

GUÍA PRÁCTICA SOBRE EL

SPAM

V 1.0 - Julio de 2006



VNM:host

INTRODUCCIÓN. ¿QUÉ ES EL SPAM? ¿CÓMO DEFENDERNOS?

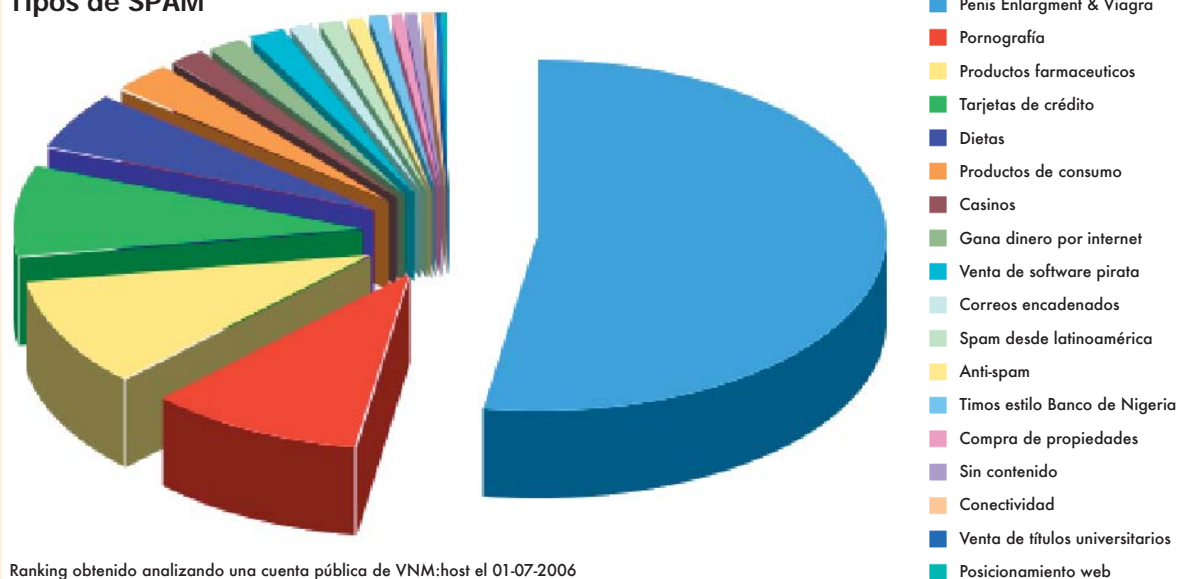
¿Qué es?

Solemos denominar 'spam' a los mensajes de correo electrónico no deseados que, cada día más, suponen un problema importante para Internet. Son mensajes que buscan producir beneficios para su emisor, resultando en la mayoría de casos molestos para sus múltiples receptores, ya que suelen consistir en la difusión de publicidad engañosa.

¿A quién afecta?

En mayor o menor medida, el 'spam' afecta a toda la comunidad de usuarios de Internet. Según diferentes analistas, el correo basura supone ya más de un 50% del correo electrónico generado, cifra que algunas empresas elevan al 80%. Afecta al obligar a los usuarios a dedicar tiempo en su eliminación, genera tráfico, ancho de banda y espacio superfluo, y obliga a destinar a los proveedores de servicios recursos de hardware y software para su transmisión, análisis y filtrado, cada vez con mayor intensidad.

Tipos de SPAM



¿Por qué a mí?

Existen múltiples formas mediante las que un 'spammer' consigue tu dirección de e-mail. En la mayor parte de casos se obtienen rastreando la web y extrayendo todas las direcciones de correo que aparecen publicadas. Otra de las fórmulas más habituales consiste en acceder a listas de discusión o foros en los que figura como referencia una dirección de e-mail. También surge de empresas que venden datos de contacto a terceras personas, aspecto que se suele consentir al aceptar condiciones de uso que casi nadie se para a leer. Este fenómeno es frecuente en suscripciones a boletines, listas de distribución o cualquier otro tipo de servicio que requiera un correo de contacto. En caso de tener un dominio registrado, su simple existencia conlleva que figure en bases de datos públicas a nivel interna-



cional, que muchos 'spammers' utilizan para enviar correo basura a direcciones aleatorias que se puedan construir a partir de este dominio.

¿Qué hace VNM:host para ayudarme?

Todo el correo que llega a los servidores de VNM:host es filtrado para evitar la proliferación de virus y 'spam'. En relación a los virus, la eficacia de nuestros sistemas se aproxima al 100%, eliminando automáticamente la amenaza. En el caso del 'spam', los filtros instalados suelen identificar la mayoría de mensajes no deseados, marcándolos con la etiqueta [SPAM] para facilitar su reconocimiento y posterior borrado.

¿Por qué no se impide que me lleguen estos mensajes?

Cada vez resulta más difícil distinguir un correo electrónico convencional de un mensaje considerado como 'spam'. Es más, dependiendo del perfil de cada usuario, un mensaje puede ser considerado o no 'spam' (Ej. La publicidad de una revista deportiva puede ser útil a ciertos usuarios y ser considerada 'spam' por otros). Los filtros de VNM:host analizan las cabeceras, cuerpos de texto y características de cada mensaje para detectar si recibes correo malintencionado, aunque existe la posibilidad de que, por su formato, un mensaje que quieras recibir pueda ser marcado como 'spam' (per ejemplo, un mensaje con "Felicidades!!!!!" como asunto). Por ello preferimos que seas tú mismo quien decida qué mensajes borrar y qué mensajes confirmar. Aún así, si estás seguro de que el filtro identifica correctamente todos los mensajes considerados 'spam', indica en el apartado "Filtros y Reglas" de tu panel de control de hosting que quieres borrar automáticamente este tipo de mensajes.

