

MEMORANDO

“Caracterização da Actuação no Combate ao spam”

Análise das respostas ao questionário

ÍNDICE

1. Enquadramento da realização do questionário.....	3
2. Análise das respostas ao questionário	4
2.1 Questão 1 - Que medidas são adoptadas com vista à promoção da segurança dos serviços prestados?	4
2.2 Questão 2 - Para a prossecução destas medidas, o trabalho é desenvolvido em cooperação com os operadores de redes públicas de comunicações?	5
2.3 Questão 3 - Como é que mantém a actualização em relação aos desenvolvimentos no enquadramento segurança e custos inerentes à adopção de um nível apropriado de segurança?	6
2.4 Questão 4 - Como é que se mantém informado acerca de problemas de segurança informática e SPAM?	7
2.5 Questão 5 - Que medidas adopta quando detecta uma falha no sistema de segurança inerente ao serviço que presta?	7
2.6 Questão 6 - Qual o procedimento adoptado, se a adopção de medidas adequadas não depende da sua empresa?.....	8
2.7 Questão 7 - Quais as medidas preventivas aconselhadas aos clientes relativamente ao envio de SPAM?	9
2.8 Questão 8 - Quais as medidas adoptadas para preservar os clientes de receberem SPAM?	10
2.9 Questão 9 - Que medidas preventivas são adoptadas como combate às situações de fraude de identidade? É implementado algum mecanismo de autenticação?	11
2.10 Questão 10 - Que medidas adopta quando verifica que as mensagem de SPAM são provenientes de prestadores de serviços de acesso à Internet sediados no país? E se forem provenientes de prestadores de serviços sediados na Europa? E ainda se forem prestadores de serviços sediados fora da União Europeia?	12
3. Principais conclusões	13

1. Enquadramento da realização do questionário

Em Maio de 2008 foi lançado um inquérito para diagnóstico de caracterização da actuação no combate a comunicações não solicitadas (spam) pelos prestadores de acesso à Internet e prestadores de serviço de correio electrónico.

Este questionário pretendeu estender-se ao universo dos ISP registados¹ na ANACOM. De um total de 36 empresas, recebeu-se resposta por parte de 18² e é nesta base que é realizado o presente relatório.

O formulário do questionário consta do anexo, tendo sido divulgado no sítio da Internet da ANACOM³. A solicitação de participação na resposta ao questionário foi igualmente realizada por ofício.

Dado ser a primeira vez que a ANACOM realiza este questionário, optou-se por questões abertas, em que não são formuladas rigidamente as respostas possíveis, antes se apresentaram opções de resposta como exemplo. Se por um lado esta metodologia pode contribuir para alguns desvios resultantes da necessária interpretação da resposta, por forma a agrupar e daí tirar conclusões para o todo, a opção alternativa em que se indicariam opções de resposta rígidas, poderia revelar-se inadequado face à realidade e experiência de actuação das empresas nacionais.

O formulário do questionário teve na base um questionário promovido pela ENISA⁴. Para além da confiança que este facto traduz, o formulário do questionário foi ainda avaliado positivamente por parte de alguns dos operadores previamente contactados.

O diagnóstico resultante do inquérito pretende ser o primeiro passo para traçar, concertadamente com os ISP, acções de combate a spam.

¹ [Prestadores do serviço de acesso à internet fixa em actividade - 1º trimestre 2008](#)
[Prestadores do Serviço de Acesso à Internet de Banda Larga Fixa - 1º trimestre de 2008](#)
[Prestadores com oferta de Serviços de Banda Larga Móvel - 1º trimestre de 2008](#)

² Empresas que responderam ao inquérito: Bragatel, Cabovisão, PT Comunicações, PT Wi-Fi, PT Prime, ReferTelecom, SemCabo, Tvtel, Vodafone, Cyclopinet, TMN, Connex, Fleximédia, Sonaecom, NSFI, Zon TV Cabo, Nortenet, Claranet

³ Página Inicial : Comércio Electrónico : Spam - Combate a comunicações não solicitadas : Questionário - Combate a comunicações não solicitadas -
<http://www.anacom.pt/template12.jsp?categoryId=275882>

⁴ [Provider Security Measures – ENISA - 2006](#)

A realização deste inquérito tem também como objectivo formular uma base de contactos de ISP que permita uma melhor interacção para futuras acções que venham a ser implementadas para o combate ao spam.

