contiene un enlace pero 698 observan el campo DE/FROM del correo recibido. Esto indica que, en muchos casos, se desconoce que el correo efectivamente puede ser creado apócrifamente falseando esos campos (*spoofing*) y, por lo tanto quienes observen sólo ese dato podrían ser engañados por el delincuente.



De todas formas, son muy pocos los usuarios que observan una sola de todas las características propuestas.

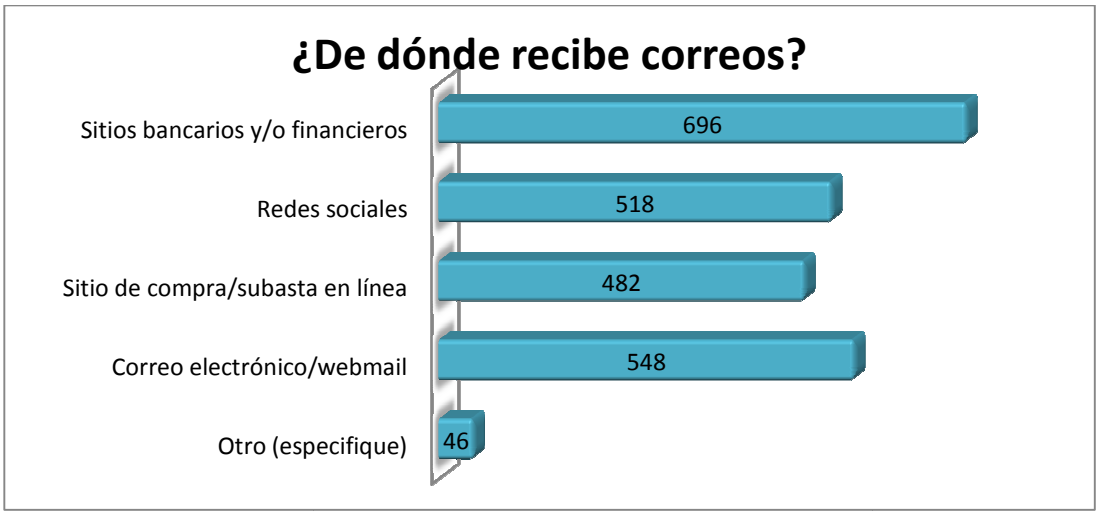
Por otro lado 116 dicen considerar otras opciones, entre ellas:

- Observar que el enlace contenga HTTPS.
- Recepción de correos de entidades en las cuales el usuario no tiene cuenta.
- Existencia de URL cortas.
- Tipos y cantidad de datos solicitados: si el usuario sólo evalúa la cantidad de información solicitada, es un indicio de que podría ser fácilmente engañado.

- Conocimiento del remitente: una vez más queda en evidencia que algunos usuarios desconocen que el remitente de un correo puede ser manipulado.
- Diseño o aspecto visual del mensaje: ¿un correo más “bonito” indica su veracidad?
- Algunos usuarios dicen que observan si se trata de un premio, una lotería o un correo con promociones de productos farmacéuticos o a buen precio; lo cual nuevamente comprueba la confusión existente entre Spam, Scam y Phishing.
- Buscar el caso en Internet, lo cual valida la importancia de lo realizado desde **Segu-Info**, publicando información sobre cada uno de los casos de Phishing recibidos y analizados, para que los usuarios puedan comprobar fácilmente si se trata de un engaño.

Pregunta 3

En esta pregunta se desea conocer cuáles son las entidades de las cuales es más común recibir correos electrónicos falsos. En este caso los sitios bancarios/financieros se llevan el primer puesto, seguidos muy de cerca por el Phishing de redes sociales, los webmail y los sitios de compra/venta/subasta de productos.