- Como el 'spam' es enviado por terceras personas que imitan los mensajes convencionales y examinan los filtros para detectar formas de superarlos, la batalla contra el 'spam' evoluciona continuamente, resultando prácticamente imposible asegurar una eficacia total contra este tipo de amenaza.

- De hecho, la empresa de seguridad electrónica Blue Security, que lideraba internacionalmente el combate a los 'spammers', anunció su rendición en el mes de mayo de 2006, advirtiéndolo que "no se tienen los medios necesarios para acabar con el 'spam'". La compañía y sus clientes habían sido atacados deliberadamente por difusores de 'spam', ante lo que Blue Security optó por cerrar la empresa "para evitar una guerra a gran escala que no tenemos la autoridad de iniciar" y que podría afectar al funcionamiento global de la Red.



¿Qué puedo hacer ahora?

Si recibes mensajes de 'spam' en una cuenta de correo, ten por seguro que sus emisores seguirán enviando mensajes no deseados a esta dirección. En caso de que necesites mantener esta cuenta, deberás limpiarla con cierta frecuencia para evitar la acumulación de este tipo de mensajes.

- Tienes también la opción –recomendada– de crear reglas a través de un programa de gestión de correo –como Outlook o Thunderbird–, señalando rasgos distintivos de los correos no deseados que recibas con más frecuencia para su eliminación automática. O bien personalizar los filtros y reglas que actúan en el servidor al recibir los mensajes, como explicaremos más adelante.

¿Cómo podría evitarlo?

El único método realmente viable es la prevención. Nunca publiques una dirección de correo que quieres que sea segura en una web, no firmes comentarios en foros o listas de discusión con este correo y no te suscribas a boletines o fuentes informativas que, como hemos comentado, suelen vender los datos de contacto a terceros. Resultan especialmente peligrosas las suscripciones a webs que proporcionen contenidos para adultos, ya que muchas de ellas han sido creadas específicamente para captar receptores de correo malintencionado.

- Utiliza varias cuentas de correo: una segura para tus contactos habituales o la recepción de correo importante y otra/s para su difusión pública o usos diversos. Cuando hagas pública la dirección puedes optar por escribirla en un formato fácil de reconocer para personas pero difícil para un robot (ej. pepitoperezA-RROBAmidominioPUNTOcom o bien referenciar la dirección con el texto en una imagen), con lo que evitarás su localización automática.

- Nunca respondas a un correo identificado como 'spam' y nunca accedas a las solicitudes de baja de suscripción, ya que suelen utilizarse para confirmar que una dirección de correo está activa. Otro elemento de riesgo está en las imágenes anexas en correos no deseados, que debes evitar abrir, ya que suelen contener códigos de programación que confirman al emisor de 'spam' que el mensaje ha sido recibido en tu cuenta. La mayoría de programas de gestión de correo bloquean por defecto la descarga de imágenes de los mensajes. En caso contrario, puedes señalar esta opción como predeterminada en las preferencias.

Guía práctica sobre el SPAM

- Si quieres suscribirte a listas de debate o señalar direcciones de contacto en la web, recomendamos utilizar cuentas secundarias, de las que puedas prescindir si adviertes que estás recibiendo grandes cantidades de 'spam'. Con un plan de hosting profesional dispones de 100 cuentas, que puedes aprovechar plenamente para alternar diferentes direcciones de e-mail. En caso de suscripciones a listas potencialmente peligrosas, como las que incluyen contenido erótico, aconsejamos optar por cuentas gratuitas de correo –como Hotmail, Yahoo o Gmail– que ofrecen una elevada capacidad de almacenamiento sin costes para el usuario.

¿Cómo se propaga?

Estos mensajes suelen enviarse de forma masiva y automatizada a miles de usuarios y sin tener en cuenta la identidad de los receptores, tras haber recopilado las direcciones de correo mediante robots de búsqueda, compra de datos o técnicas ilícitas como el uso de determinados virus para obtener todos los contactos procedentes, por ejemplo, de la agenda que utilizamos en nuestro programa de gestión de correo. Los virus también pueden hacer que los usuarios enviemos miles de correos electrónicos sin saberlo, siendo utilizados por el emisor de 'spam' para garantizar su anonimato. Además los 'spammers' pueden ocupar servidores para utilizarlos como propagadores de correo no deseado, falsificar las cabeceras y los correos remitentes, cambiar continuamente de direcciones, etc., lo que complica la correcta identificación de los autores de estas prácticas ilícitas.

¿CÓMO CONFIGURAR MI PROGRAMA DE CORREO PARA FILTRAR SPAM?

Utilizando un programa de correo podrás definir reglas o filtros para eliminar automáticamente los mensajes de 'spam' que lleguen a tu buzón. Habrás apreciado que muchos de los mensajes no deseados contienen referencias a productos como "viagra" o repiten palabras que inequívocamente consideras 'spam'. Analizando los correos que recibes podrás definir estos filtros, indicando, por ejemplo, que quieres que todos aquellos mensajes que contengan la palabra "viagra" o la frase "gane dinero rápido" se dirijan directamente a la papelera, sin pasar por tu buzón de entrada. Cuantas más reglas crees y más precisas sean éstas, mayor será su eficiencia para reducir la carga de mensajes basura.

