[Capítulo 4]

Correo electrónico

Cambiar el lector de correo: Thunderbird

Igual que en el caso del navegador, no es recomendable utilizar el lector de correo que lleva incorporado Windows, *Outlook Express*, ni tampoco su hermano mayor, *Outlook*, que suele venir incluido en *Microsoft Office*, sino algún otro sustituto como puede ser *Thunderbird*. Este es un lector de correo de los mismos creadores de *Firefox* y que, por lo tanto, dispone de muchas de sus mismas características: mayor seguridad, código abierto, gratuito, multiplataforma, extensible...

Porqué debería usar Thunderbird en lugar de Outlook?

En primer lugar, *Thunderbird* ofrece mucha más seguridad que *Outlook*. A principios de 1999 vio la luz el virus *Melissa*, el primer virus con una gran expansión que utilizaba el correo electrónico para reproducirse. Al abrir un archivo que llevaba adjunto el mensaje el virus se ejecutaba y se enviaba a si mismo a las primeras 50 entradas de la libreta de direcciones de *Outlook*. Al año siguiente apareció el famoso virus ILOVEYOU, que también utilizaba las direcciones de *Outlook* para enviarse al ejecutar un fichero adjunto al mensaje.

En 2001, el virus *Nimda* aprovechaba una vulnerabilidad en *Outlook* para ejecutarse sin necesidad de interacción por parte del usuario. No era necesario abrir ningún fichero adjunto, el simple hecho de visualizar el mensaje ya ejecutaba el virus. Aunque estos son los más conocidos no son los únicos virus que existen que utilizan *Outlook* para propagarse.

Otra razón para usar *Thunderbird* es el filtro que incorpora para detectar el correo basura, *spam* que suele llenar nuestros buzones con mensajes comerciales indeseables, y del que hablaremos después más detalladamente. También dispone de otra serie de opciones para proteger nuestra privacidad, como la desactivación de la visualización de imágenes en mensajes sospechosos de ser *spam*.

Finalmente, *Thunderbird* nos facilita la migración desde *Outlook* o desde *Outlook Express*, ya que permite importar todos los datos desde estos dos programas o desde versiones anteriores de *Netscape*.

Correo basura

Conocemos como *spam* o "correo basura" aquellos mensajes no deseados o no solicitados que llegan a nuestra cuenta de correo. Habitualmente, consisten en publicidad de productos poco o nada legales o en esquemas para hacerse rico rapidamente.

Los *spammers*, como se conoce a la gente que envía este tipo de correos, utilizan esta técnica porque es una manera muy barata y rápida de hacer llegar el mensaje a muchísima gente. Al no ser el *spammer* el que carga con los gastos de enviar esos correos, sino que suelen ser o bien los usuarios que los reciben o bien el servidor desde donde se envían, pueden enviar millones de mensajes al mismo tiempo. Uno de los últimos métodos utilizados por los *spammers* es el uso de ordenadores infectados por virus, de los cuales toman el control remotamente y desde donde envían el *spam*. Existen, incluso, organizaciones que venden listas con las direcciones de estos ordenadores listos para ser usados como plataformas de envío masivo de mensajes.

El problema para el usuario es que, hoy en dia, el *spam* suele superar en número a los mensajes que sí le interesan, de forma que tiene que borrar una gran cantidad de mensajes que no quiere leer para llegar al correo genuino. Todo esto, además, vigilando de no perder entre todo este *spam* mensajes realmente importantes. Según algunos estudios, un tercio del correo electrónico enviado en Estados Unidos es *spam*, aunque hay quien considera este porcentaje muy bajo y dependiendo del servidor podría llegar a tasas del 98% del correo recibido.

