GUIAS DE SEGURIDAD UJA

Correo electrónico no solicitado (SPAM)

Servicio de Informática
Vicerrectorado de Tecnologías de la Información
y la Comunicación y Universidad Digital
Universidad de Jaén

Edición: **enero 2018**

Contenidos

1. ¿Qué es el SPAM?

A modo de curiosidad, el origen de la palabra **SPAM** proviene de Estados Unidos. Una famosa empresa de charcutería americana lanzó en 1937 una carne en lata originalmente llamada *Hormel's Spiced Ham*. El SPAM (de la contracción de "Spiced Ham", en español "jamón con especias") fue el alimento de los soldados soviéticos y británicos durante la Segunda Guerra Mundial, y desde 1957 fue comercializado en latas que ahorraban al consumidor el uso del abrelatas.

Un tiempo después, el grupo de humoristas británicos Monty Python empezó a hacer burla de la carne en lata. En un sketch de su programa *Monty Python's Flying Circus* repetían a todas horas la palabra SPAM, lo que interfería con la conversación normal, algo similar a lo que ocurre actualmente en el correo electrónico, donde el SPAM interfiere en la lectura de los mensajes normales.

Actualmente, se define como SPAM o correo basura al conjunto de mensajes publicitarios que son enviados de forma masiva a un número elevado de usuarios al mismo tiempo, sin ser solicitados y que perjudican o interfieren con el resto de mensajes recibidos. Generalmente son recibidos por correo electrónico, pero también a través de otros medios, como el teléfono, la mensajería electrónica o actualmente las redes sociales.

Los mensajes considerados como SPAM tienen una serie de elementos característicos:

- Generalmente tienen un contenido publicitario.
- Suelen tener asuntos llamativos, para captar la atención del destinatario.
- La dirección del remitente suele ser desconocida e incluso en muchos casos falsificada. Los mensajes generalmente no permiten ser contestados. Y en el caso de que provengan de direcciones válidas, no sirve de nada contestar a estos mensajes de SPAM. Generalmente las respuestas serán dirigidas a usuarios que no tienen nada que ver con ellos.

El SPAM es un fenómeno que se ha generalizado en los últimos años, y cuya tendencia general va en aumento, hasta el punto de representar un porcentaje muy elevado de los mensajes de correo electrónico que se mueven en todo el mundo. Se calcula que aproximadamente el 80% de los mensajes de correo electrónico que circulan actualmente por Internet son SPAM.

Las medidas y soluciones anti-SPAM han evolucionado considerablemente para intentar detener esta plaga, pero aun así, los spammers no dejan de adaptarse e inventan nuevos sistemas para intentar que el SPAM sea efectivo, evitando así las distintas soluciones anti-spam.

2. Técnicas usadas por los spammers

La principal pregunta que se hace un usuario de correo electrónico que recibe SPAM de forma masiva es: ¿Por qué recibo de repente tanto correo basura? ¿Cómo han capturado mi cuenta de correo?

Generalmente, el principal objetivo de los spammers es el de conseguir el mayor número de direcciones de correo válidas y operativas. Para ello, utilizan numerosas y variadas técnicas, algunas de ellas muy sofisticadas:

- **Usan listas de correo:** los spammers consigue darse de alta en numerosas listas de correo y mediante diferentes técnicas consiguen las direcciones de correo electrónico de todos los usuarios pertenecientes a cada una de esas listas.

- Hacen uso de **programas específicos de rastreo automático** que recorren Internet en busca de direcciones de correo a partir de numerosas fuentes (páginas web, foros de discusión, blogs, etc).

- A partir de la **compra de extensas bases de datos de direcciones de correo** comercializadas por particulares o empresas. En el caso de España, esta práctica incumple la actual Ley Orgánica de Protección de Datos de carácter personal (LOPD de 15/1999 del 13 de Diciembre).