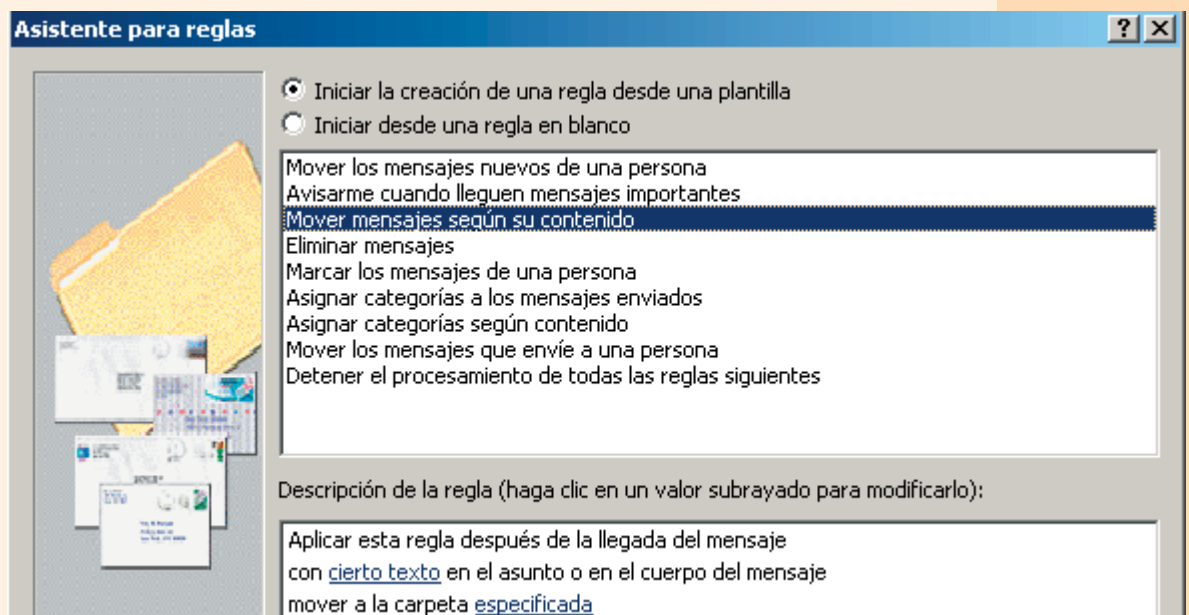
- Para eliminar directamente los mensajes que sean identificados como 'spam' o como virus por nuestro filtro, deberás crear una regla que indique que quieres eliminar los mensajes que incluyan en el asunto la palabra [SPAM] y otra que descarte los mensajes que aparezcan marcados como [VIRUS]. Recuerda que existe la posibilidad de que correos que aparezcan señalados como 'spam' puedan ser de tu interés: bien porque promocionen un servicio o producto que demandes o bien porque un mensaje masivo o que contenga características similares al correo basura pueda ser identificado como tal.

- A continuación indicamos los pasos para configurar las reglas o filtros en los programas de correo electrónico más demandados. Puedes seleccionar mensajes por su contenido, por el texto que contiene el asunto, por el remitente o por su destinatario; indicar cual será su destino (Ej. Una carpeta determinada, la papelera...), y marcar los requisitos de cada regla (Ej. Que contenga la frase "millonario en dos días"). En general, podrás crear el número de reglas que necesites para automatizar la gestión del 'spam'.

Microsoft Outlook

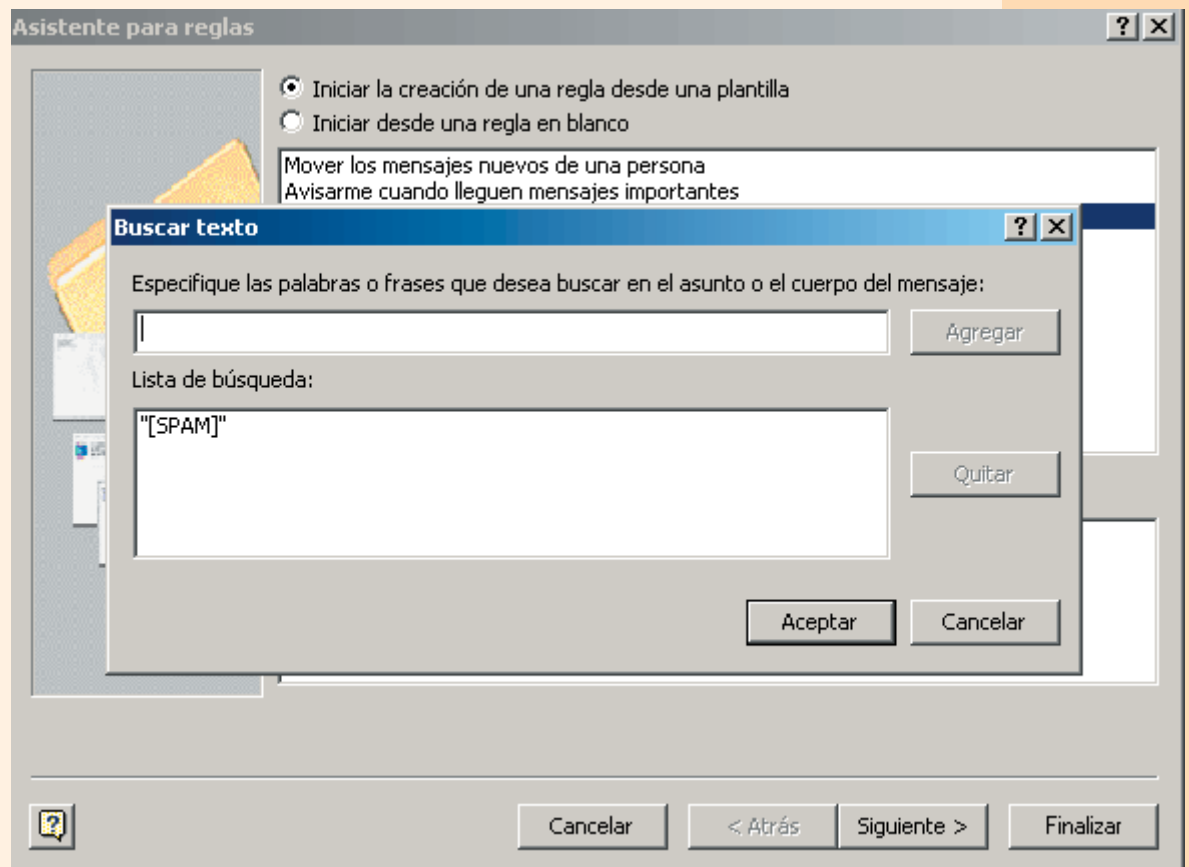
Primero debes acudir al Asistente para Reglas, a través de las opciones del menú superior Herramientas / Asistente para reglas. Una vez allí, pulsa el botón "Nueva..." para crear una nueva regla.