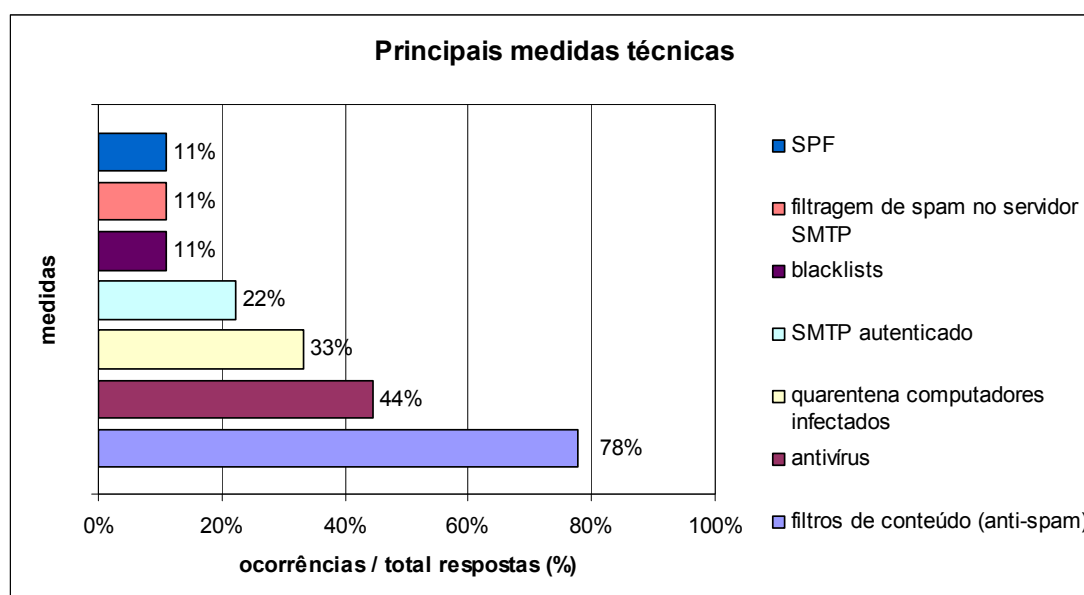
2. Análise das respostas ao questionário

Dado que as questões formuladas são abertas, existe a possibilidade de resposta múltipla (indicação de vários aspectos numa mesma resposta). Este facto faz com que a soma das percentagens que forem sendo referidas durante a análise não seja 100%.

2.1 Questão 1 - Que medidas são adoptadas com vista à promoção da segurança dos serviços prestados?

A resposta foi segmentada por dois tipos de actuação – medidas técnicas e medidas organizacionais.

Nas medidas técnicas destacam-se os filtros anti-spam e anti-vírus, com 78% e 44% das empresas a referi-los.