Para conseguir direcciones de correo donde poder enviar sus mensajes, los *spammers* suelen recorrer las páginas web, mediante programas conocidos como *bots*, buscando palabras que coincidan con el formato de una dirección de correo (es decir, cualquier cosa que se parezca a nombre@servidor.com). Para impedir que los spammers puedan encontrar así nuestra dirección podemos utilizar una serie de técnicas distintas:

- Distorsionar deliberadamente nuestra dirección, de forma que quien quiera escribirnos pueda hacerlo, pero un *bot* utilize una dirección erronea por no saber interpretarla. Por ejemplo, si nuestro correo es minombre@example.com podríamos transcribirlo como minombreQUITAR@ESTOexample.com. Esto debemos hacerlo siempre que nuestra dirección vaya a aparecer publicada en cualquier sitio (un foro, un comentario en alguna página,...)

- Utilizar dos cuentas diferentes, nuestra cuenta habitual, cuya dirección solo proporcionaremos a gente de confianza, y una cuenta en un servidor gratuito para todos los sitios que nos pidan una dirección de correo para podernos registrar. De este modo, si nos envían spam a esa dirección no la recibiremos en nuestra cuenta personal.

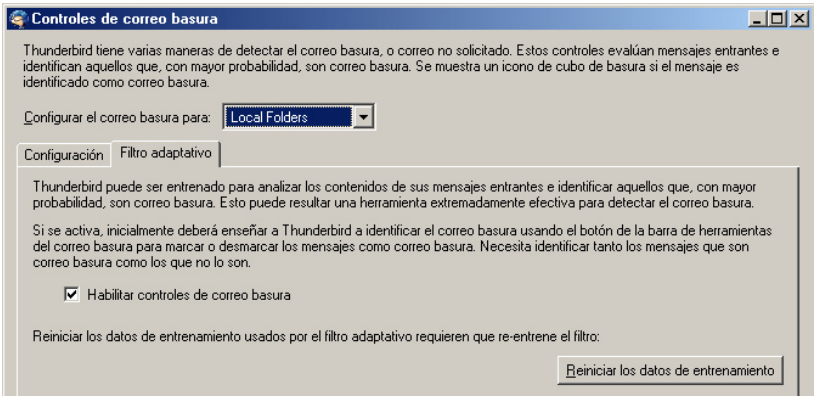
- Muchas de estas direcciones se consiguen pidiendo la dirección para que nos envíen algo a nosotros o a algún amigo (felicitaciones "electrónicas", chistes,...). No debemos dar nuestra dirección ni la de nadie en ninguno de estos sitios si no es de total confianza.

- En caso de que recibamos *spam* en nuestra cuenta no debemos responder nunca al mensaje recibido, ya que la dirección de origen suele ser falsa. Aunque muchos de estos correos suelen llevar una dirección donde podemos darnos de baja, no debemos hacerlo nunca ya que de esta manera confirmaríamos al spammer que nuestra dirección de correo realmente existe y que además hemos leído el mensaje que nos ha enviado, con lo cual nos convertimos en un objetivo deseado para que nos envíen más correo de este tipo.

Detectando el correo basura automáticamente

Thunderbird dispone de una herramienta para clasificar el correo electrónico, de forma que puede detectar automáticamente y con una gran probabilidad de acierto si un mensaje es *spam* o es un correo legítimo. Para ello utiliza un algoritmo conocido como *filtro bayesiano*, que consiste en conocer la probabilidad de que una palabra aparezca en un mensaje corriente y en uno de *spam*. De este modo, examinando las palabras de un mensaje y conociendo sus diferentes probabilidades será capaz de distinguir entre un tipo y otro.

Para activar este filtro debemos ir al menú *Herramientas -> Controles de correo basura*



y en el apartado *Filtro adaptativo* marcamos la opción *Habilitar controles de correo basura* para todas las cuentas que tengamos.

Una vez activado deberemos entrenar a *Thunderbird* para que reconozca que mensajes son correo basura y cuales son correo legítimo.

Para ello utilizaremos el botón *Basura* de la barra de tareas en caso de que encontremos un mensaje de *spam* y queramos clasificarlo como tal.

Utilizaremos el botón *No es correo basura* en caso de que *Thunderbird* nos clasifique algún correo incorrectamente como *spam*.

Una vez hayamos entrenado suficientemente al programa, este será capaz de clasificar correctamente los correos que recibamos y puede moverlos directamente a una carpeta especial si así se lo indicamos, para que ni siquiera tengamos que verlos.

