

Proyecto conjunto:

Servicios de Red e Internet

Implantación de Aplicaciones

Web

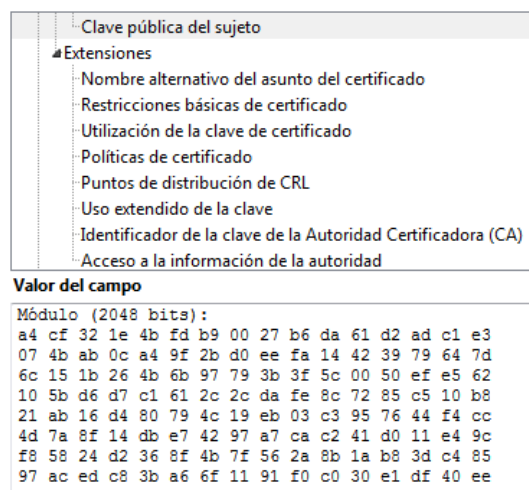
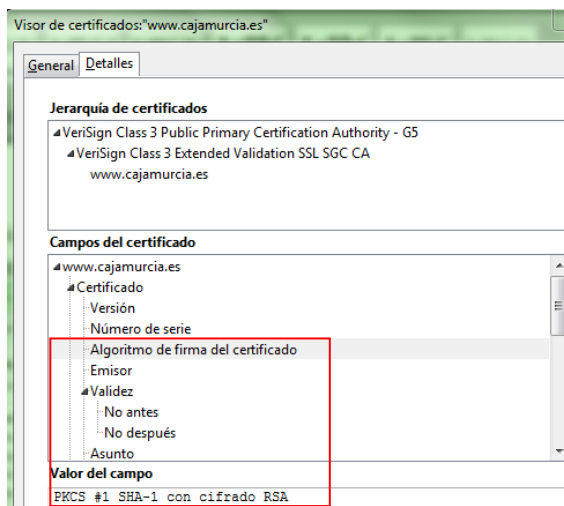
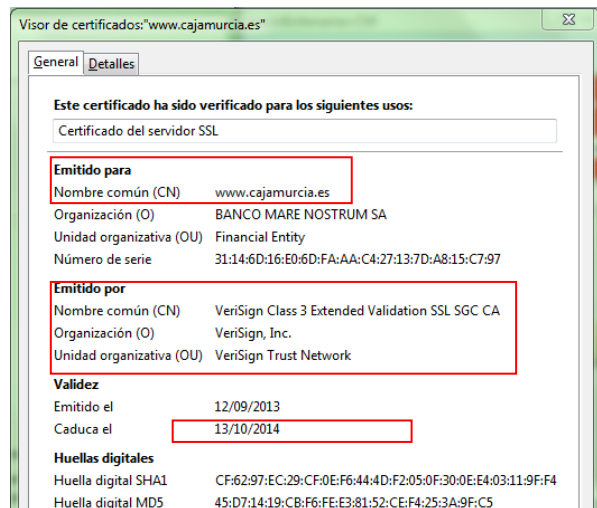
**Servidores Web, Certificados seguros para
HTTPS, capa SSL y Sistemas Gestores de
Contenido**

Antonio José Miñarro Miñarro
2º ASIR – SRI y IAW

Actividades con los navegadores (clientes)