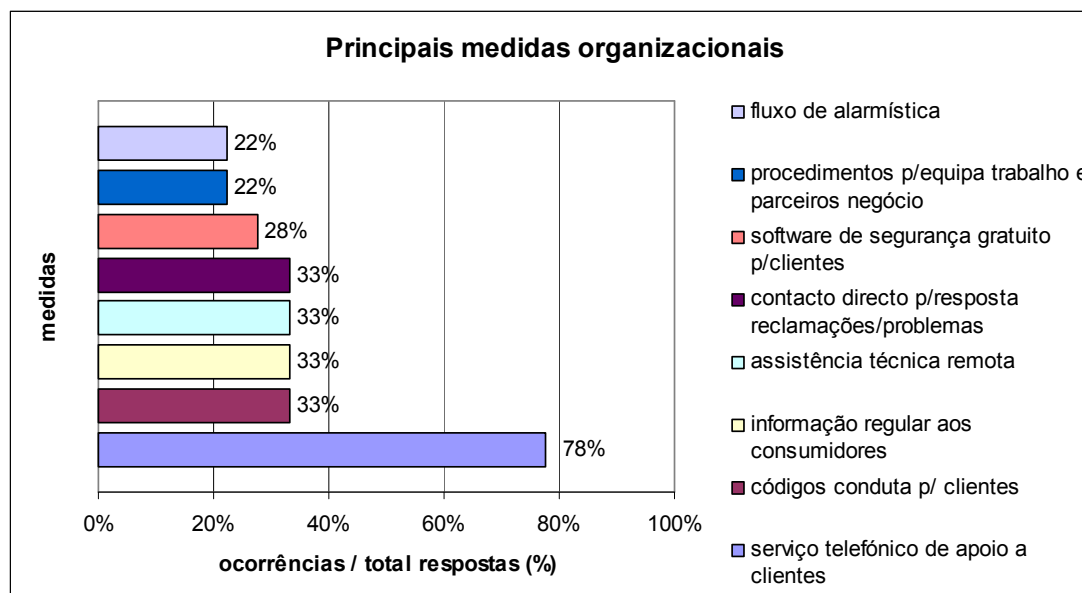
SPF - Sender Policy Framework⁵

SMTP - Simple Mail Transfer Protocol⁶

⁵ Sender Policy Framework ou SPF é um sistema que evita que outros domínios (endereço da internet) enviem emails não autorizados em nome de um domínio.

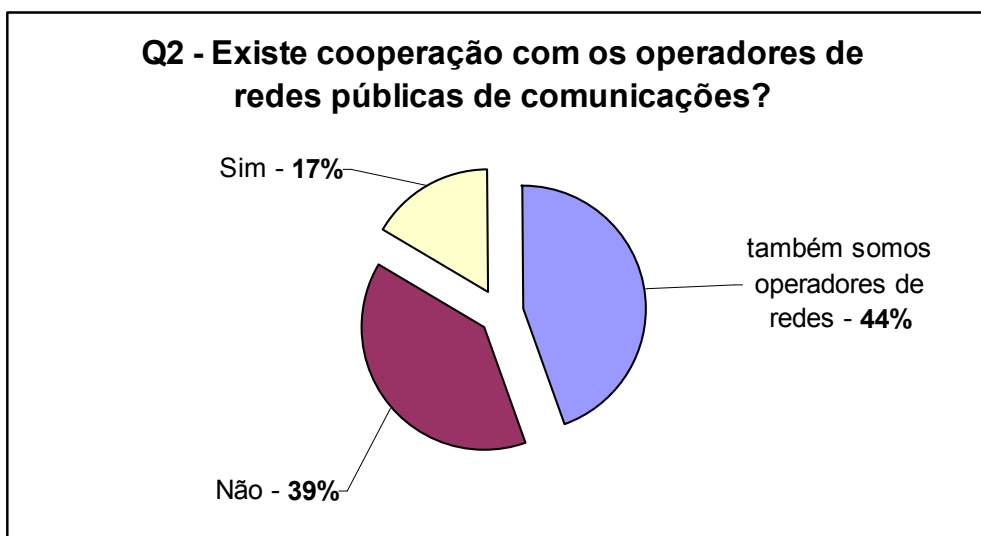
⁶ Simple Mail Transfer Protocol ou SMTP é o protocolo padrão para envio de e-mails através da Internet.

Nas medidas organizacionais, são particularmente relevantes o serviço telefónico de apoio a clientes (78%) e a existência de códigos de conduta ou de regras para utilização dos serviços, referindo a questão do spam (33%).



2.2 Questão 2 - Para a prossecução destas medidas, o trabalho é desenvolvido em cooperação com os operadores de redes públicas de comunicações?

44% dos respondentes afirmam acumular a prestação de serviços de acesso à Internet e correio electrónico com a gestão da rede, depreendendo-se daqui que a acção será concertada. Dos restantes, a maioria (7 empresas em 18 respondentes) actua de forma não coordenada com os operadores de redes.