- Te encontrarás con esta ventana:



Guía práctica sobre el SPAM

- Debes seleccionar la opción "Mover mensajes según su contenido" en la ventana anterior. Posteriormente, pulsa sobre el enlace subrayado "cierto texto". Saltará una nueva ventana en la que te pedirá el texto a buscar. Debes escribir la palabra o frase que identifique un mensaje como 'spam' y pulsar el botón "Agregar", de manera que la ventana quede como muestra el gráfico inferior, y pulsar "Aceptar".



- Tras ello, pulsa sobre el texto subrayado "especificada" para elegir la carpeta de destino de los mensajes (normalmente será la carpeta "Eliminados", o bien una carpeta "SPAM" que hayas creado específicamente). Así podrás discriminar los mensajes, revisarlos, y eliminarlos definitivamente si lo deseas, en apenas unos segundos. Para borrarlos sin pasar revisión elige simplemente la opción "Eliminar mensajes" en la plantilla superior, en lugar de "Mover mensajes según su contenido".

- Finalmente, pulsa el botón "Siguiendo" en el resto de pantallas y el botón "Finalizar" en la última. La regla quedará establecida.

Microsoft Outlook Express

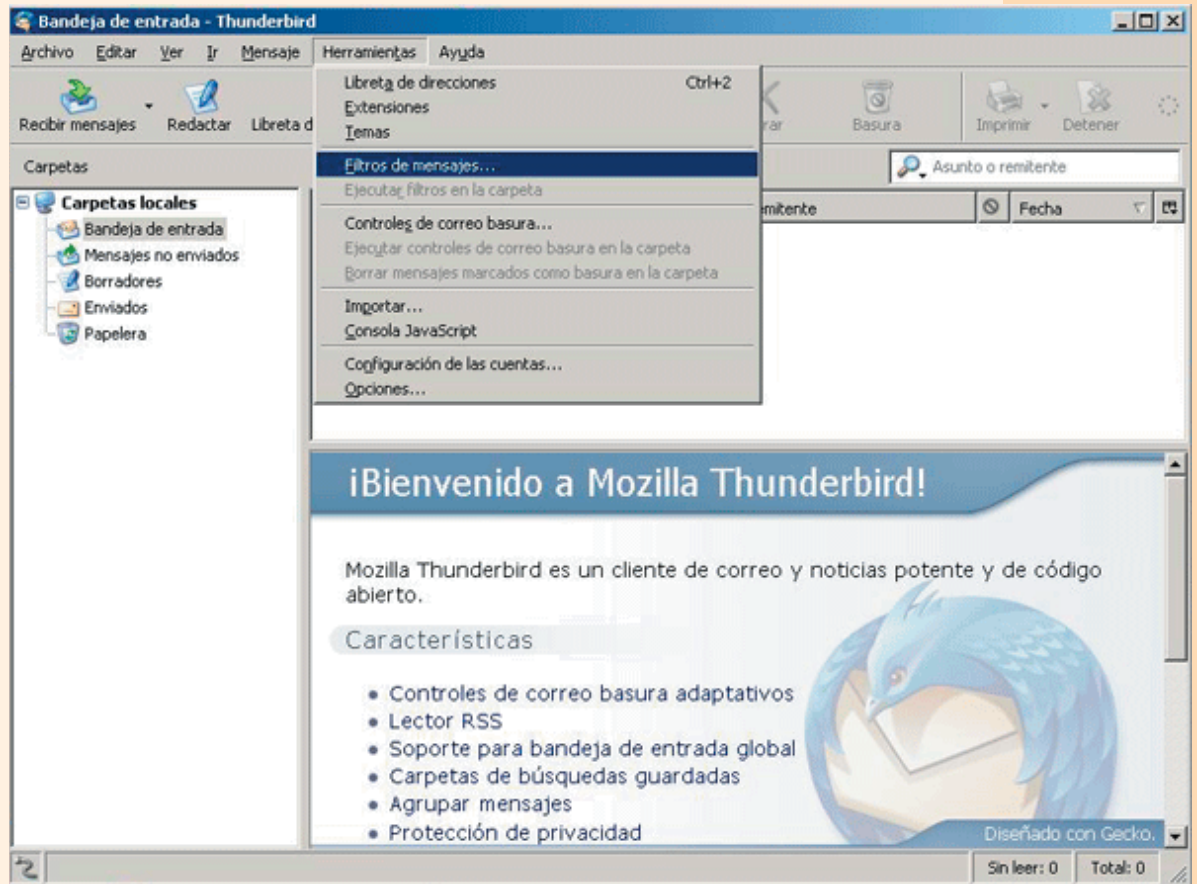
Accede a la configuración de reglas de mensaje a través de la opción Herramientas / Reglas de mensaje / Correo, tras lo cual el procedimiento es prácticamente idéntico al señalado.