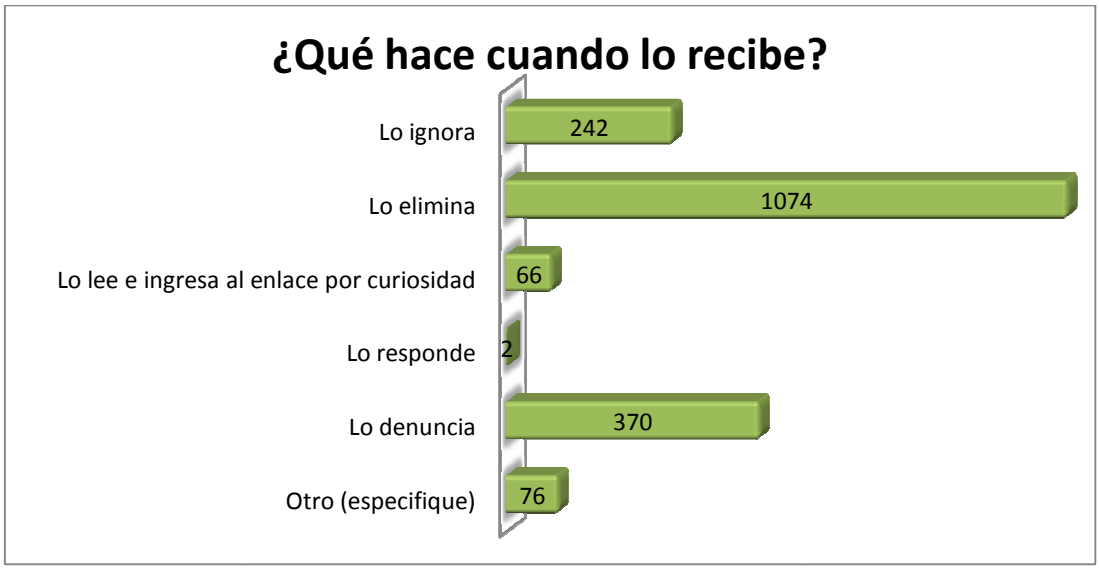
Este resultado deja claro que efectivamente debe prestarse la misma atención a cualquier tipo de correo falso ya que los delincuentes no dudan en utilizar todos los medios a su disposición para obtener información sensible del usuario.

Aquí también es importante destacar que cualquiera de los datos robados podría ser utilizado posteriormente por el delincuente para ingresar a otro tipo de cuenta ya que **8 de cada 10 usuarios utiliza la misma combinación de usuario y contraseña como datos de acceso** para ingresar al *home-banking* y a su cuenta de correo o red social. Por lo tanto si un delincuente obtiene los datos de acceso al correo de un usuario, también estará en condiciones de ingresar a su cuenta bancaria o a su red social y efectuar un robo de identidad.

Otros usuarios, demostrando nuevamente la confusión existente con el Spam, dicen recibir correos de promociones farmacéuticas, productos electrónicos, software, regalos, ofertas, loterías y promociones, además de correos con archivos adjuntos.

Pregunta 4

En este caso se desea conocer qué hace el usuario cuando recibe un correo que identifica como falso y no es sorpresa averiguar que la mayoría (1074 usuarios) lo elimina, muchos simplemente lo ignoran y otros (370) afortunadamente lo reportan (ver siguiente pregunta) para que las entidades competentes puedan proceder a su bloqueo e investigación técnica y legal.



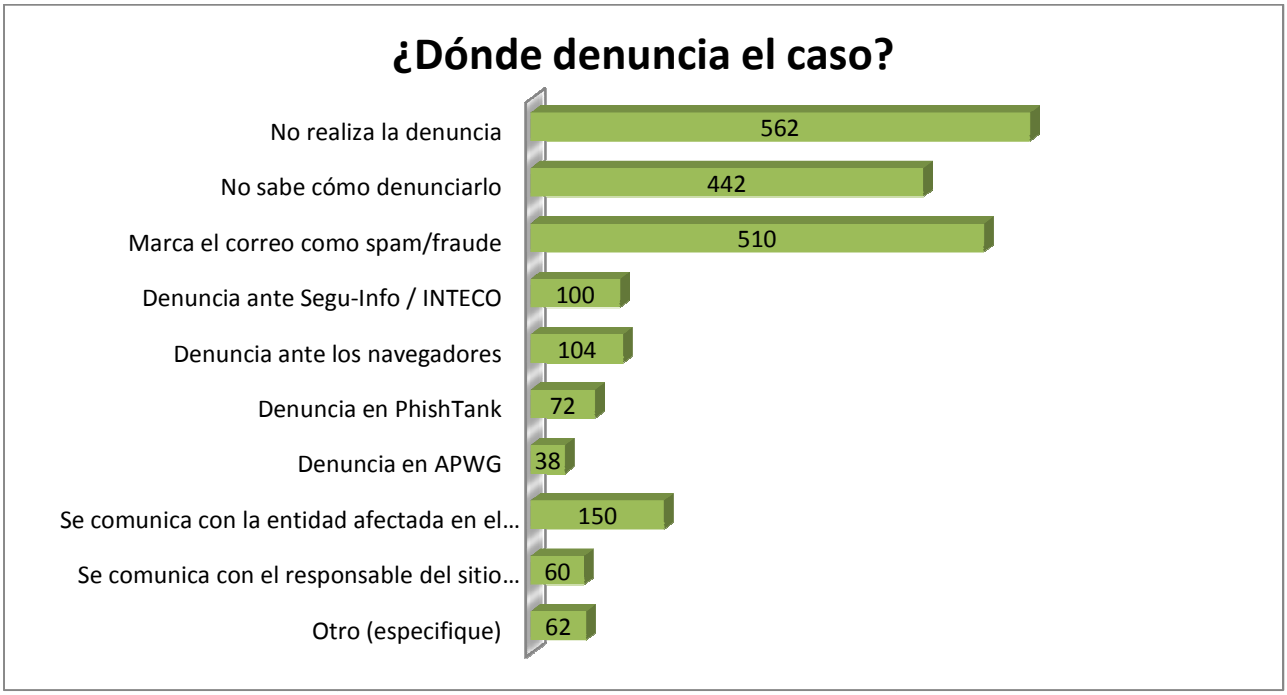
En este caso debe llamarse la atención sobre dos aspectos fundamentales: por un lado, la importancia de que haya más usuarios responsables que reporten y, por otro, la curiosidad de algunos usuarios que ingresan al sitio falso para averiguar su procedencia. En este caso es importante que quien lo haga, respete ciertas medidas de seguridad para evitar daños en sus cuentas o sistemas personales: es recomendable el uso máquinas virtuales en este análisis y por supuesto jamás utilizar datos verdaderos en las pruebas realizadas.

