

POLITICA ANTI-SPAM PARA USO DE LOS SOCIOS DE AEPROVI

1. OBJETO

El objeto de esta política es definir un conjunto de medidas que deben ser cumplidas por los miembros de AEPROVI a fin de minimizar el problema del correo electrónico no solicitado.

2. ALCANCE

Esta política aplica cuando el cliente usa la infraestructura de mensajería electrónica del proveedor de servicio de Internet.

3. REQUISITOS

El contrato de servicios suscrito entre el proveedor y el usuario final debe incluir una autorización al Proveedor para realizar un procesamiento adicional al correo electrónico entrante y saliente con el objetivo de minimizar el spam e informar de los posibles riesgos de pérdida de información que implica el uso de los filtros.

4. DEFINICIONES

Sin perjuicio de las definiciones establecidas en la legislación nacional o internacional vigente o en los RFCs publicados por IETF, esta política se sujeta a las siguientes definiciones:

- a) Servicio de correo electrónico: Es un servicio de envío y recepción de mensajes que contienen información electrónica entre dos o más computadores o cualquier otro dispositivo de tecnología similar utilizando una red de interconexión al internet donde el contenido, el origen y el destino están “disponibles libremente” a terceros y donde el envío y la recepción de los mensajes son controlados por los usuarios.
- b) Acción de relay: Uso de la infraestructura del proveedor de servicios para el envío de correo electrónico.
- c) SPAM: Es correo electrónico masivo y no solicitado. Técnicamente, un mensaje de correo electrónico también es considerado SPAM cuando el remitente está incluido dentro de una o más listas negras que son revisadas por el proveedor del servicio.
- d) Filtro anti-spam: Procesamiento adicional que realiza el proveedor de servicios de valor agregado que presta servicios de internet para minimizar el envío o recepción de spam.
- e) Proveedor: Socio de AEPROVI que provee correo electrónico como una aplicación sobre la red Internet.
- f) Lista negra pública: Es un listado de direcciones electrónicas, direcciones IP y dominios que corresponden a remitentes de correo electrónico calificados como generadores de spam, administradas por organismos nacionales o internacionales que recopilan, mantienen y actualizan dicha lista.
- g) Lista negra privada: Es un listado de direcciones electrónicas, direcciones IP y dominios que corresponden a remitentes de correo electrónico calificados como generadores de spam, creada y modificada por solicitud expresa de destinatarios finales y administrada, mantenida y actualizada por el Proveedor.
- h) Lista blanca: Es un listado de direcciones electrónicas, direcciones IP y dominios que corresponden a remitentes de correo electrónico calificados como autorizados, creada y modificada por solicitud expresa de destinatarios finales y administrada, mantenida

- y actualizada por el Proveedor.
- i) Zona reversa DNS: Resuelve el nombre de dominio a partir de la dirección IP

5. MEDIDAS MÍNIMAS CONTRA LA RECEPCIÓN DE SPAM

El proveedor deberá implementar filtros anti-spam en sus servidores que deberán:

- a) Revisar al menos 3 listas negras públicas del catálogo definido por AEPROVI. Los mensajes cuyas direcciones remitentes estén incluidas en dichas listas serán eliminados del servidor sin que sea necesario informar al destinatario.
- b) Identificar cadenas de texto típicas de spam por lo menos en 2 idiomas: español e inglés, del catálogo definido por AEPROVI. Los mensajes que incluyan estas cadenas de texto serán eliminados del servidor sin que sea necesario informar al destinatario.

AEPROVI pondrá a disposición de los usuarios el catálogo de listas negras y cadenas de texto a través de su portal.

6. MEDIDAS MÍNIMAS CONTRA LA GENERACIÓN DE SPAM

El proveedor deberá cumplir y hacer cumplir lo siguiente:

- a) A fin de que sus clientes no sean ingresados injustamente en listas negras debido a configuraciones incompletas, el proveedor se compromete a configurar en sus servidores DNS la zona reversa de todos sus servidores de correo electrónico.
- b) Impedir e informar claramente sobre el uso indebido del correo electrónico por parte de sus usuarios tomando oportunamente las medidas que sean necesarias y que estén permitidas en la legislación nacional.
- c) Se prohíbe al Proveedor la difusión de las direcciones de correo electrónico de sus usuarios finales o clientes.
- d) Se prohíbe al Proveedor generar spam.

7. FORMA Y PLAZO DE CUMPLIMIENTO

El filtrado anti-spam del correo electrónico, necesario para cumplir con esta política, podrá ser suministrado con infraestructura propia del Proveedor o podrá ser contratado como un servicio a un tercero.

El plazo de cumplimiento de la presente política será de 6 meses a partir de su aprobación para socios actuales y 3 meses luego de su afiliación para socios nuevos.

8. PARTICIPACIÓN DE AEPROVI

A fin de ayudar a sus socios (en cuanto disponga de la infraestructura necesaria) AEPROVI podrá:

- a) Mantener una lista negra pública.
- b) Ofrecer el servicio de filtro anti-spam conforme a la política vigente.
- c) Proveer un catálogo de por lo menos 10 alternativas de listas negras públicas para el cumplimiento de esta política.
- d) Proveer un catálogo de cadenas de texto típicas relacionadas con el spam.
- e) Vigilar periódicamente el buen cumplimiento de la presente política, para lo cual AEPROVI desarrollará un procedimiento.
- f) AEPROVI mantendrá una lista en su intranet del portal www.aeprovi.org.ec con los

nombres de personas o empresas identificados como generadores de spam y que sean notificados por los asociados

9. VIGENCIA DE LA POLITICA

10. Sin perjuicio de poderlo hacer en cualquier tiempo, a fin de reflejar los cambios en el mercado, el contenido de esta política técnica deberá ser revisado por lo menos cada 6 meses. Las modificaciones podrán ser sugeridas por cualquiera de los miembros mediante solicitud al Presidente y deberán ser aprobadas por la Junta General. En caso de no recibir solicitudes de modificación la política vigente se aprobará automáticamente por 6 meses más.

11. MEDIDAS RECOMENDABLES

- a) Implementar listas negras privadas y blancas. Esta opción se utilizará bajo pedido de un cliente, pero siempre y cuando no afecte el servicio de otro usuario final.
- b) Alertar al destinatario mediante modificación de cabeceras (añadiendo texto al asunto) acerca de mensajes que le han sido entregados, pero que potencialmente podrían ser spam.

Esta política se aprobó en la Junta General realizada en la ciudad de Guayaquil el 18 de abril del 2007