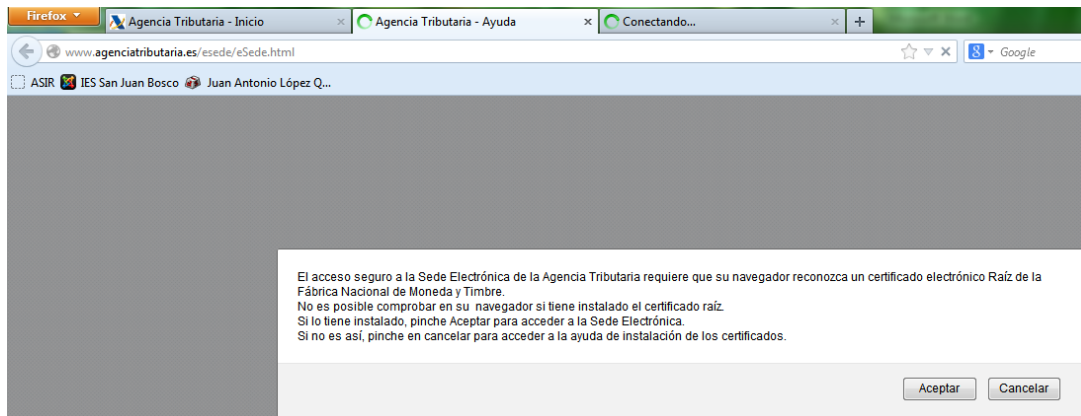
1. Visita una Web que utilice HTTPS y comprueba los siguientes datos: Para quién se emitió el certificado, CA, algoritmo, fecha de caducidad y clave pública. Entregar datos obtenidos y pantallas de capturas

La web visitada es la de Caja Murcia con el navegador cliente Google Chrome (<https://www.cajamurcia.es>). Como vemos a la izquierda de la URI, en la barra de direcciones podemos acceder a la información sobre el certificado que está usando este sitio. Comprobamos que usa certificado por el uso del protocolo HTTP sobre SSL (https://) y por el icono verde de un candado. Accedemos como se muestra en la primera captura y comprobamos los datos necesarios (Capturas 2, 3 y 4)




2. Instala el certificado de una Web segura, visita la Web y comprueba que no vuelve a pedirte autorización, borra el certificado y visítala de nuevo. (Windows y Linux). Entregar paso a paso y pantallas de capturas.

En esta ocasión vamos a acceder desde el navegador cliente Mozilla Firefox, porque al parecer Google Chrome instala de manera predeterminada este certificado sin pedirnos confirmación. Para ellos hemos visitado la web de la Agencia Tributaria (www.agenciatributaria.es). Como se ve en esta primera captura, el sitio web nos muestra un mensaje requiriendo la instalación del certificado electrónico Raíz, reconocido por la FNMT, lo que confirma la veracidad del sitio que estamos visitando. La práctica es idéntica en un cliente Mozilla Firefox de Windows que en otro de Linux, por lo que se omiten las capturas y explicación



Si clicamos aceptar intentaremos acceder a la web sin instalar el certificado, por lo que tendremos el siguiente mensaje de advertencia:



Esta conexión no está verificada

Ha pedido a Firefox que se conecte de forma segura a www.agenciatributaria.gob.es, pero no se puede confirmar que la conexión sea segura.

Normalmente, cuando se intenta conectar de forma segura, los sitios presentan información verificada para asegurar que está en el sitio correcto. Sin embargo, la identidad de este sitio no puede ser verificada.

¿Qué debería hacer?

Si normalmente accede a este sitio sin problemas, este error puede estar ocurriendo porque alguien está intentando suplantar al sitio, y no debería continuar.

▼ Detalles técnicos

www.agenciatributaria.gob.es usa un certificado de seguridad no válido.

No se confía en el certificado porque el certificado emisor es desconocido.

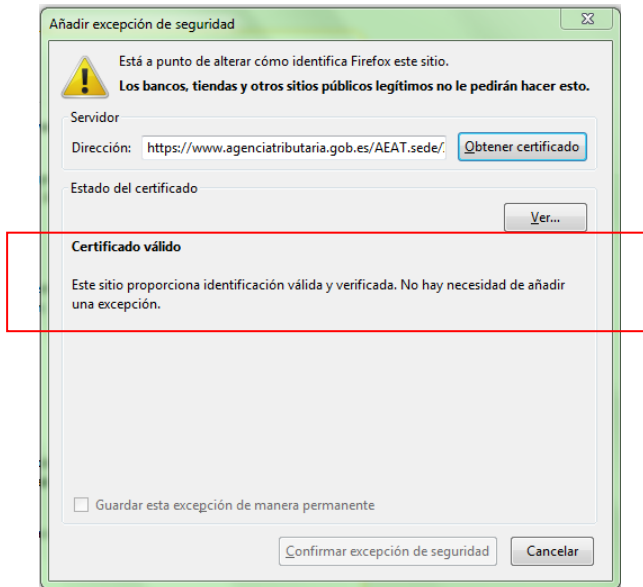
(Código de error: sec_error_unknown_issuer)