Eudora

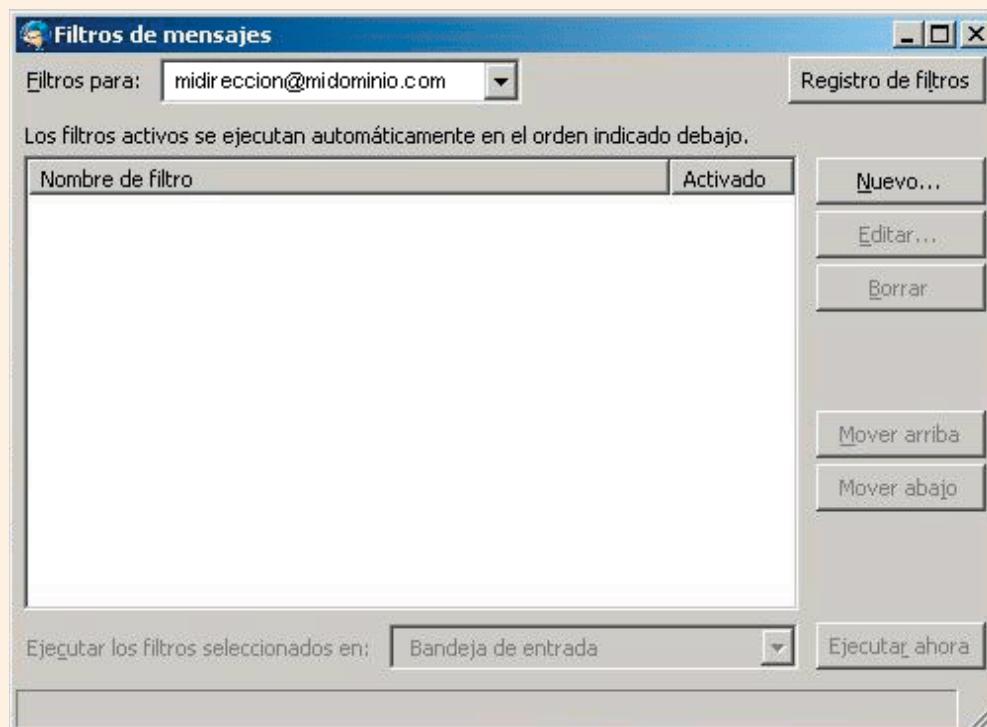
Debes activar en el menú textual superior la opción 'Herramientas' y 'Filtros', configurando las reglas y los procedimientos a quienes aplicar cuando se cumplan las condiciones que indiques.

Mozilla Thunderbird

Accede a Herramientas / Filtros de Mensajes

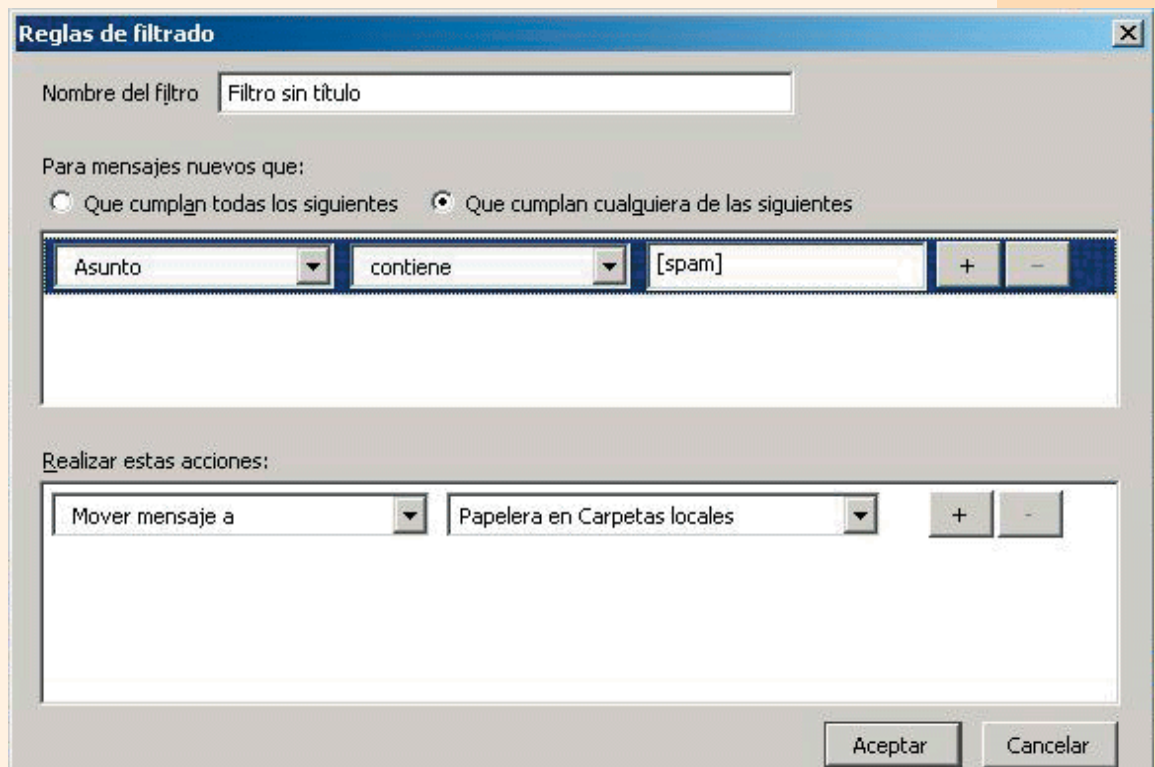


- Llegarás a esta pantalla. Pulsa en el botón 'Nuevo...' para añadir un filtro.