2.3 Questão 3 - Como é que mantém a actualização em relação aos desenvolvimentos no enquadramento segurança e custos inerentes à adopção de um nível apropriado de segurança?

78% refere que actua fundamentalmente com base na legislação, incluindo esta resposta a referência a normas europeias.

O segundo factor de maior peso são as “práticas normalizadas da indústria” (61%) e o terceiro as “melhores práticas internacionais” (39%).

Refira-se também o factor “escuta dos clientes e parceiros” (22%) e os sites da especialidade (17%).

Poderá daqui inferir-se que o combate a spam passa por uma legislação clara para todos os intervenientes e uma cooperação ao nível da divulgação e adopção das “boas práticas”.

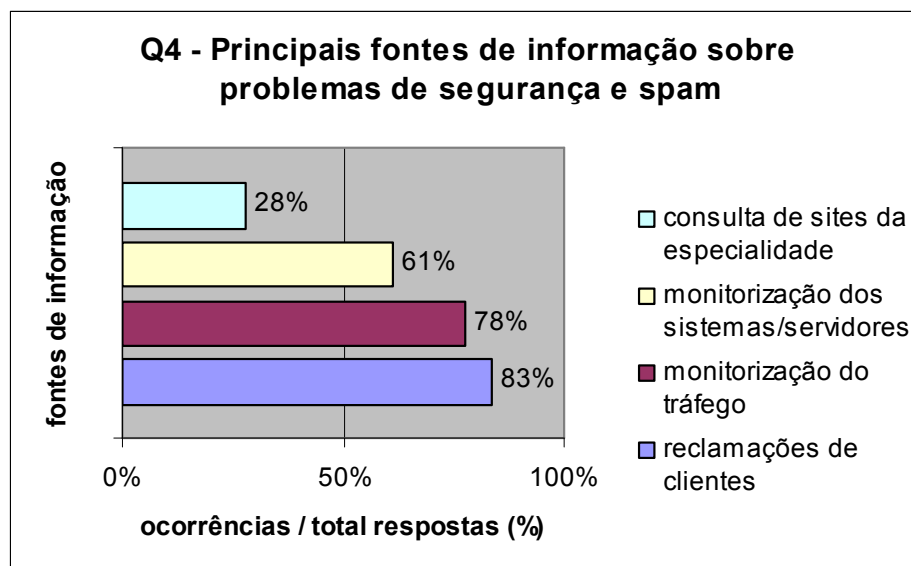
legislação nacional e internacional (incluindo normas europeias)	78%
práticas normalizadas da industria	61%
melhores práticas internacionais	39%
“escuta” dos clientes e parceiros	22%
sites da especialidade	17%
conhecimento resultante da experiência real na actividade	6%
protocolos com entidades nacionais e internacionais	6%

2.4 Questão 4 - Como é que se mantém informado acerca de problemas de segurança informática e SPAM?

Os factores chave de informação sobre os problemas de segurança informática e spam são:

- Reclamações dos clientes (83%)
- Monitorização do tráfego e sistemas (78% e 61% respectivamente)
- Consulta de sites da especialidade (28%)

As reclamações dos clientes são a principal fonte de informação sobre os problemas de segurança. De relevar também o facto de os ISP estarem activos para garantir a segurança informática através da monitorização do tráfego.