Entre las demás respuestas se destaca la presencia de usuarios que marcan el correo como Spam, otros que proceden a analizarlo por *hobbie* o porque su trabajo así lo requiere, o aquellos que agregan el remitente o la dirección IP a una lista negra para bloqueos futuros.

Pregunta 5

Cuando se pregunta dónde reportan el correo o sitio falso (en caso de hacerlo), el 42% de los usuarios dice no denunciar los casos de Spam que recibe y el 78% de ellos reconocen no saber cómo hacerlo.

Segu-Info recibe denuncias de Phishing vía correo electrónico a phishing [arroba] segu.info.com.ar y a través de su formulario de denuncias.



En lo que respecta a quienes realizan alguna acción con el correo, la mayoría sólo dice marcarlo como Spam o fraude en su cliente de correo electrónico, navegador o webmail.

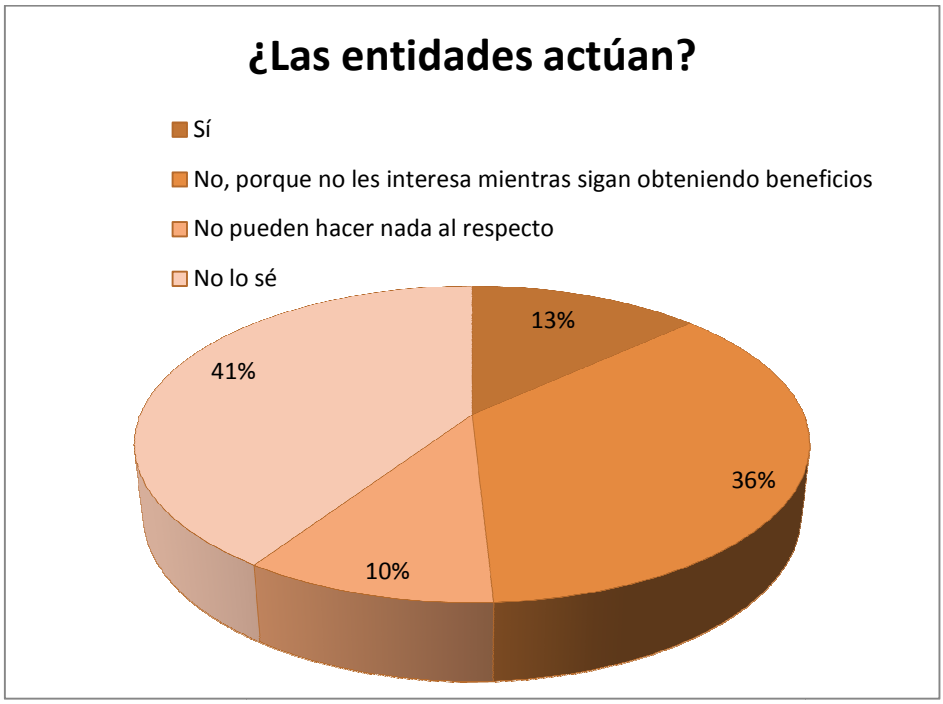
Otros, en cambio en una actitud más responsable y activa se comunican con la entidad afectada o con distintas organizaciones, como **Segu-Info**, para que se proceda a la investigación del caso y al bloqueo del mismo.

Entre quienes respondieron otras opciones se destaca que la mayoría lo hace a la unidad de delitos informáticos de la policía de sus respectivos países.

Pregunta 6

Esta última pregunta estaba orientada a conocer la opinión de los usuarios sobre las actividades que realizan (o no) las entidades afectadas por los casos de Phishing.