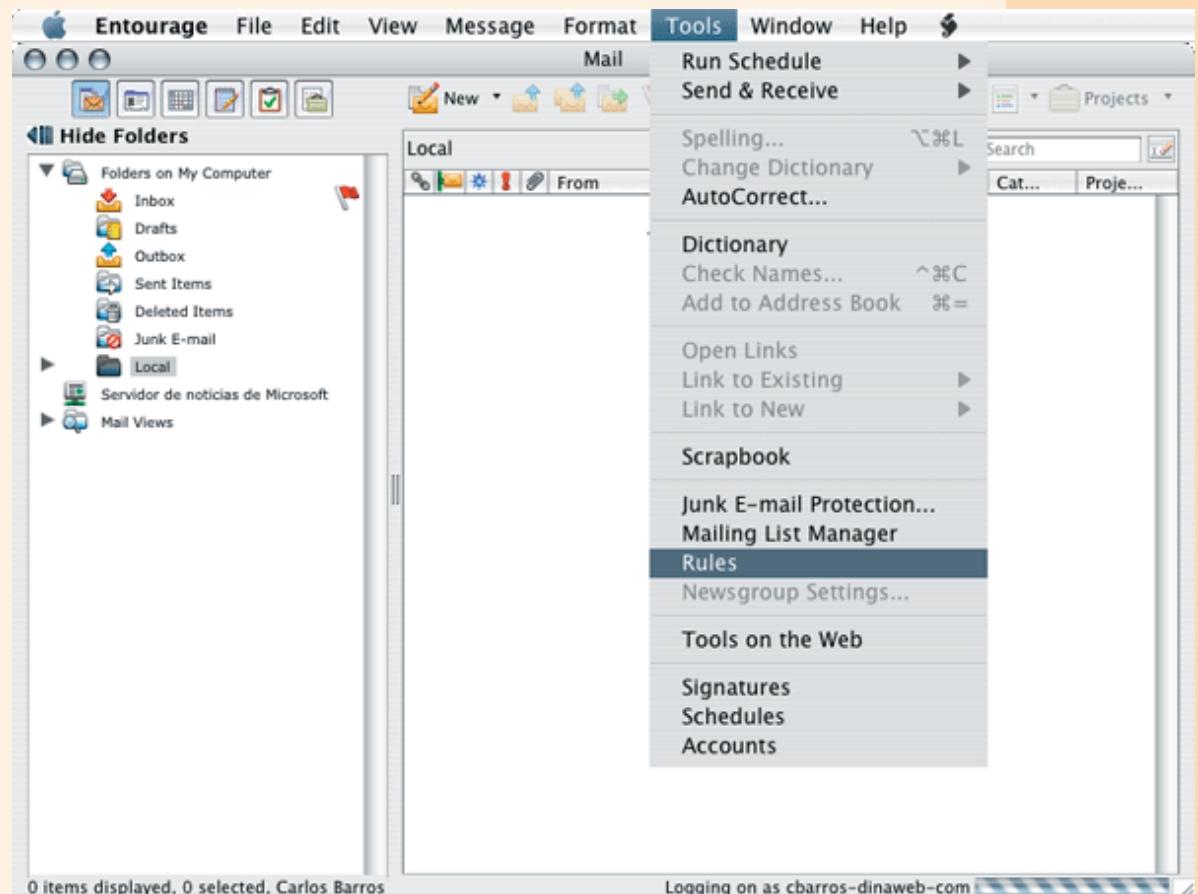
Guía práctica sobre el SPAM

- Crea los filtros necesarios, indicando si quieres que se apliquen sólo cuando se cumplan todos los requisitos o si quieres que sean filtrados todos los mensajes que cumplan características de cualquiera de las reglas que vas a crear.



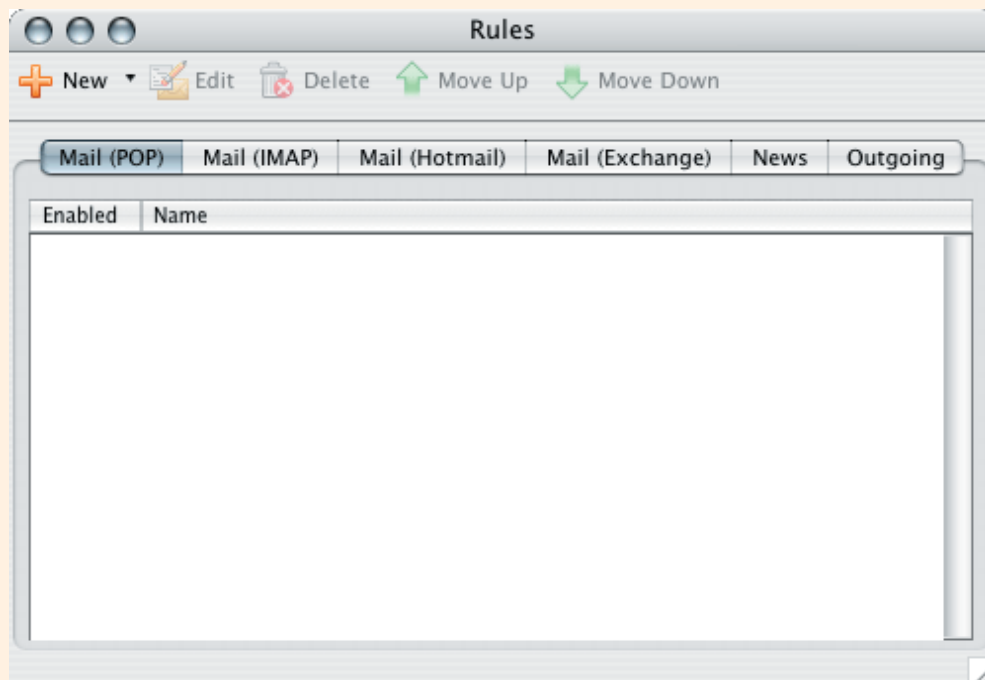
Microsoft Entourage (Mac)