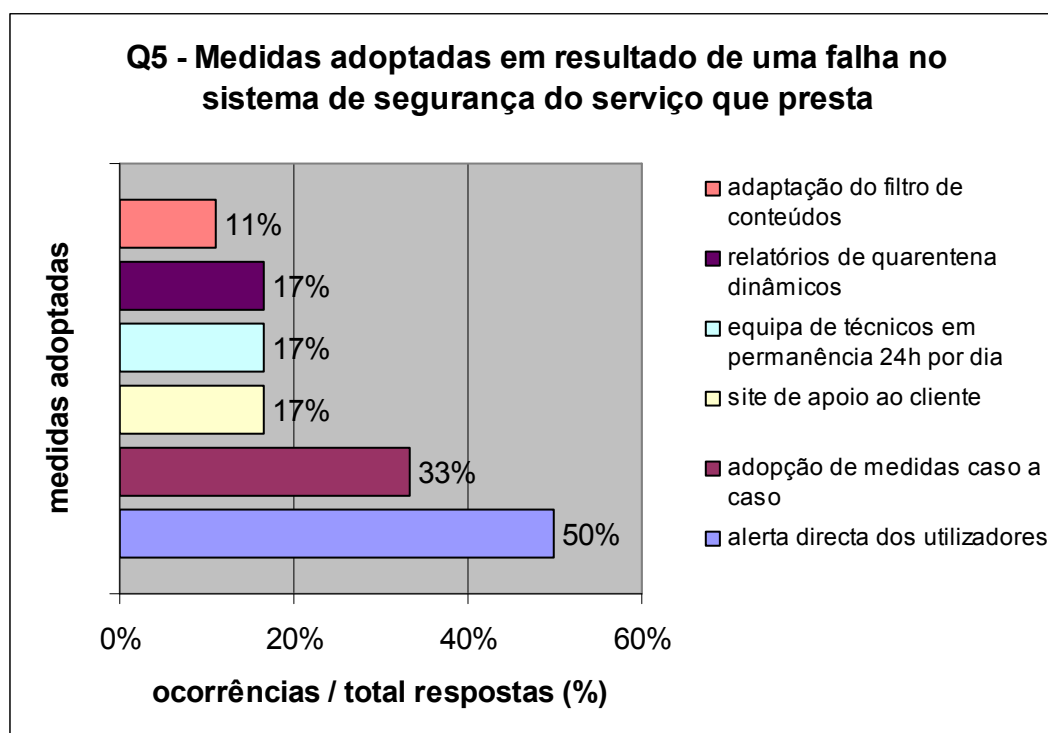


2.5 Questão 5 - Que medidas adopta quando detecta uma falha no sistema de segurança inerente ao serviço que presta?

A leitura das respostas transmite a percepção de ter havido uma certa dificuldade de interpretação desta e da próxima questão, já que de alguma forma uma complementava a outra. Pretendia averiguar-se na presente questão o que os ISP fariam em face de uma falha originada no seu próprio sistema e na questão 6 o que fariam em cooperação quando a falha é originária em terceiros. Em virtude destes factos, repescou-se na resposta a esta e à questão 6 os factores determinantes segundo o pretendido com uma e outra questão.

A actuação perante uma falha própria, leva os ISP a:

- Alertarem directamente os utilizadores (50%)
- Prestarem apoio através de uma equipa de técnicos em permanência 24 h por dia (17%) ou através de informação no site (17%)
- Manutenção de relatórios de quarentena dinâmicos com as ocorrências (17%) e adaptação do filtro de conteúdos (11%)