El 46% de los usuarios dice no saber qué hacen las entidades afectadas lo cual refleja que evidentemente estas deben realizar mayores esfuerzos en comunicarse con sus clientes y usuarios y explicar cuáles son los procedimientos llevados a cabo en caso de detectar un correo o sitio falso.



Por otro lado, el 36% de los usuarios dice que las entidades no hacen nada al respecto porque la ecuación costo/beneficio les sigue siendo positivo y entonces optan por ocultar los casos y reembolsar el dinero que cualquier afectado pueda perder en un caso de Phishing.

Lamentablemente esta política aún es seguida por muchas entidades bancarias de América Latina e incluso en algunos países las leyes de protección del ciudadano y consumidor han comenzado a castigar a aquellas entidades que realicen ninguna acción, lo cual debería ser entendido como un llamado de atención y así estas entidades deberían comenzar a actuar en forma responsable ante sus clientes.

Finalmente el 13% de los usuarios dice que efectivamente las entidades hacen algo al respecto y el 10% restante piensa que las entidades no pueden hacer nada, lo cual, al parecer coincide con la opinión de los responsables de dichas entidades ya que, luego de más de una década de existencia del Phishing, las mismas siguen sin actuar.

Conclusiones

Los resultados obtenidos por la encuesta de **Segu-Info** dejan en evidencia algunos factores que no deben pasar desapercibidos por usuarios y entidades afectadas:

- Muchos usuarios dicen reconocer un caso de Phishing pero lo confunden con otros tipos de amenazas como el Spam y el Scam. Algunas veces se suele pensar que se conoce sobre un tema pero este pensamiento atenta contra la seguridad y es un indicador de falta de educación en dicho área. Este punto también queda en evidencia cuando la mayoría de los usuarios dice no saber cómo proceder delante de un caso de Phishing confirmado.
- Existe una clara falta de compromiso con la denuncia y la persecución de casos de correos y sitios falsos y esto facilita el trabajo de los delincuentes.
- Ante la falsa creencia de que el Phishing es sólo financiero, se demuestra que existen correos falsos de cualquier tipo y los mismos pueden ser utilizados de igual manera para robar todo tipo de información sensible.
- Los usuarios desconocen si sus entidades los protegen o no ante este tipo de fraudes.
- Las entidades ocultan los casos de Phishing y los procedimientos de prevención y solución (si los hay). Esta no es una política adecuada para defender a sus clientes, sobre todo con las tasas actuales de crecimiento de este tipo de fraudes y estafas.

Desde **Segu-Info** esperamos que este tipo de estudios sean más frecuentes y puedan reflejar con claridad que es necesario un mayor esfuerzo en educar, capacitar y hacer conocer este tipo de fraudes porque, hasta ahora los delincuentes llevan todas las de ganar y parece existir un acuerdo tácito entre los usuarios y las entidades afectadas para no hacer nada al respecto.

Anexo – Encuesta

¿Cree que sabe reconocer un correo electrónico falso?	
Sí	898
No	80
A veces	336
2. ¿Qué observa para reconocer un correo falso?	
Imágenes en el cuerpo	274
Errores de ortografía/redacción	508
Enlaces y destino de los mismos	816
Asuntos llamativos	532
Idioma	392
Adjuntos	482
Saludos en la cabecera del correo ("Estimado...")	294
Firma al pie	156
Origen del mensaje (campo "DE" o "FROM")	698
Cantidad de destinatarios del correo	278
Clasificación dada por los filtros de correo (spam o correo falso)	428
Análisis de cabecera del correo	448
Todas las anteriores	288
Otro (especifique)	116
¿De qué tipo de entidad recibe mayor cantidad de correos falsos?	
Sitios bancarios y/o financieros	696
Redes sociales	518
Sitio de compra/subasta en línea	482
Correo electrónico/webmail	548
Otro (especifique)	46
4. ¿Qué hace en el caso de reconocer un correo falso?	
Lo ignora	242
Lo elimina	1074
Lo lee e ingresa al enlace por curiosidad	66
Lo responde	2
Lo denuncia	370
Otro (especifique)	76
5. ¿Dónde denuncia los correos falsos?	

No realiza la denuncia	562
No sabe cómo denunciarlo	442
Marca el correo como spam/fraude	510
Denuncia ante Segu-Info / INTECO	100
Denuncia ante los navegadores	104
Denuncia en PhishTank	72
Denuncia en APWG	38
Se comunica con la entidad afectada en el correo	150
Se comunica con el responsable del sitio web donde está alojado el sitio falso	60
Otro (especifique)	62
6. ¿Cree que las entidades hacen lo necesario para evitar los casos de Phishing?	
Sí	174
No, porque no les interesa mientras sigan obteniendo beneficios	472
No pueden hacer nada al respecto	134
No lo sé	534