- Una técnica muy habitual es la **generación de direcciones de correo artificiales a partir de un dominio de Internet**, cambiando el nombre de usuario y enviando mensajes a las mismas. Estos ataques se suelen hacer mediante diccionarios de palabras o directamente mediante fuerza bruta, probando numerosas combinaciones de letras y números de forma automática. El servidor de correo electrónico perteneciente a ese dominio devolverá mensajes de error por cada una de las direcciones no válidas. Así, los spammers averiguan cuáles de las direcciones generadas son reales.

- A partir de **correos electrónicos con chistes, cadenas y adjuntos** que se suelen reenviar sin ocultar las direcciones (sin usar el campo Bcc), y que pueden llegar a acumular docenas de direcciones en el cuerpo del mensaje, pudiendo ser capturadas por un troyano o por un usuario malicioso.

- **Spam a través de ventanas emergentes (pop-ups)**. Se produce cuando estamos navegando por Internet y el navegador nos empieza a lanzar ventanas secundarias con mensajes, publicitarios o no, que poco o nada tienen que ver con la página que estamos visitando.

- **Hoaxes**. Son mensajes de correo electrónico, generalmente distribuidos en cadena, con contenido falso o engañoso. Algunos de estos mensajes están relacionados con virus falsos, fórmulas para ganar rápidamente una enorme cantidad de dinero, falsos mensajes de solidaridad y timos de lo más variado.

- A partir de la **entrada ilegal en servidores** lo que permite a los atacantes descargar cuentas de correo electrónico, una vez comprometidos los servidores.

- **Mediante troyanos y ordenadores zombis pertenecientes a botnets**. Desde hace un tiempo se ha extendido el uso de una técnica consistente en la creación de virus y troyanos que se expanden masivamente por ordenadores que no están

protegidos adecuadamente. Estos ordenadores infectados son utilizados por los spammers como "ordenadores zombi", que envían correo basura a sus órdenes, pudiendo incluso rastrear los discos duros o clientes de correo en busca de más direcciones. Esto puede causar perjuicios al usuario que ignora que esta infectado (no tiene por qué notar nada extraño), al ser identificado como spammer por los servidores a los que envía spam sin saberlo, lo que puede conducir a que se le deniegue el acceso a determinadas páginas o servicios. Actualmente, se calcula que el 40% de los mensajes no deseados se envían de esta forma.

- **Servidores de correo mal configurados**. En concreto los servidores configurados como open relays (reencaminadores abiertos) no necesitan un usuario y contraseña para que sean utilizados para el envío de correos electrónicos, por lo que cualquier puede hacer uso de ellos para el envío. Existen diferentes bases de datos públicas que almacenan listas de servidores configurados como open relays que permiten que los spammers hagan uso de ellos.

3. Cómo combatir el SPAM. Medidas prácticas

A pesar de que no existen técnicas infalibles para protegerse del correo basura, existen diferentes técnicas que podemos poner en práctica para restringir la disponibilidad de nuestras direcciones de correo electrónico, así como la prevención y la reducción de los mensajes de tipo SPAM recibidos en la bandeja de entrada de nuestro cliente de correo electrónico:

- **Desconfiar de los correos de remitentes desconocidos**. Ante la duda, eliminarlos directamente.

- **No abrir ficheros adjuntos sospechosos** procedentes de desconocidos o que no hayamos solicitado. **En cualquier caso, analizar los adjuntos con un buen antivirus** antes de ejecutarlos en nuestro sistema.

- **Utilizar el filtro anti-spam** de nuestro cliente de correo electrónico y marcar los correos como correo basura aquellos que estamos seguros que lo son, para entrenar al filtro y mejorar la detección en el futuro.

- **Ocultación de direcciones**. Esto se puede hacer publicando un nombre y dirección falsos. Los usuarios que quieren recibir correo legítimo podrán alterar sus preferencias en sus cuentas de manera que los usuarios puedan entenderlo, pero los spammers no. Por ejemplo, podríamos renombrar la cuenta

  usuario@ejemplo.com

  como

  usuarioNOS@PAM.ejemplo.com

  Cualquiera podría enviarnos correo sustituyendo la parte NOS@PAM por @, pero para un spammer sería una dirección no válida.

  Otra variante consiste en el uso de una imagen para publicar nuestra dirección de correo electrónico, en lugar de escribirla directamente.