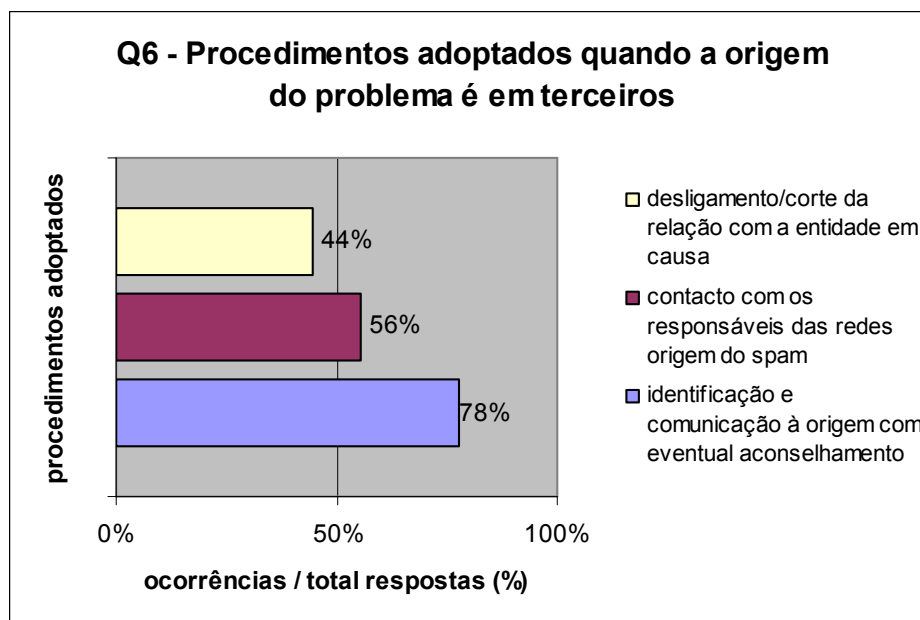


2.6 Questão 6 - Qual o procedimento adoptado, se a adopção de medidas adequadas não depende da sua empresa?

A primeira medida adoptada pelos ISP nacionais quando a falha de segurança vem de fora é a identificação da origem, comunicação e eventual aconselhamento (78%). Por vezes os ISP entram em contacto com os responsáveis das redes de origem do spam (56%). A medida mais dura é adoptada em casos extremos e concretiza-se pela descontinuidade do serviço com a entidade em causa (44%).

Pode concluir-se que a via adoptada na grande maioria dos casos é o diálogo e o aconselhamento. Nem sempre no entanto esta prática é possível e o corte com a entidade emissora de spam pode acontecer quando esta aparece em listas negras. Pode daqui inferir-se como é positiva a promoção de listas brancas para as empresas que se dedicam ao marketing de forma

séria e que por vezes, na inviabilidade destas listas brancas, são confundidas com “spammers”.



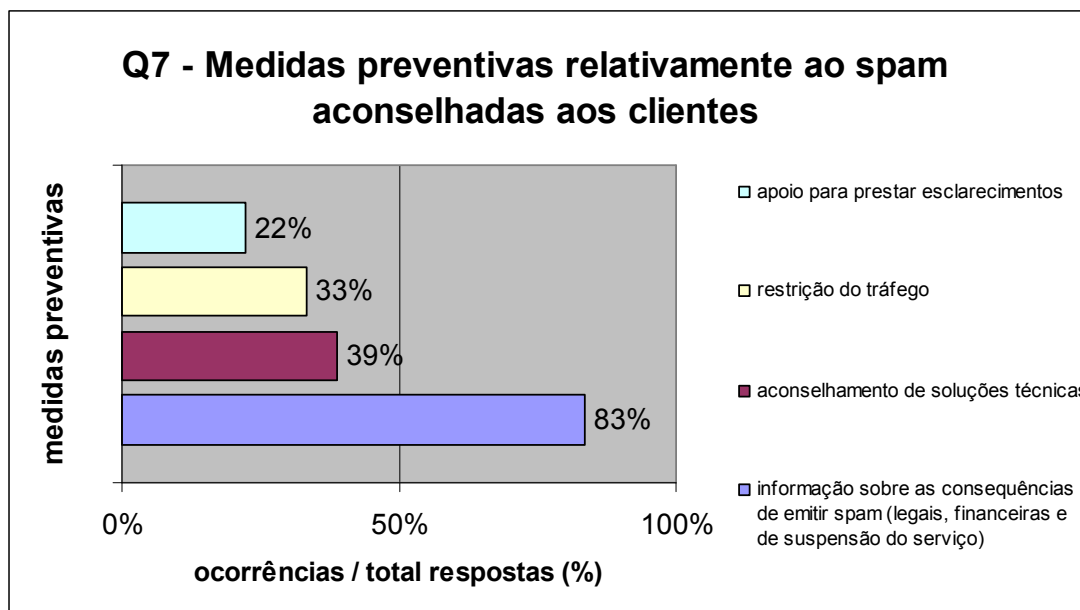
2.7 Questão 7 - Quais as medidas preventivas aconselhadas aos clientes relativamente ao envio de SPAM?

O trabalho na prevenção do spam assenta fundamentalmente na promoção de códigos conduta ou de boas práticas de utilização de serviços. Quando é detectado spam, a primeira iniciativa é informar sobre as consequências que advêm desta prática (83%), consequências estas que podem ser legais, financeiras e, em última análise, de suspensão do serviço.