▼ Entiendo los riesgos

Si sabe lo que está haciendo, puede obligar a Firefox a confiar en la identificación de este sitio. **Incluso aunque confie en este sitio, este error puede significar que alguien esté interfiriendo en su conexión.**

No añada una excepción a menos que sepa que hay una razón seria por la que este sitio no use identificación confiable.

Si intentásemos añadir una excepción para que Firefox accediera aun no teniendo el certificado, no sería posible, al menos para este sitio, ya que como indica el mensaje:



Si clicásemos en Cancelar obtendríamos una página con las instrucciones para descargar e instalar los certificados necesarios. Seguimos las sencillas instrucciones:

Para acceder correctamente a la Sede Electrónica de la Agencia Tributaria es necesario que descargue e instale los siguientes certificados (certificado raíz y certificado de sede electrónica) emitid Debe descargar los archivos .CER que se corresponden con cada uno de los dos certificados electrónicos necesarios, "AC RAIZ FNMT-RCM" y "AC APE" e instalarlos en el orden que le indicamo (Si lo desea, puede consultar más información al respecto en la página web de la FNMT).

Paso 1: Descarga e instalación del certificado raíz de la FNMT (AC RAIZ FNMT-RCM)

Pulse sobre el botón "Descargar certificado". Aparecerá una ventana solicitando que confíe en una nueva Autoridad Certificadora. Marque las 3 casillas "Confíar en..." y haga clic en "Aceptar". Por último, acepte las siguientes ventanas del navegador.

Descargar certificado

A continuación dispone de una serie de capturas de pantalla que pueden servirle de indicación para seguir el proceso arriba descrito (pase el ratón por encima para ver la imagen ampliada).

Ministerio de Hacienda y Administraciones Públicas | Fiscalidad Autónoma y Local | Fiscalidad No Residentes | Enlaces de Interés

Agencia Tributaria

Ayuda

Inicio > Ayuda en Línea > Información y Requisitos

Para acceder correctamente a la Sede Electrónica de la Agencia Tributaria, debe descargar los archivos .CER que se corresponden con cada navegador. (Si lo desea, puede consultar más información al respecto en la página de Ayuda).

Paso 1: Descarga e instalación del certificado raíz de la Sede Electrónica de la Agencia Tributaria.

Pulse sobre el botón "Descargar certificado". Aparecerá una ventana solicitando que confíe en una nueva Autoridad Certificadora (CA). Por último, acepte las siguientes ventanas del navegador.

Descargar certificado

A continuación dispone de una serie de capturas de pantalla que pueden servirle de indicación para seguir el proceso arriba descrito (pase el ratón por encima para ver la imagen ampliada).

Pulse el botón "Continuar" de esta página para seguir con la instalación del certificado de sede electrónica.

Continuar

Pulse el botón "Continuar" de esta página para seguir con la instalación del certificado de sede electrónica.

Continuar

Paso 2: Descarga e instalación del certificado de la subsele (AC APE)

El procedimiento de descarga e importación es similar al del certificado raíz.

Pulse sobre el botón "Descargar certificado". Aparecerá una ventana solicitando que confíe en una nueva Autoridad Certificadora. Marque las 3 casillas "Confíar en..." y haga clic en "Aceptar".

Descargar certificado

A continuación dispone de una serie de capturas de pantalla que pueden servirle de indicación para seguir el proceso arriba descrito (pase el ratón por encima para ver la imagen ampliada).

Paso 3: Instalación finalizada.

Si ha seguido las indicaciones paso a paso, ya tiene correctamente configurado su navegador para acceder a la nueva Sede Electrónica de la Agencia Tributaria. Pinche aquí para acceder a la sede electrónica.