- **No responder nunca al SPAM.** Los spammers solicitan a menudo respuestas respecto al contenido de sus mensajes, utilizando cualquier respuesta recibida del destinatario como la confirmación de que una dirección de correo electrónico es válida. Igualmente, muchos mensajes de SPAM contienen enlaces o direcciones que aparentemente permiten al usuario ser eliminado de la lista de correo de SPAM. En la gran mayoría de los casos estos enlaces no conducen a la dirección del destinatario, sino que conducen a más SPAM.

  Las direcciones de los remitentes en los mensajes de SPAM a menudo son falsificadas, incluyendo en muchos casos direcciones legítimas de usuarios obtenidas de una lista. Si respondemos a estos mensajes, nuestra respuesta podrá llegar a usuarios de correo electrónico inocentes cuya dirección ha sido comprometida, con lo que contribuimos aún más a difundir el problema.

- **Ser cautos al rellenar formularios en páginas web.** Los formularios permiten a los usuarios remitir su correo electrónico, además de muchos otros datos, mediante un simple navegador web. Estos formularios son usados a menudo por los spammers de forma que quien lo rellena no puede ver la dirección de correo electrónico destino a la que se envían los datos, por lo que resultan una forma habitual de captar direcciones de correo electrónico. **Esta recomendación es especialmente importante si nos solicitan contraseñas, números de tarjeta de crédito o cualquier otra información sensible.**

- **Desactivar HTML en el correo electrónico** siempre que sea posible. Muchos clientes de correo actuales incorporan funcionalidades web, tales como la composición y visualización de mensajes en formato HTML, y la inclusión de imágenes. Esto puede generar todo un conjunto de amenazas como SPAM mediante imágenes, inclusión de código en lenguaje javascript que puede redirigir el navegador web del usuario a páginas de publicidad, etc. Si desactivamos en nuestro cliente de correo electrónico la vista previa de los mensajes, la descarga automática de imágenes y otros elementos y no usamos HTML, imágenes o archivos adjuntos en nuestros mensajes, tenemos mucho menos riesgo de recibir SPAM y evitaremos cualquier posible código malicioso que pueda estar incluido en el cuerpo de los mensajes.

- **Disponer de direcciones de correo electrónico alternativas.** Muchos usuarios de correo electrónico tienen a veces la necesidad de dar su dirección de correo electrónico en sitios web sin tener la garantía absoluta de que el sitio no enviará SPAM. Una forma de eliminar este riesgo consiste en proporcionar una dirección de correo electrónico temporal o secundaria que usaremos solo en estos casos, asegurando así nuestra dirección de correo habitual.

- Tener precaución con los **mecanismos de recuperación de contraseñas que ofrecen muchos sitios webs.** Generalmente proponen elegir una pregunta que le harán al usuario en caso de que solicite recuperar su contraseña. En estos casos, se recomienda utilizar una pregunta cuya respuesta sólo conozcamos nosotros.

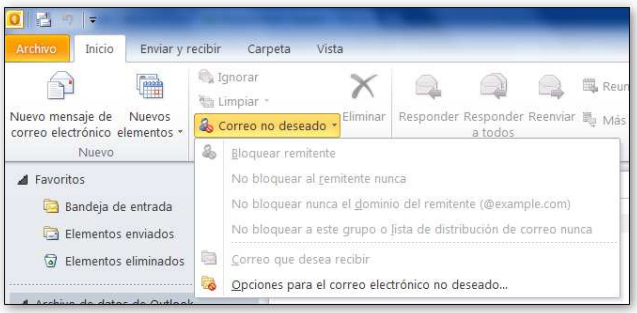
- **No facilites tu cuenta de correo a desconocidos** ni la publiques alegremente en Internet.

- Cuando reenvíes mensajes a múltiples destinatarios **utiliza siempre la copia oculta** (CCO ó BCC) para introducir las direcciones de los destinatarios.