Os ISP optam também pelo aconselhamento técnico (39%) e disponibilizam-se para prestar esclarecimentos (22%).

Em 33% dos casos restringe-se o tráfego, o que significa fazer uso de listas negras.

Das respostas recolhidas, é de salientar os efeitos positivos que os códigos de conduta podem ter como medida dissuasora das práticas de spam.



2.8 Questão 8 - Quais as medidas adoptadas para preservar os clientes de receberem SPAM?

Saliente-se o papel da auto-regulação dos ISP no que respeita à protecção dos seus clientes contra o spam.

Assim, 16 dos 18 respondentes afirmam proporcionar de forma gratuita o filtro de spam no serviço de correio electrónico.

Em 18 respondentes, 7 dizem oferecer o antivírus e 5 aconselham boas práticas para evitar o spam.

Este resultado parece evidenciar haver espaço para maior iniciativa no aconselhamento de adopção de boas práticas de forma a evitar o spam, pois esta parece ser uma medida ainda não muito significativa no cômputo geral das medidas adoptadas para a protecção dos clientes.

Por outro lado, parece poder concluir-se que existe “relutância” em promover as listas negras, brancas e cinzentas. Ainda que se admita que estas para serem úteis terão de estar em permanente actualização, um intercâmbio de informação entre os ISP para alimentar estas listas actualizadas, poderá trazer benefícios à actuação no combate ao spam.

Q8 – Principais medidas adoptadas para preservar os clientes de receberem spam

oferta gratuita de filtro de spam	89%
oferta de software antivírus	39%
aconselhamento sobre boas práticas para evitar spam	28%
bloqueamento via listas negras	17%
apoio técnico ao cliente	11%
monitorização da performance e qualidade dos serviços e rede	11%

2.9 Questão 9 - Que medidas preventivas são adoptadas como combate às situações de fraude de identidade? É implementado algum mecanismo de autenticação?

5 empresas admitem não implementar nenhum mecanismo de autenticação.
12 empresas fazem autenticação SMTP e 5 publicam informação SPF.

Q9 – Medidas preventivas adoptadas para combate à fraude de identidade

<u>autenticação SMTP</u>	67%
não é implementado nenhum mecanismo de autenticação	28%
<u>publicação de informação SPF</u>	28%
<u>SIDF</u>	11%
<u>mecanismo de autenticação único (SSO)</u>	6%
<u>DKIM para e-mail outbound</u>	6%

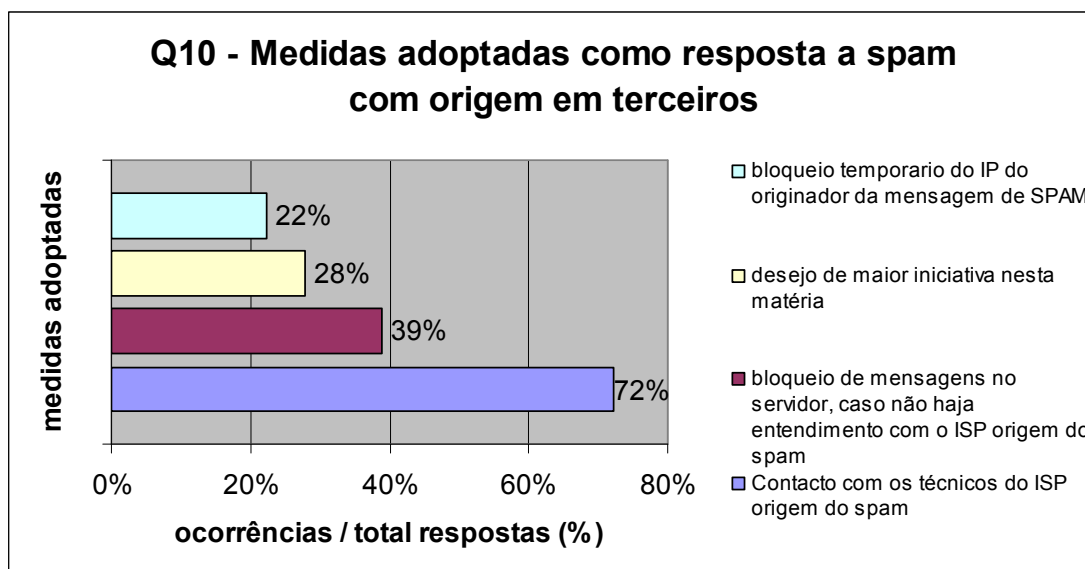
2.10 Questão 10 - Que medidas adopta quando verifica que as mensagem de SPAM são provenientes de prestadores de serviços de acesso à Internet sediados no país? E se forem provenientes de prestadores de serviços sediados na Europa? E ainda se forem prestadores de serviços sediados fora da União Europeia?