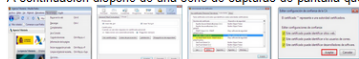
Puede comprobar que los certificados están correctamente instalados si accede al menú de Firefox, "Herramientas", "Opciones", "Avanzado", y selecciona la pestaña "Cifrado". Haga clic en "Ver certificados" y seleccione "Autoridades".

Localice la autoridad "FNMT-RCM" en el listado, marque AC RAIZ FNMT-RCM y haga clic en el botón "Editar". Verifique que las 3 casillas de la ventana "Editar configuración de confianza de la CA" están marcadas. Pulse "Aceptar".

A continuación seleccione AC-APE FNMT-RCM y realice la misma comprobación. Haga clic en el botón "Editar". Verifique que las 3 casillas de la ventana "Editar configuración de confianza de la CA" están marcadas. Pulse "Aceptar".

Si los certificados están instalados en la pestaña "Autoridades" y las casillas indicadas están activadas su configuración es correcta.

A continuación dispone de una serie de capturas de pantalla que pueden servirle de indicación para seguir el proceso arriba descrito (pase el ratón por encima para ver la imagen ampliada).



Tras la instalación podemos comprobar en el Administrador de certificados de Firefox como todo está correctamente instalado:

Administrador de certificados

Sus certificados | Personas | Servidores | Autoridades | Otros

Tiene certificados en archivo que identifican estas autoridades certificadoras:

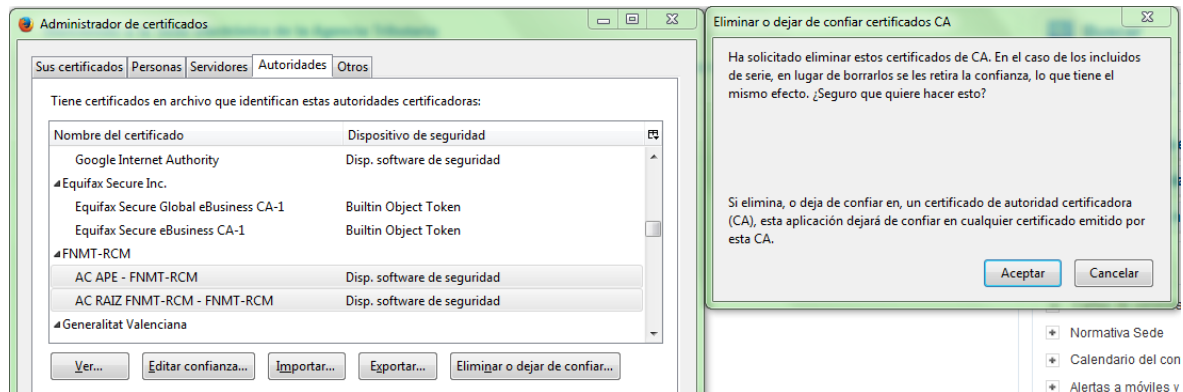
Nombre del certificado	Dispositivo de seguridad
Equipax Secure eBusiness CA-1	Builtin Object Token
▲ FNMT-RCM	
AC APE - FNMT-RCM	Disp. software de seguridad
AC RAIZ FNMT-RCM - FNMT-RCM	Disp. software de seguridad
▲ Generalitat Valenciana	
Root CA Generalitat Valenciana	Builtin Object Token
▲ GeoTrust Inc.	
GeoTrust Global CA	Builtin Object Token

Ver... | Editar confianza... | Importar... | Exportar... | Eliminar o dejar de confiar... | Aceptar

Y ya podemos acceder a la web de la Agencia Tributaria de manera segura mediante https, sin el mensaje que nos aparecía antes para instalar certificados:

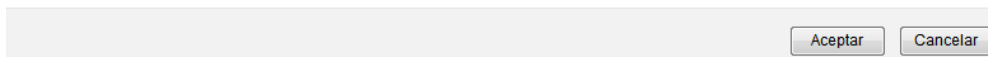


Ahora desde el Administrador de certificados forzamos la eliminación de los certificados que hemos instalado:



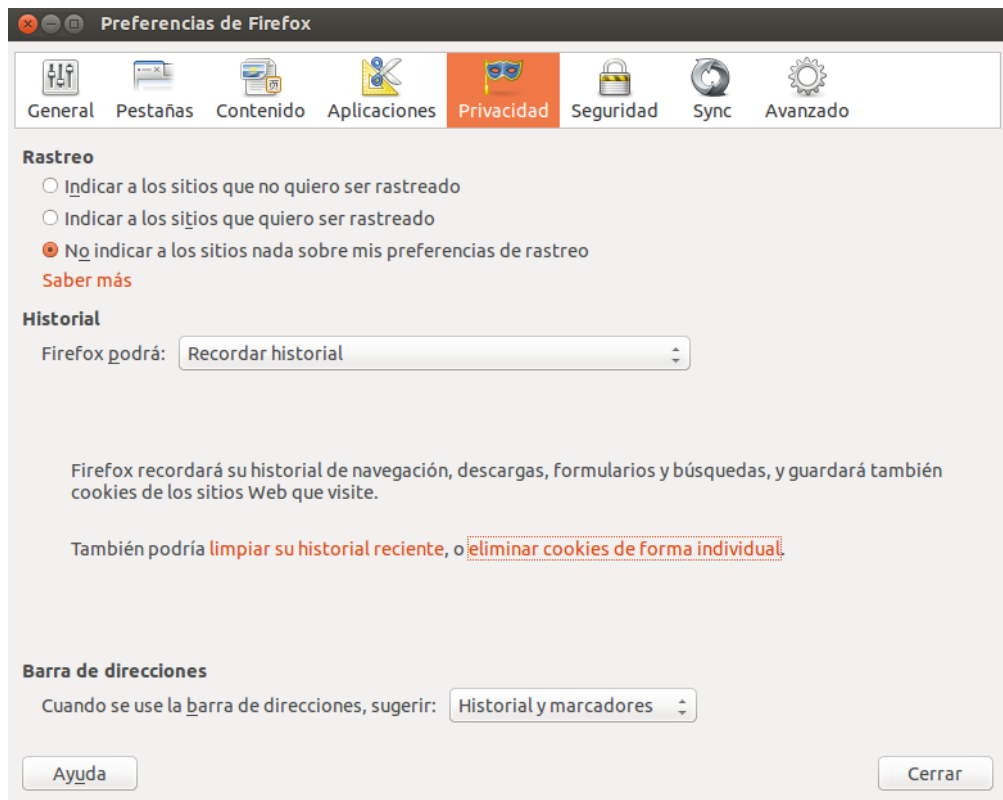
Y cuando volvemos a visitar el sitio de nuevo, vuelve a aparecer el mensaje anterior:

El acceso seguro a la Sede Electrónica de la Agencia Tributaria requiere que su navegador reconozca un certificado electrónico Raíz de la Fábrica Nacional de Moneda y Timbre.
 No es posible comprobar en su navegador si tiene instalado el certificado raíz.
 Si lo tiene instalado, pinche Aceptar para acceder a la Sede Electrónica.
 Si no es así, pinche en cancelar para acceder a la ayuda de instalación de los certificados.