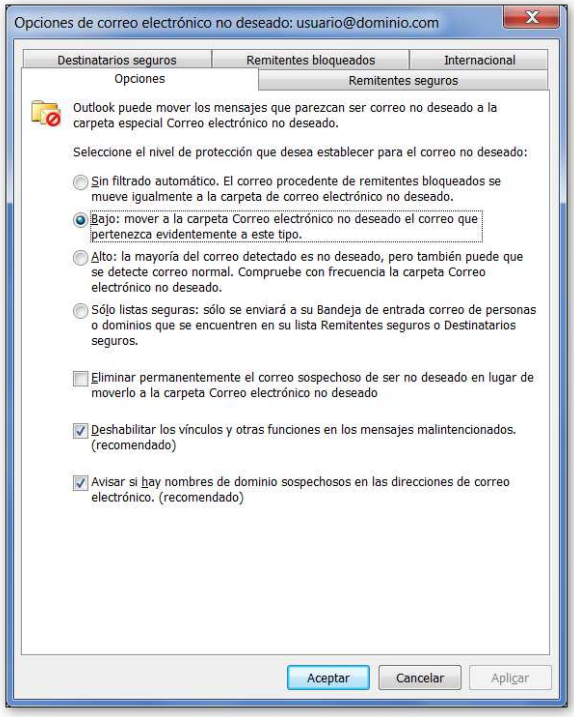
4. Filtrar el SPAM en el cliente de correo electrónico

4.1. Microsoft Outlook

La configuración de los filtros anti-spam se hace desde la pestaña **Inicio > Correo no deseado > Opciones para el correo electrónico no deseado**.



A partir de aquí accedemos a la ventana de configuración de las distintas opciones del filtro anti-spam de Outlook:



En ella podemos configurar los siguientes elementos:

- **Selección del nivel de protección**: tenemos varias opciones: sin filtrado automático (filtro anti-spam desactivado), bajo, alto o solo aceptar correo de las listas de remitentes o destinatarios que hayamos definido como seguros. Estos elementos se pueden configurar mediante las pestañas: Remitentes seguros,

Destinatarios seguros y Remitentes bloqueados. Mediante la pestaña "Internacional" podemos bloquear dominios de nivel superior y juegos de caracteres de idiomas específicos.

- **Eliminar definitivamente el correo sospechoso.** Por defecto se mueve a la carpeta "Correo electrónico no deseado".

- **Deshabilitar vínculos (enlaces) y otros elementos potencialmente sospechosos** en los correos. Esto evita que el usuario haga clic en elementos sospechosos que suelen ser las vías principales de infección (opción recomendada).

- **Avisar si hay nombres de dominio sospechoso en las direcciones de correo** (opción recomendada).

Configuraciones adicionales

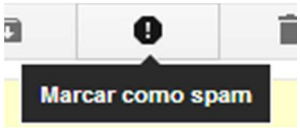
Como medidas adicionales, podemos desactivar el uso de HTML en el correo. Esto se hace desde el menú **Archivo > Opciones > Correo > Redactar mensajes**. En el desplegable que aparece ("Redactar mensajes en este formato"), seleccionaremos "Texto sin formato".

4.2. Gmail (Google)

Gmail detecta automáticamente los mensajes de SPAM y los sospechosos, y ambos son marcados como SPAM. Cuando abrimos la etiqueta SPAM, vemos todos los mensajes marcados como correo no deseado por nosotros o por Gmail. En la parte superior de cada correo, se muestra una etiqueta donde se explica por qué se ha colocado en SPAM.

Puede haber varios casos:

- **Direcciones de correo electrónico falsas.** Esto significa que la dirección de origen es prácticamente idéntica a la de un remitente conocido. Por ejemplo: en vez de la letra "O", la dirección tiene el número "0". En estos casos, no respondas al mensaje ni abras ningún enlace hasta que compruebes que la dirección corresponde a un remitente fiable. Si detectas una dirección de correo falsa, pero no está marcada con una advertencia, puedes marcar el correo como SPAM con el siguiente botón:



- **Suplantación de identidad (*phishing*).** Algunos spammers intentan engañarte para que compartas datos personales, como contraseñas o números de tarjetas de crédito. Cuando veas esta advertencia:
  - No respondas al correo ni abras ningún enlace.
  - Si no tienes claro que el correo sea de un remitente fiable, denuncia el mensaje por phishing: https://support.google.com/mail/contact/abuse

NOTA: Google nunca te pedirá datos personales por correo electrónico.