Accede a Tools / Rules (Herramientas / Reglas)

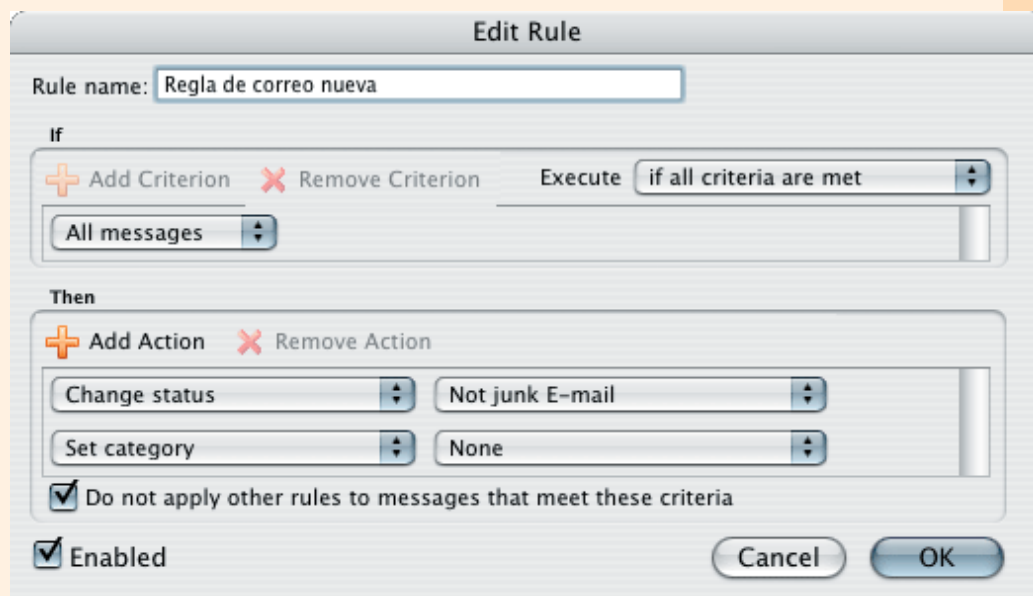


Guía práctica sobre el SPAM

- Verás esta pantalla. Pulsa 'New' (Nueva) para crear una regla.



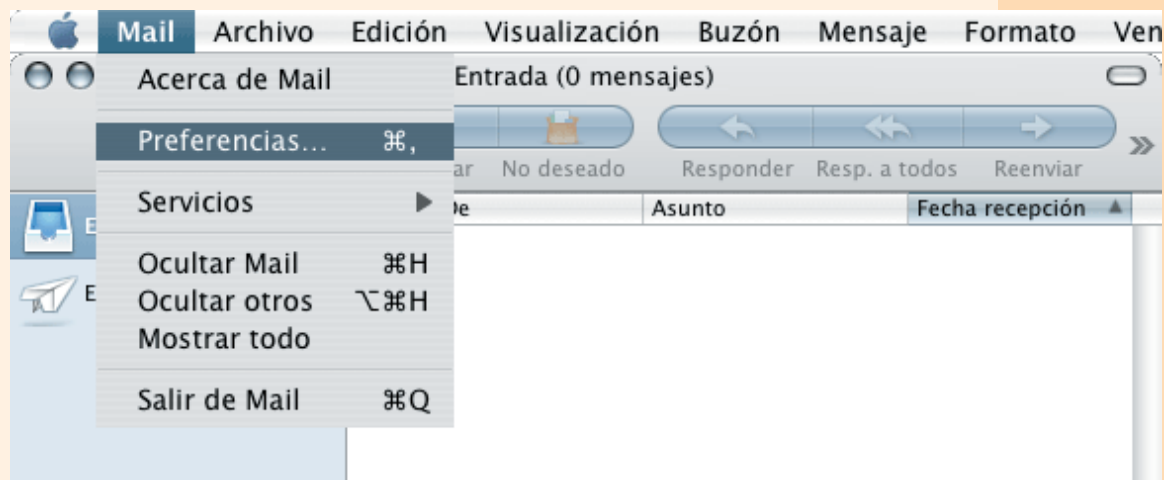
- Indica un nombre, marca si los mensajes deben cumplir todos los criterios o si basta con que cumplan cualquiera de ellos para ser filtrados.



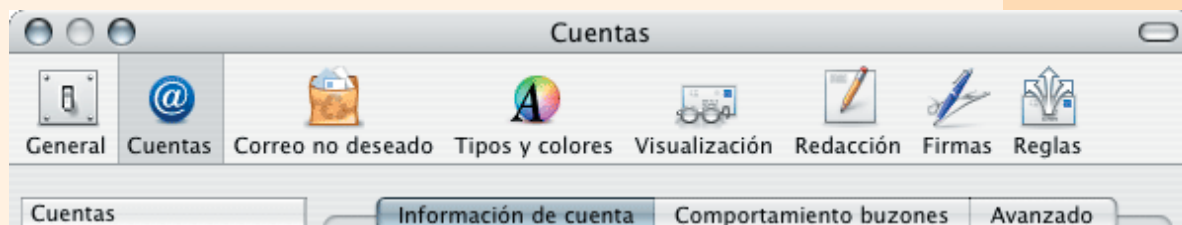
- Define completamente cada una de las reglas y conseguirás reducir sustancialmente el número de mensajes basura que lleguen a tu dirección de correo.