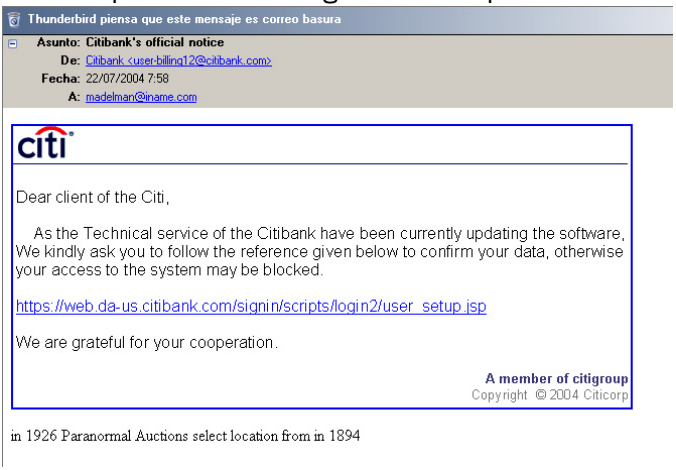
En caso de que activemos esta última opción es recomendable revisar una vez por semana la carpeta de correo basura, de forma que no perdamos algún correo importante al haber sido mal clasificado.

Phishing

Una modalidad de timo usada en Internet es el envío de emails que simulan provenir de nuestro banco o de alguna tienda de Internet, como Amazon. Suelen avisar de que nuestra contraseña puede haber sido comprometida, que están validando a los usuarios o nos piden que confirmemos algún cargo que se ha hecho a nuestra nombre. Para ello necesitan que entremos en nuestra cuenta y nos ofrecen un enlace que permite entrar directamente en ella.

Este enlace nos va a redirigir a una página creada por el timador, con un aspecto lo más parecido posible al original, pero controlada por él, de forma que cuando introduzcamos nuestro número de cuenta o DNI y la contraseña asociada, estos no irán a parar al banco o tienda, sino al timador que dispondrá de ellos y podrá acceder a nuestra cuenta como si fuéramos nosotros.

Estos correos suelen estar escritos en formato HTML y simulan con gran fidelidad el look corporativo del banco o tienda, por lo que puede resultar sencillo que el usuario caiga en la trampa sin darse cuenta.


Thunderbird piensa que este mensaje es correo basura

Asunto: Citibank's official notice
De: Citibank <user-billing12@citibank.com>
Fecha: 22/07/2004 7:58
A: madelman@iname.com

citi

Dear client of the Citi,

As the Technical service of the Citibank have been currently updating the software, We kindly ask you to follow the reference given below to confirm your data, otherwise your access to the system may be blocked.

https://web.da-us.citibank.com/signin/scripts/login2/user_setup.jsp

We are grateful for your cooperation.

A member of citigroup
Copyright © 2004 Citicorp

in 1926 Paranormal Auctions select location from in 1894

Como ejemplo, podemos ver este correo donde se informa que el software utilizado por el banco está siendo actualizado y que es necesario que entremos en nuestra cuenta para verificar nuestros datos. Para ello, ofrecen un supuesto enlace que parece apuntar a la página de Citibank, pero que gracias a la manipulación de la dirección en realidad apunta a http://200.246.11.135:3127/cit/index.htm que corresponde a una máquina que está bajo el control del timador.

Como protegernos del phishing?

Debemos tener en cuenta que es muy poco probable que nuestro banco nos envíe un correo electrónico para verificar nuestros datos o para informarnos de algún cargo a nuestra cuenta. Aun así, existe la posibilidad de que alguno de estos correos sea realmente de nuestro banco, pero debemos asegurarnos de ello y tomar una serie de precauciones antes de actuar:

- Tener en cuenta que el correo puede ser falso por lo que deberemos comprobarlo por algún otro medio

- Comprobar que el correo está bien escrito, sin faltas de ortografía, bien redactado y es coherente. Los *phishers*, muchas veces, ni siquiera se preocupan de preparar bien sus mensajes o de escribirlos correctamente.

- No acceder nunca a la página mediante el enlace que nos ofrecen. Es mucho más seguro acceder a través del navegador y escribir nosotros mismos la dirección para entrar.

- En caso de duda ponernos en contacto telefónico con la entidad para comprobar la autenticidad y veracidad del mensaje recibido.

Cadenas

Con cierta regularidad recibimos en nuestros buzones electrónicos mensajes enviados en cadena por conocidos nuestros donde se nos advierte de supuestos peligros, de supuestos virus o se nos pide nuestra colaboración para algún tipo de proyecto.

Estos correos, conocidos como *hoaxes*, suelen ser enviados con la mejor intención, pero resultan casi siempre falsos, como una especie de leyenda urbana distribuida por Internet.

Podemos distinguir un mensaje de este tipo porque suele anunciar grandes desgracias en caso de que no lo reenvíes a un cierto número de personas, no suelen ir firmados, nos prometen regalos por parte de alguna compañía o nos ofrecen alguna información poco creíble. Algunos ejemplos de este tipo de correos son:

- Envía este email a 10 personas y un niño recibirá un dolar por cada mensaje
- Nokia esta haciendo promoción de sus móviles. Envía este email a 800 personas y recibirás un móvil gratuito
- Hay un virus muy peligroso. Busca cierto fichero en tu disco y si existe borralo
- Reenvía esta cadena a 15 amigos o te quedaras calvo en menos de una semana

No debemos reenviar nunca estos correos puesto que, con ello, lo único que conseguimos es saturar el tráfico de la red y llenar los buzones de nuestros conocidos de mensajes que probablemente no les interesen. En caso de duda, podemos consultar la página Rompecadenas para saber si un correo es de este tipo.

Privacidad del correo

Normalmente consideramos que los correos electrónicos que enviamos son como una carta, van guardado dentro de un sobre y nadie puede leerlos. Esto no es cierto, ya que estos correos viajan como texto plano (es decir, texto visible a simple vista) por lo que pueden ser vistos por cualquier sistema por donde pasen. Debemos tener en cuenta que, muchas veces, los mensajes no viajan directamente al servidor del destinatario, sino que pasan por diversos servidores intermedios antes de llegar a su destino. Podemos verlo en las cabeceras de un correo real:

```
Received: from 205-158-62-26.outblaze.com
([205.158.62.26] helo=spf4.us.outblaze .com) by xxxx
with esmtp (Exim 3.35 #1 (Debian)) id 1AWFK5-0004pF-00
for <xxx@xxx.com>; Tue, 16 Dec 2003 14:33:14 +0100

Received: from web60809.mail.yahoo.com
(web6080.mail.yahoo.com [216.155.196.72]) by
spf4.us4.outblaze.com (Postfix) with SMTP id
9E99D1BA1EE for <xxx@xxx.com>; Tue, 16 Dec 2003
13:38:21 +0000 (GMT)

Received: from [213.0.240.13] by
web60809.mail.yahoo.com via HTTP; Tue, 16 Dec 2003
14:38:03 CET
```

Cada una de las lineas *Received* indica un servidor por donde ha pasado el correo, de forma que cualquiera de los servidores puede haber leído el contenido del mensaje enviado.

Además, si utilizamos el protocolo IMAP para leer el correo, este suele quedar almacenado en el servidor, donde el administrador puede leerlo facilmente. Esto desde luego no es legal pero es difícilmente detectable.

También existe la posibilidad, en caso de estar utilizando una cuenta de correo otorgada por la empresa en que trabajamos, que esta esté controlada, es decir, que se monitorice el uso de esta e incluso el contenido de los emails enviados y recibidos. La legalidad de este tipo prácticas no está demasiado clara, habiendo incluso sentencias judiciales contradictorias.

De forma similar al correo tradicional, el remitente de un correo electrónico es muy fácil de falsificar. Si queremos cambiar el remitente de una carta tan solo debemos escribir la dirección que nos interese en el reverso del sobre; de igual manera podemos modificar el remitente de un correo electrónico. La mayoría de programas de correo permite cambiar la cabecera y indicar la dirección que nosotros queramos, y aunque se puede saber si el remitente ha sido falseado este es un proceso complicado y que puede no llevarnos a descubrir el verdadero remite.

Cómo podemos proteger nuestro correo?

Para resolver el problema de la falta de privacidad y de la autenticación se utiliza la firma digital; esta permite confirmar que quien envía el mensaje es quien dice ser y/o cifrar el mensaje de forma que solo su destinatario pueda leerlo. Existen diversos sistemas de firma digital, entre ellos los más conocidos y utilizados son S/MIME y los basados en OpenPGP.

Los programas de firma digital permiten dos funciones principales: la firma y el cifrado de los mensajes.

La firma permite garantizar que el origen del mensaje es el correcto y que el contenido del mensaje no ha sido modificado.

El cifrado permite que solo el destinatario pueda leer un determinado mensaje. Habitualmente se combina con la firma, de forma que solo el destinatario correcto verá el contenido del mensaje y podrá saber que no ha sido manipulado y además podrá garantizar por quien ha sido enviado.

Cómo funciona la firma digital

Para conseguir la seguridad requerida en el correo electrónico se utilizan una serie de funciones matemáticas, englobadas dentro del campo de la criptografía. Existen varios conceptos clave para entender como funciona todo el sistema:

- **Criptografía de clave simétrica:** Los sistemas de clave simétrica utilizan una misma clave para cifrar y descifrar, de forma que tanto el emisor como el receptor del mensaje deben ponerse de acuerdo previamente en la clave a utilizar. El mensaje a enviar se divide en bloques de igual tamaño y a cada uno de estos bloques se le aplica la misma función de cifrado. El receptor aplica la función de descifrado a cada uno de los bloques recibidos y obtiene el mensaje original. Ejemplos de este tipo de algoritmos son *DES*, *Blowfish* o *AES-Rijndael*.
- **Criptografía de clave asimétrica:** Los sistemas de clave asimétrica utilizan claves distintas para cifrar y para descifrar. De esta forma, se pretende evitar el problema de que los comunicantes tengan que acordar previamente una clave. Cada uno de ellos dispone de un par de claves, una pública, que permite cifrar y verificar firmas y una privada, que permite descifrar y firmar. La clave pública se puede distribuir a cualquier persona y la clave privada es la que debe mantenerse en secreto. Si "A" quiere enviar un mensaje a "B" debe cifrarlo con la clave pública de "B", de forma que este solo podrá ser descifrado con la clave privada de "B". Ejemplos de este tipo de algoritmos son *RSA* o *ElGamal*.

- **Funciones resumen (hash):** Las funciones resumen hacen corresponder un mensaje de longitud arbitraria a otro de longitud fija (el *hash*, normalmente más pequeña). Esta función debe cumplir dos condiciones: ha de ser difícil encontrar dos mensajes diferentes cuyo *hash* sea el mismo y dado el *hash* ha de ser imposible conocer el mensaje original.

El inconveniente de los sistemas de clave asimétrica es que son mucho más lentos que los de clave simétrica, por lo que se suelen cifrar los mensajes con un clave simétrica aleatoria (clave de sesión) que se cifra con un sistema de clave asimétrica para darla a conocer al otro participante de la conversación. De este modo, en lugar de cifrar todo el mensaje (que potencialmente puede ser muy extenso) con la clave pública solo cifraremos una clave de sesión, lo cual nos ahorrará mucho tiempo.

La mejor forma de entender como funciona todo esto es ver un ejemplo: supongamos que "A" quiere enviar un mensaje cifrado a "B". Para ello deberá hacer:

1. Crear una clave aleatoria K
2. Cifrar el mensaje original M con la clave K obteniendo M'
3. Cifrar la clave K con la clave pública de B, obteniendo K'
4. Enviar M' y K' a B

Cuando B reciba M' y K' deberá hacer:

1. Descifrar K' con su clave privada, obteniendo K
2. Descifrar M' con la clave K, obteniendo M

Este proceso se complica si además de enviar el mensaje cifrado se quiere enviar también firmado, pues entonces también entran en juego la clave privada y la pública de A.

Si "A" quiere enviar un mensaje firmado a "B" (de forma que B puede asegurar que A ha escrito ese mensaje y que el contenido no ha sido modificado) deberá hacer:

1. Hacer un resumen del mensaje M, obteniendo H
2. Cifrar H con su clave privada, obteniendo H'
3. Enviar M y H' a B

Cuando B reciba M y H', para comprobar que ha sido enviado por A deberá hacer:

1. Hacer un resumen de M, obteniendo J
2. Descifrar H' con la clave pública de A, obteniendo H
3. Si H es igual a J la firma es correcta

Finalmente, si A quiere enviar a B un mensaje cifrado y firmado deberá realizar los siguientes pasos:

- Primero se debe firmar el mensaje:
  1. Hacer un resumen del mensaje M, obteniendo H
  2. Cifrar H con su clave privada, obteniendo H'
  3. Juntamos M y H' obteniendo N
- Después se debe cifrar N:
  1. Crear una clave aleatoria K
  2. Cifrar el mensaje N con la clave K obteniendo N'
  3. Cifrar la clave K con la clave pública de B, obteniendo K'
  4. Enviar N' y K' a B

Y B para leer el mensaje y comprobar que ha sido escrito por A deberá hacer:

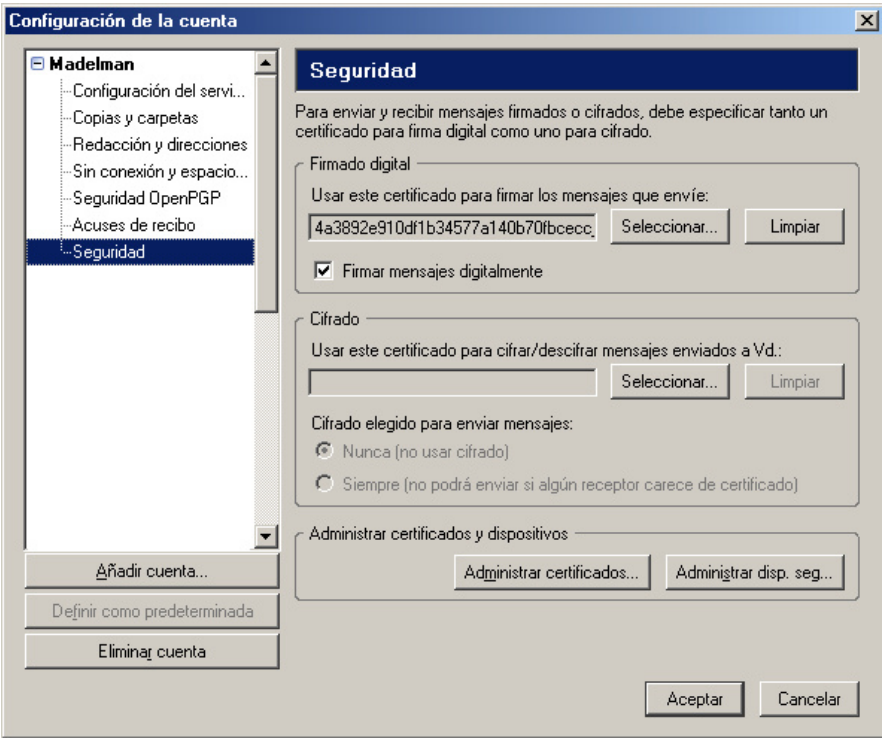
1. Descifrar K' con su clave privada, obteniendo K
2. Descifrar N' con la clave K, obteniendo N
3. N está compuesto por M y H'
4. Hacer un resumen de M, obteniendo J
5. Descifrar H' con la clave pública de A, obteniendo H
6. Si H es igual a J todo ha sido correcto

Automatizando el proceso

La teoría matemática detrás de este proceso es complicada, por suerte existe una serie de programas como GPG que se encarga de realizar todos estos pasos por nosotros automáticamente. Además, también se comprime el mensaje que queremos enviar para reducir el espacio que ocupa y aumentar la seguridad. Otra medida que utiliza GPG es la petición de una contraseña antes de poder usar la clave privada, de forma que nadie pueda usar nuestra clave privada sin conocer esta contraseña.