- **Mensajes de un remitente no confirmado.** Significa que Gmail no puede confirmar que el correo haya sido enviado por la persona o empresa del remite. Cuando veas esta advertencia:

  - No respondas al correo ni abras ningún enlace.
  - Si no tienes claro que el correo sea de un remitente fiable, denuncia el mensaje por phishing: https://support.google.com/mail/contact/abuse

  Si tienes la certeza de que el mensaje es fiable:

  - En su parte superior, haz clic en **No es spam**.
  - Para evitar que los mensajes de un remitente de confianza se coloquen en Spam, sigue las siguientes instrucciones: https://support.google.com/mail/answer/185812#trusted_sender

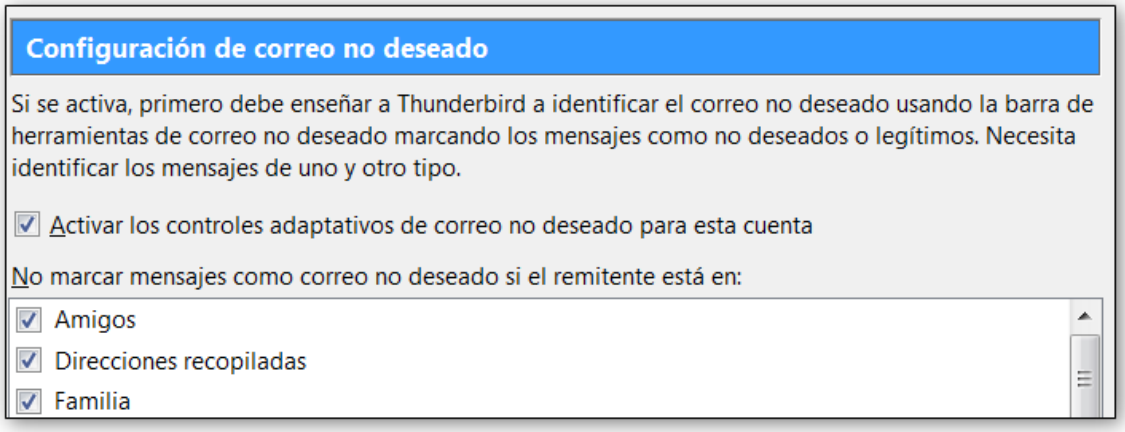
- **El mensaje está vacío.** Los spammers a menudo envían mensajes sin nada en el cuerpo o en el asunto para saber si las direcciones son válidas. Después de confirmarlo, envían spam a esas direcciones. Si el correo te parece sospechoso, no respondas. Puedes **denunciarlo como spam** o como **phishing**. En cambio, si el correo es de alguien que conoces y crees que te lo ha mandado sin querer, selecciona **No es spam**.

- **Si recibes spam de uno de tus contactos**, es posible que un usuario malintencionado haya interceptado su cuenta. En tal caso:

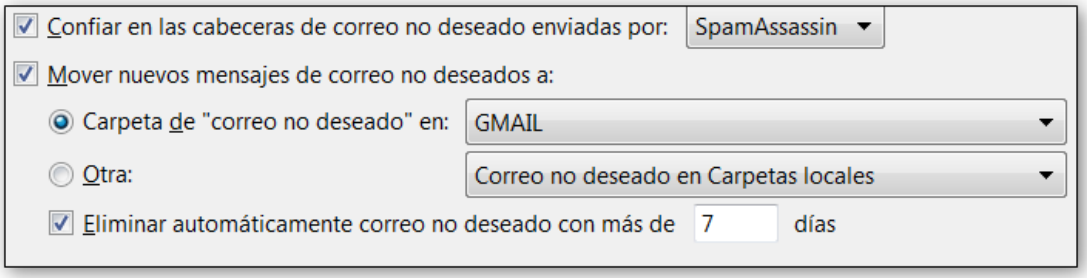
  - No respondas al correo.
  - Denuncia el mensaje haciendo clic en **El mensaje parece sospechoso** en la alerta de spam. De esta forma, se envía un informe al equipo de Gmail para que lo investigue. Seguirás recibiendo correos de ese contacto en el futuro.
  - Avisa a tu contacto y aconséjale que siga las siguientes sugerencias de seguridad de Gmail: https://support.google.com/mail/answer/7036019