Mail (Mac)

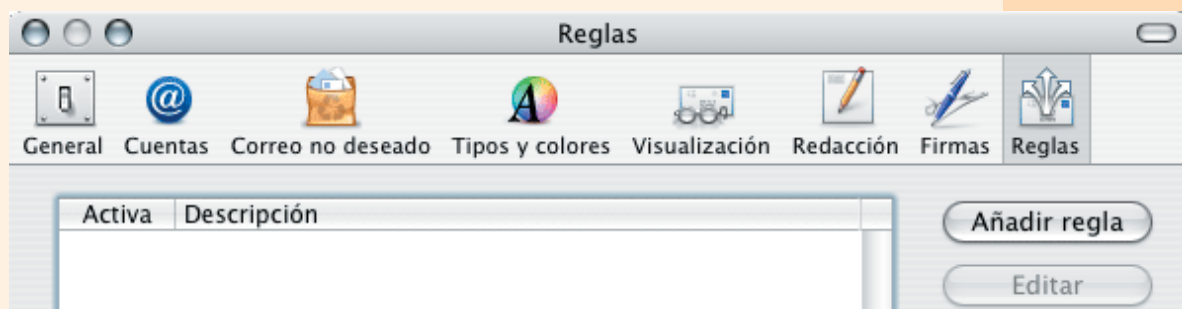
Accede a Mail / Preferencias



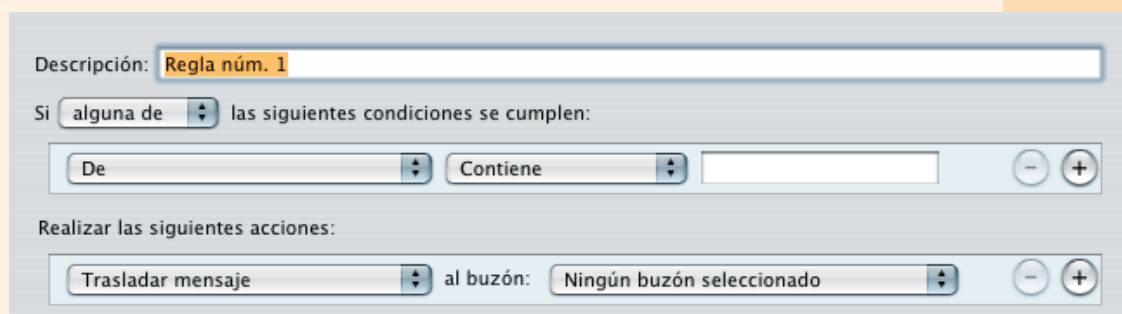
- Verás esta pantalla. Debes seleccionar el icono 'Reglas', situado en la parte superior derecha.



- Pulsa 'Añadir Regla' para definir y crear un filtro de correo.



- Señala un nombre identificativo, marca si todos los criterios se deben cumplir o si filtrarás todos los mensajes en que se verifique cualquier criterio de los que señales. Define el número de reglas que necesites.



¿CÓMO DEFINIR FILTROS Y REGLAS EN EL SERVIDOR PARA ELIMINAR SPAM ANTES DE QUE LLEGUE A MI CORREO?

Accede al apartado "Filtros y Reglas", dentro de la sección e-mail de tu panel de control de hosting.

The screenshot shows a hosting control panel for 'midominio.com'. On the left is a navigation menu with 'Filtros y reglas' highlighted. The main content area is divided into three sections: 'Administración del dominio' (showing IP and access URL), 'Actualizaciones y avisos' (with a 'Filtros y reglas' sub-section containing a date and description of the spam filter), and 'Utilización de Recursos' (showing disk space and monthly traffic usage with pie charts).

Filtro Antispam

The screenshot shows the configuration form for the Antispam filter. It includes tabs for 'Filtro Antispam', 'Filtro Antivirus', 'Reglas de Correo', and 'Importar/Exportar'. The form has the following options:

- Activar Filtro Antispam para el dominio (recomendado)
- Lista blanca. No aplicar el filtro Antispam a los siguientes dominios/cuentas de email (uno por línea). (Empty text box)
- ¿Qué hacer con los mensajes detectados como SPAM?
 - Recibirlos con la etiqueta [SPAM] en el asunto del mensaje (recomendado).
 - Eliminarlos automáticamente del servidor.

Buttons: 'Aplicar Cambios'

- El filtro antispam actúa por defecto y marca los mensajes que identifica como correo no deseado con la etiqueta [SPAM] o bien permite eliminarlos automáticamente. Recomendamos mantenerlo activo para facilitar la selección de mensajes y combatir eficazmente el correo basura.

- Añade dominios y/o direcciones de correo seguras en la "Lista Blanca" cuando quieras que el filtro no actúe sobre estos remites, que consideras de confianza.

- Por último, puedes optar por que todos los mensajes identificados como 'spam' sean borrados antes de llegar al servidor, evitando así tener que eliminarlos de forma manual. Elige esta opción sólo si estás segur@ de que el correo que nuestros filtros determinan como correo basura son efectivamente correo basura. Existe la posibilidad de que ciertas listas de correo o información que puede ser considerada `spam` por su formato sea en realidad información de tu interés. Decide en base a las características de tus correos.

Filtro Antivirus

- El filtro antivirus está activado por defecto. Elimina el código malicioso y marca con la etiqueta [VIRUS] los mensajes afectados de forma automática. Podemos optar por eliminar en el servidor estos mensajes para no descargarlos.

Reglas de Correo

- Puedes crear en el servidor reglas del mismo tipo que las que hemos señalado para aplicar en programas como Outlook. De esta forma, las reglas actuarán directamente en el servidor, aplicando los cambios que definas sobre los mensajes que cumplan ciertas características. Crea tantas reglas como sea preciso.

Importar / Exportar

- Si tienes varios hostings contratados, puedes definir reglas para un plan concreto y exportarlas para otros planes. Importa y exporta reglas con facilidad, agilizando el proceso para proteger definitivamente tu buzón de correo de 'spam'.



VN:M:HOST