En nuestro caso vamos a utilizar la función integrada en Thunderbird, basada en S/MIME. Para ello, en primer lugar, necesitamos conseguir nuestro certificado de usuario. Podemos conseguir uno gratuitamente en http://www.cacert.org. Allí nos daremos de alta y el sistema nos enviará un correo a nuestra dirección para comprobar nuestra identidad; posteriormente, podremos descargarnos el certificado, que quedará instalado en nuestro navegador. Una vez instalado, podremos exportarlo desde el navegador (en primer lugar, para hacer una copia de seguridad) e importarlo en nuestro programa de correo.
Otra opción, en el caso de España, es utilizar el certificado que nos ofrece la Fábrica Nacional de Moneda y Timbre, que también sirve para presentar la declaración de Hacienda a través de Internet y otras gestiones con la Administración. Este certificado se puede conseguir en http://www.cert.fnmt.es

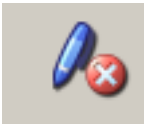
Para utilizar este certificado en Thunderbird, una vez lo hayamos exportado desde nuestro navegador, vamos al menu *Herramientas -> Configuración de cuentas* y entramos en la opción *Seguridad*. Desde allí entramos en *Administrar certificados* donde nos permitirá importar nuestro certificado.



Posteriormente debemos configurar nuestra cuenta para que use este certificado para firmar los mensajes que enviemos. Para ello, una vez importado el certificado, lo seleccionamos en la opción de Firmado digital y marcamos la opción *Firmar mensajes digitalmente*

Una vez lo tengamos activado todos los mensajes que enviemos se firmaran digitalmente y nuestros contactos podrán comprobar que el correo recibido es legítimo. Para ello necesitarán tener nuestra clave pública, que les deberemos proporcionar nosotros y que podemos obtener exportándola desde el navegador (recordando siempre de no distribuir nuestra clave privada a nadie bajo ningún concepto).

Cuando alguien nos envíe un correo electrónico firmado podremos comprobar si es válido o no. Thunderbird muestra un icono como este



si el mensaje está firmado pero no se ha podido comprobar la autenticidad del firmante, habitualmente porque no disponemos de su clave pública. En caso de que sí dispongamos de su clave pública Thunderbird comprobará la identidad y si esta es correcta mostrará el icono

con lo que podemos estar seguros de que el mensaje es de quien dice ser y que el contenido no ha sido modificado por nadie. También podemos hacer servir estos certificados para enviar correo cifrado, de forma que solo su destinatario pueda leerlo.

Referencias

Artículos sobre la privacidad del correo en el trabajo
http://www.baquia.com/com/20001221/art00032.html
http://www.informatica-juridica.com/trabajos/el_uso_del_correo_electronico_en_el_trabajo.asp

Artículos con información sobre el virus ILOVEYOU
http://www.virusprot.com/Vi00012a.html
http://www.vsantivirus.com/loveletter.htm

Artículo con información sobre el virus NIMDA
http://www.hispasec.com/unaaldia/1061

Artículos con información sobre la proporción de spam
http://www.theregister.co.uk/2004/04/20/idc_spam_survey/
http://it.slashdot.org/article.pl?sid=04/04/20/1558244&tid=111

Cómo evitar el spam
http://www.rickconner.net/spamweb/avoiding.html

Información sobre el spam
http://spam.abuse.net/overview/

Grupo de trabajo contra el phishing
http://www.antiphishing.org/

Artículo sobre el phishing
http://www.consumer.es/web/es/especiales/2004/09/22/109261.php

Información sobre las cadenas en el correo electrónico
http://www.rompecadenas.com.ar/

Introducción al funcionamiento PGP
http://www.pgpi.org/doc/pgpintro/