4.3. Mozilla Thunderbird

La configuración de los filtros anti-spam con este cliente de correo electrónico se hace en las opciones de configuración de las cuentas de correo. El primer paso consiste en activar el filtro anti-spam, entrando en el menú **Herramientas > Configuración de las cuentas** y en la cuenta en la que queremos activar el filtro, entramos en **Correo no deseado**. El filtro se activa marcando la casilla **"Activar los controles adaptativos de correo no deseado para esta cuenta"**.



En esa misma ventana de configuración tenemos otras opciones adicionales que podemos marcar:



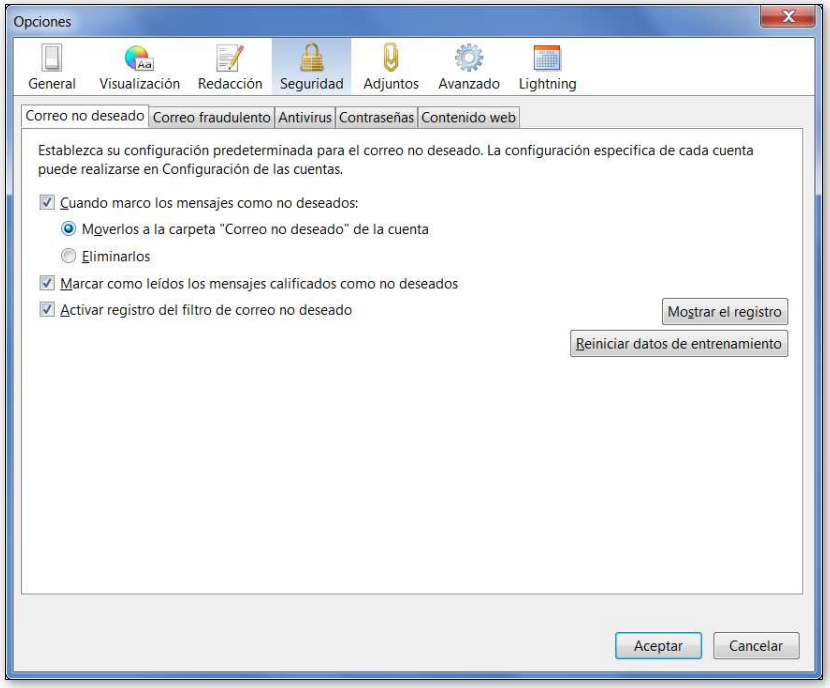
- **No marcar mensajes como correo no deseado si el remitente está en…** esta opción permite que los mensajes cuyo remitente esté en una de nuestras libretas de direcciones sean siempre aceptados (no analizados por el filtro anti-spam).

- **Confiar en las cabeceras de correo no deseado enviadas por…** permite seleccionar una serie de filtros anti-spam habituales que directamente ya insertan una etiqueta en el asunto de aquellos mensajes detectados como spam, evitando así que sean analizados por segunda vez.

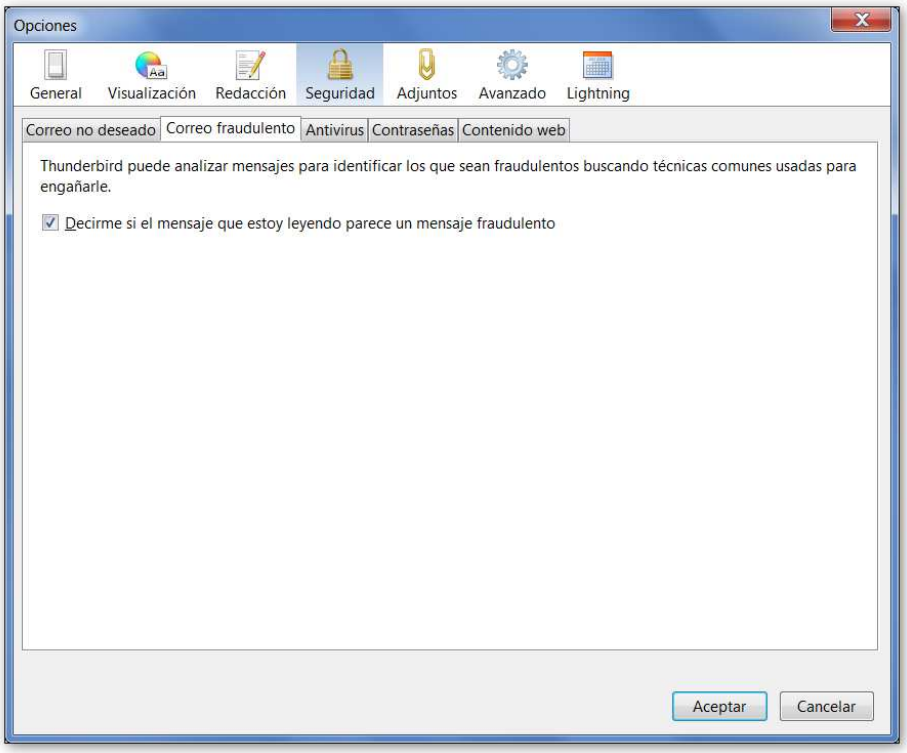
- **Mover nuevos mensajes de correo no deseado a:** nos permite indicar a qué carpeta se moverán los mensajes que sean detectados como spam por el filtro.

- **Eliminar automáticamente correo no deseado con más de X días:** permite eliminar de forma automática el correo basura que lleve filtrado más de X días, sin intervención del usuario.

Además, en Thunderbird se pueden configurar una serie de opciones relacionadas con el correo basura y la detección de mensajes fraudulentos. Estas opciones se configuran desde el menú **Herramientas > Opciones > Seguridad:**



Podemos seleccionar el comportamiento del correo marcado como SPAM (moverlo a la carpeta "Correo no deseado" o eliminarlo directamente), marcar los correos basura como leídos en cuanto son detectados y activar o no un registro con todo el correo basura detectado. Podemos reiniciar los filtros de entrenamiento (el aprendizaje que ya ha hecho Thunderbird) pulsando en **Reiniciar datos de entrenamiento**. Por último, en la pestaña "Correo fraudulento" podemos indicar a Thunderbird que active o no la detección de correo supuestamente fraudulento.



El filtro anti-spam que incorpora Thunderbird es muy efectivo. No obstante, pueden pasar correos basura que Thunderbird no detecte. En este caso, podemos marcarlos manualmente, pulsando en el icono:

(marcar este mensaje como correo no deseado). Si hacemos esto con frecuencia ayudaremos a Thunderbird a mejorar su sistema de detección.

Configuraciones adicionales

Como medidas adicionales, podemos desactivar el uso de HTML en el correo. Esto se hace desde el menú **Herramientas > Configuración de la cuenta**. En la cuenta que estemos usando, pulsamos en el link **Redacción y direcciones** y desmarcamos la opción **"Redactar mensajes en formato HTML"**.

5. Referencias en Internet

- Instituto Nacional de Ciberseguridad (INCIBE)
  http://www.incibe.es/
- Oficina de Seguridad del Internauta (OSI)
  http://www.osi.es/
- CCN-CERT
  https://www.ccn-cert.cni.es/
- Guardia Civil - Grupo de Delitos Telemáticos:
  https://www.gdt.guardiacivil.es
- Policía Nacional – Brigada de Investigación Tecnológica
  http://www.policia.es/org_central/judicial/udef/bit_alertas.html
- RedIris – Abuso en el servicio de correo electrónico
  http://www.rediris.es/mail/abuso/
- http://www.delitosinformaticos.com/