Praticamente nenhum dos respondentes definiu a actuação com distinção em termos geográficos de origem do spam. Mesmo sem esta distinção, 72% afirmaram contactar com os técnicos do ISP origem do spam.

11 em 18 admitiram bloquear mensagens em caso de não entendimento com o ISP de origem do spam.

28% revelou desejar maior iniciativa nesta matéria.

Estes dados são reveladores da importância que os ISP têm na actuação do combate a spam. De facto é por eles que passa o tráfego, pelo que o facto de desejarem ter maior iniciativa deve ser tido como uma oportunidade para empreender acções concertadas.



3. Principais conclusões

- O estabelecimento de códigos de conduta ou regras de utilização dos serviços são uma das principais medidas organizacionais para a promoção da segurança dos serviços prestados.
- As medidas adoptadas para a promoção da segurança dos serviços prestados nem sempre são coordenadas entre os prestadores de serviço e os operadores de rede.
- A legislação aparece como o principal elemento de referência quando é necessário definir um nível de segurança; O segundo e terceiro factores que estão na base desta decisão são as práticas normalizadas da indústria e as melhores práticas internacionais.
- As principais fontes de informação para a identificação dos problemas de segurança informática e spam são, por ordem decrescente de importância, as reclamações dos clientes, a monitorização do tráfego e a consulta de sites da especialidade.
- Quando ocorre uma falha de segurança interna, nomeadamente relacionada com spam, os ISP adoptam medidas de:
 - Alerta dos utilizadores,
 - Apoio através de uma equipa de técnicos que por vezes está operacional 24 h/dia,
 - Adaptação do filtro de conteúdos e relatórios de quarentena adaptados às ocorrências.

Esta actuação revela uma atitude activa e atenta dos ISP.

- Quando a falha de segurança é proveniente de terceiros, a actuação mais comum é a identificação da origem, o alerta e o eventual aconselhamento. Por vezes os ISP entram em contacto com os responsáveis das redes de origem do spam. Em casos extremos, isto é, quando as falhas colocam em perigo o funcionamento do sistema e/ou os responsáveis das redes de origem não colaboram, os ISP optam por descontinuar o serviço origem da falha de segurança.
- Alguns dos respondentes indicaram o uso de listas negras. A descontinuidade de serviço em casos extremos, conduz a relevar o contributo que têm, para além das listas negras que identificam os prevaricadores, as listas brancas que identificam aqueles que são exemplo de boas práticas.

- O trabalho de prevenção do spam assenta fundamentalmente na promoção de códigos de conduta ou de boas práticas de utilização de serviços. Quando é detectado spam, a primeira iniciativa é informar sobre as consequências que advêm desta prática, consequências estas que podem ser legais, financeiras e, em última análise, de suspensão do serviço.
- A grande maioria dos ISP proporciona anti-spam e anti-vírus de forma gratuita, o que traduz uma posição atenta e activa na segurança.
- Existem ISP que ainda não implementam qualquer mecanismo de autenticação como forma de combate a situações de fraude de identidade.
- A resposta à questão sobre as medidas adoptadas em face de mensagens de spam revelou que os ISP desejam que haja maior iniciativa nesta matéria. Por vezes, quando não há entendimento com o ISP de origem do spam, a prática é a de bloquearem o tráfego. Desta conclusão se infere que há espaço para acção concertada entre os ISP na identificação e combate aos “spammers”.