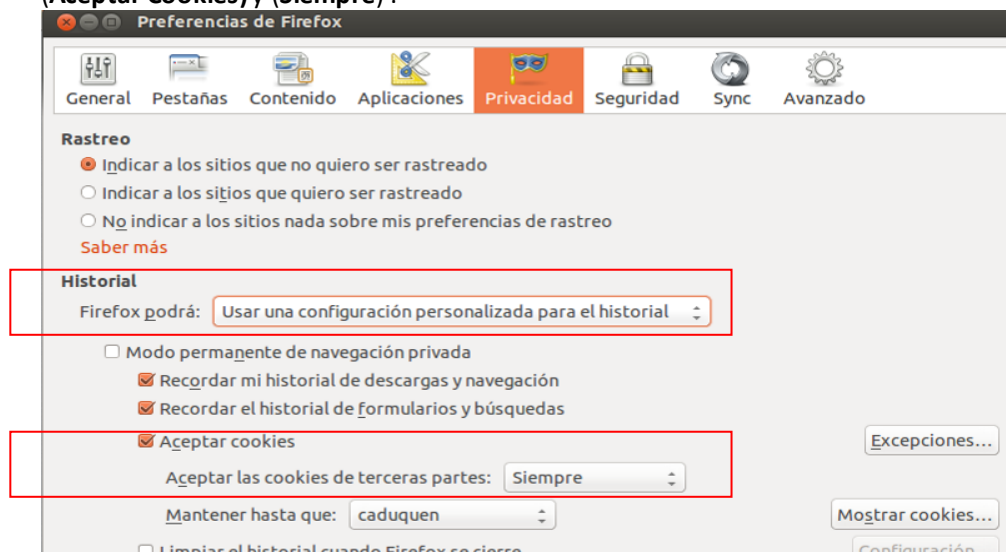


3. Configura el navegador para que acepte todas las cookies, navega unos minutos por tus Web favoritas y consulta las cookies que se han guardado en tu equipo. Una vez comprobadas bórralas para no dejar rastros de tu uso de internet y configura el navegador a su estado anterior. Entrega listado de cookies y pasos realizados.

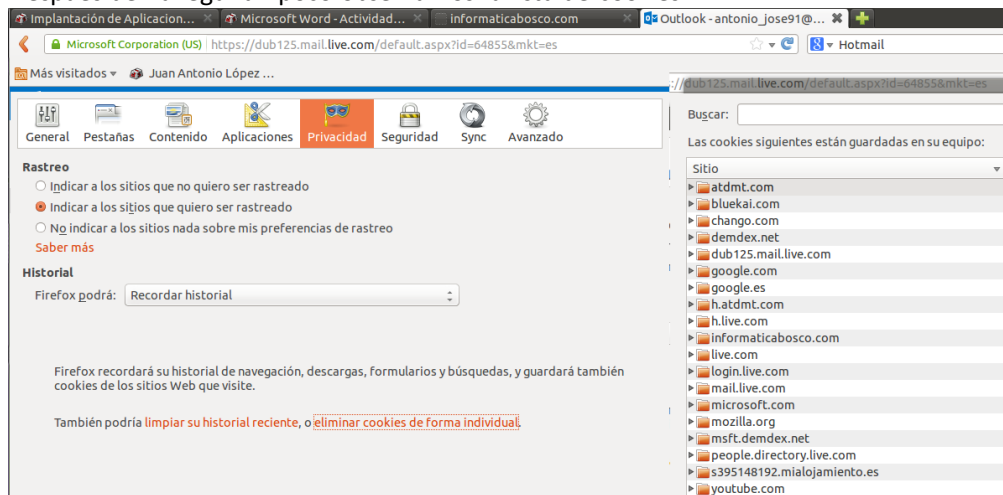
En las preferencias de Mozilla Firefox encontramos la pestaña Privacidad. Allí podemos ver, en la opción que aparece abajo (eliminar cookies de forma individual), el listado de las cookies almacenadas por el navegador.



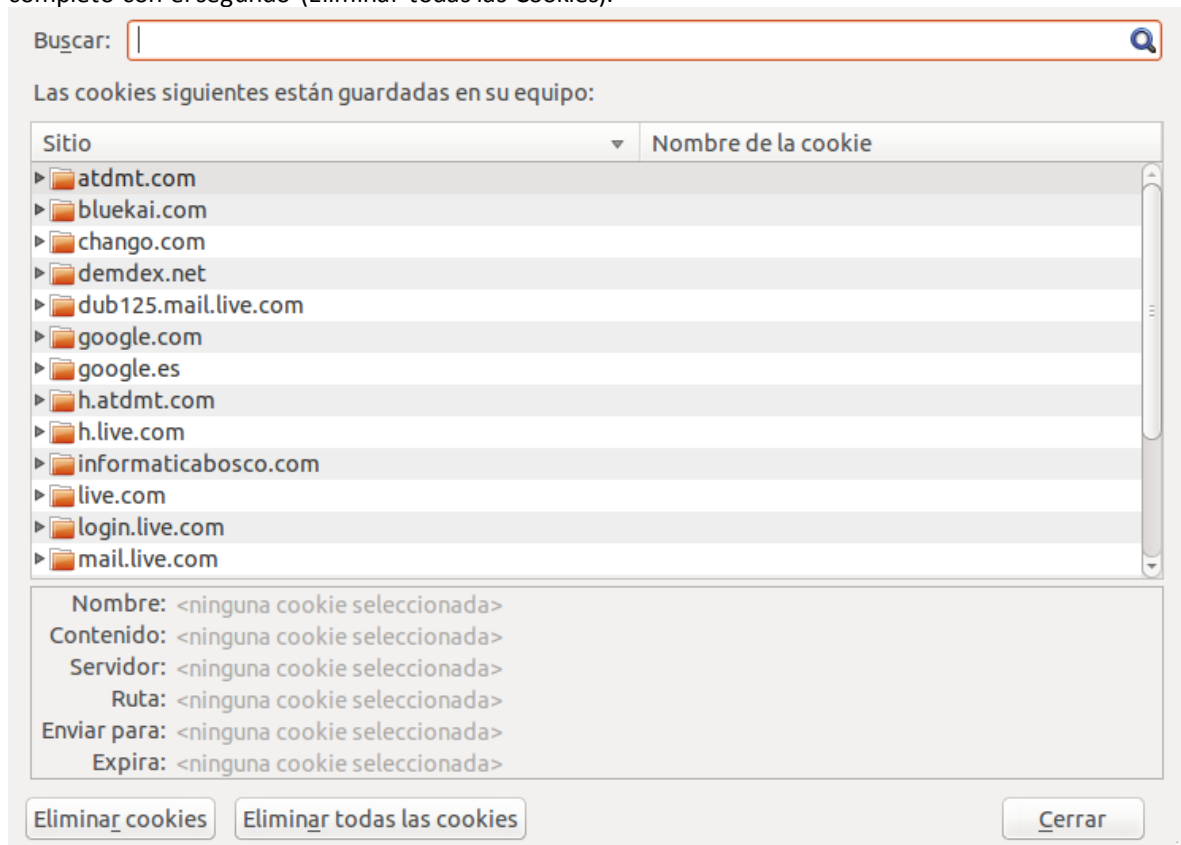
Si queremos configurar el navegador para que se guarden todas las Cookies tenemos que cambiar a la siguiente opción (**Firefox podrá: Usar una configuración personalizada para el historial**) y (**Aceptar Cookies**) y (**Siempre**) :



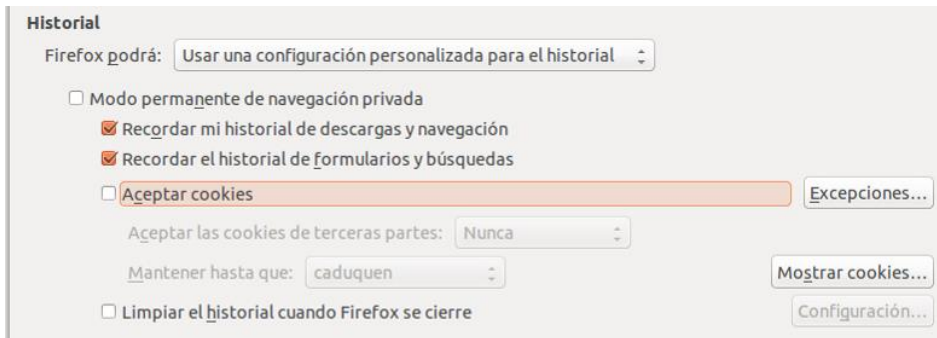
Después de navegar un poco observamos la lista de cookies:



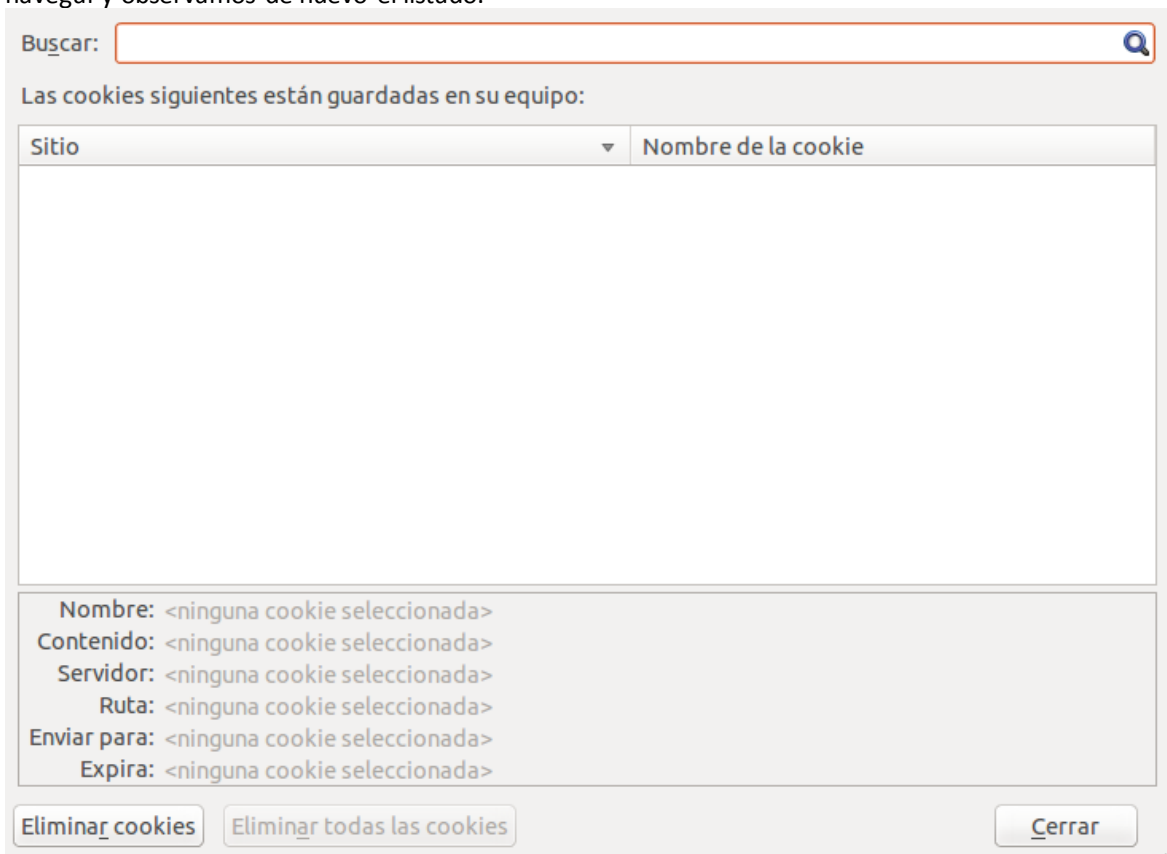
Para eliminar las Cookies accedemos al apartado en el que antes hemos consultado las Cookies y podemos eliminarlas de manera individual, con el primer botón (Eliminar Cookies) o todas por completo con el segundo (Eliminar todas las Cookies).



Y si queremos que no se guarden Cookies de los sitios que visitamos tendremos que desmarcar la siguiente opción, desde las preferencias de Firefox, pestaña privacidad:



Una vez borrado el historial de Cookies y desactivada la opción de aceptar Cookies volvemos a navegar y observamos de nuevo el listado:



Eso sí, algunas webs requieren el uso de Cookies, como Hotmail:

