Universitat de les Illes Balears

escola politècnica superior

Treball Final de Grau

Análisis de Seguridad de las "*Cookies*"

Miguel Agustín Pérez Moya

Departamento

CIENCIAS MATEMÁTICAS E INFORMÁTICA

Tutor

Pep Lluís Ferrer Gomila

Grado

Ingeniería Telemática

Escuela Politécnica Superior

Universidad de las Islas Baleares

Palma, 1 de septiembre de 2016

ÍNDICE

LISTADO DE FIGURAS

LISTADO DE ACRÓNIMOS

ICO - *Information Commission Office*.

IETF - *Internet Engineering Task Force*.

IP - *Internet Protocol*.

http - *Hypertext Transfer Protocol*.

HTTPS - *Hypertext Transfer Protocol Secure*.

P3P - *Platform for Privacy Preferences*.

RFC - *Request For Comments*.

TCP - *Transmission Control Protocol*.

OSI - *Open System Interconnection*.

URL - *Uniform Resource Locator*.

WWW - *World Wide Web*.

RESUMEN

El protocolo HTTP permite proporcionar servicios a los usuarios de los sitios *web*, pero puede requerir de las denominadas "*Cookies*" para permitir las transacciones de información utilizando el mencionado protocolo. No se conserva información de estado al utilizar el protocolo HTTP, lo cual dificulta el comercio electrónico a través de la *web*. Las *cookies* son necesarias ya que sin su uso no sería posible la transacciones realizadas en el ámbito del comercio electrónico, pero su utilización también puede conllevar problemas de seguridad sobre todo en relación a la privacidad de los usuarios.

Este trabajo tiene como primer objetivo exponer el motivo por el cual las *cookies* son necesarias para proporcionar servicios por parte de determinados sitios *web*. Adicionalmente se expondrán las utilidades que nos proporciona el uso de las *cookies*, así como la estructura e información que contienen. Por otro lado, se mostrará el método utilizado para su uso, y se definirán los tipos de *cookies* que son utilizadas actualmente.

A continuación se procederá a describir las implicaciones que tiene el uso de *cookies*, sobre todo en relación a la privacidad de los usuarios que visitan sitios *web* que requieren el uso de *cookies*. También se explicarán los problemas que implican el uso de las *cookies* y las posibles alternativas existentes.

La creciente preocupación de los usuarios de Internet en relación al uso de las *cookies* y la implicación que estas puede tener respecto de la privacidad de los usuario, ha provocado que diversos organismos mundiales, entre ellos la Unión Europea, hayan desarrollado una normativa de aplicación obligatoria dentro de su área de acción con el fin de proteger la privacidad de sus ciudadanos al usar servicios de sitios *web* que usen *cookies*.

La última parte del trabajo tiene por objetivo analizar el tratamiento que tres navegadores diferentes realizan a las *cookies* a partir de las opciones de configuración que pueden seleccionar los usuarios. A partir de una opción de configuración se analizará el comportamiento del navegador al visitar varios sitios *web* que proporcionan diferentes servicios a los usuarios. Finalmente a partir de los resultados se realizarán unas recomendaciones al usuario respecto de la configuración óptima del navegador de forma que salvaguarden al máximo la privacidad de estos.

1. INTRODUCCIÓN

1.1 Introducción

Internet es un conjunto de redes de comunicación interconectadas que permiten el intercambio de mensajes mediante la utilización de la pila de protocolos TCP (*Transmission Control Protocol*)/IP (*Internet Protocol*).

La utilización de este medio de comunicación supuso un cambio radical en los hábitos de millones de personas del planeta. La interconexión de redes de telecomunicaciones y la diversidad de dispositivos disponibles que hoy en día pueden conectarse fácilmente a Internet, han proporcionado nuevos servicios que han facilitado el acceso a la información y servicios a los usuarios. Este acceso permite el intercambio de información de forma mucho más rápida y eficiente entre dispositivos muy distanciados físicamente.

Uno de los servicios más importantes que se proporciona a los usuarios como consecuencia del desarrollo de Internet es la *web,* que en su origen permitía la consulta remota de archivos de hipertexto mediante la utilización del protocolo HTTP.

HTTP es un protocolo que no conserva información de estado, lo cual significa que una vez que un sitio *web* ha contestado una petición de un cliente, el servidor cierra la conexión sin almacenar ninguna información del cliente. Este hecho proporciona una ventaja y es que los sitios *web* no necesitan retener información sobre los clientes entre peticiones y ha permitido el desarrollo de servidores *web* que gestionen miles de conexiones TCP simultáneamente. Sin embargo, hoy en día muchas aplicaciones *web* requieren que se mantenga información sobre el estado del usuario, por lo tanto ha sido necesario establecer otros métodos que permitan simultáneamente la utilización del protocolo HTTP y el almacenamiento de información de estado en el ordenador del cliente. El mecanismo más habitual que permite la utilización del protocolo HTTP manteniendo la información de estado son las *cookies*.

El primer documento que formalizó las especificaciones que debían cumplir las *cookies* fue el RFC 2109 emitido en febrero de 1997. Unos años más tarde se emitió un nuevo documento, el RFC 2965, que hacía obsoleto el RFC emitido anteriormente. Por último, en abril de 2011 se emitió el RFC 6265 el cual está categorizado por IETF como "*Internet Standards Track document*", por ser un documento que posee un alto grado de madurez técnica.

El objetivo inicial de las *cookies* era permitir la implementación de los carros de compra virtuales. En las primeras implementaciones, las *cookies* eran aceptadas por defecto y por tanto eran guardadas en los ordenadores de los clientes sin que estos fueran conscientes de que una pequeña cantidad de información había sido guardada por un sitio *web* a través del navegador. En el momento que se empezó a dar a conocer la utilización de *cookies* por parte de los sitios *web*, se despertó un interés mediático debido a las posibles implicaciones relativas a cuestiones de privacidad.

La mayor controversia en torno a la utilización de las *cookies* es debida a que mediante su uso se puede permitir el rastreo de los hábitos de navegación de los usuarios, creando perfiles de usuario cuyo interés está basado en fines comerciales y que pueden considerarse como una intrusión en la privacidad de los usuarios. De hecho, el RFC 6265 reconoce las implicaciones relativas a la seguridad y dice textualmente: "Aunque las *cookies* han tenido históricamente muchos infortunios que degradan su seguridad y privacidad, los campos de las cabeceras *Cookie* y *Set-Cookie* son ampliamente usados en Internet."

Actualmente, los sitios *web* ubicados dentro de la Unión Europea están obligados según la normativa actual vigente a mostrar al usuario cuál es la política que aplica en relación al uso de las *cookies*.

El uso de las *cookies* no es el único mecanismo a partir del cual se puede obtener información relacionada con la privacidad de los usuarios, ya que hoy en día debido a los adelantos tecnológicos, incluso sin el uso de las temidas *cookies*, es posible espiar a los usuarios

creando un perfil de los intereses y actividades de estos mediante la llamada “huella digital”. Esta técnica parte del hecho que cada usuario normalmente usa su propio dispositivo, lo cual implica una relación directa entre el dispositivo y la persona que lo utiliza y permite rastrear los hábitos de navegación, las revelaciones realizadas en redes sociales, registros de compra, movimientos y rutinas a través de los teléfonos móviles, con el fin de permitir clasificar los usuarios con diferentes fines como puedan ser comerciales o sociales.

1.2 Agradecimientos

El presente trabajo de final de grado fue realizado bajo la supervisión del Dr. Pep Lluís Ferrer Gomila, a quien me gustaría expresar mi agradecimiento, por hacer posible la realización del presente trabajo. Además de agradecer su tiempo y dedicación que tuvo para que este trabajo saliera de forma exitosa.

A todos los profesores que tuve durante el grado, ya que gracias a ellos obtuve los conocimientos adquiridos durante estos años.

A todos mis compañeros, en especial a Jordi Ballester y Ángel Torres ya que sin ellos y su ayuda no hubiese sido posible llegar hasta aquí.

A mi familia, por los sacrificios realizados y que han contribuido a la obtención de mi Grado.

A mi padre, por estar presente en mi memoria y ayudarme a finalizar lo que empecé hace muchos años.

A todos vosotros, mi mayor reconocimiento y gratitud.

2. FUNDAMENTOS DE LAS *COOKIES*

2.1 ¿Qué es una *cookie*?

La palabra *Cookie* viene de "*Magic Cookie*" y es una pequeña información que es creada por el servidor *web*, contiene información del cliente, por ejemplo: nombre, identificador de usuario, contenido carrito de compra, información personal, etc; y que es guardada por el navegador en el ordenador del cliente. La *cookie* es transmitida como parte de la información contenida en una cabecera HTTP. El navegador no modificará el valor de la *cookie* y la incluirá en las peticiones que realice al sitio *web* que la creó. Este al recibir una petición que contenga una *cookie* sabrá que el cliente no es un cliente nuevo sino que ya le ha realizado una petición con anterioridad.

La *cookie* contiene cualquier dato que el servidor quiere transmitir al cliente pero con una limitación debido al tamaño máximo que puede tener la *cookie*. Por otro lado, de acuerdo al RFC 6265, los navegadores deben tener una capacidad mínima de almacenamiento de 4096 bytes por *cookie*.

Una *cookie* no identifica un usuario sino que identifica la relación computador-navegador-usuario. Por tanto, un navegador guardará todas las *cookies* de los diferentes usuarios en el computador que han utilizado ese navegador para navegar. El espacio que el navegador dispone para guardar *cookies* está limitado, aunque las especificaciones definidas en el RFC 6265 indican que el navegador debe tener capacidad para almacenar al menos 50 *cookies* por dominio y 3000 *cookies* en total.

El hecho de no utilizar *cookies* implica que cada petición que se realice a un sitio *web* es una evento aislado, ya que como hemos explicado, HTTP es un protocolo que no conserva información de estado, y por tanto una petición es totalmente independiente de la posterior y la anterior. Sin embargo, el hecho de utilizar las *cookies* permite al servidor *web* relacionar una petición con otras peticiones. Así, las *cookies* se podrían considerar como un mecanismo que permite la creación de sesiones HTTP con información de estado.

Algunos sitios *web* utilizan el mecanismo de las *cookies* para proporcionar diversos servicios a los usuarios, como por ejemplo, facilitar la navegación de estos a través del sitio, personalizar la información que se muestra al usuario, permitir realizar compras *online* más ágiles, etc. Otros sitios *web* utilizan la capacidad que proporcionan las *cookies* de recopilar información para diversos fines, como por ejemplo, el análisis de información demográfica o la creación de perfiles de usuarios, entre otros.

2.2 ¿Para qué sirve una *cookie*?

Las *cookies* son utilizadas con diferentes fines, como hemos comentado anteriormente, pero principalmente las *cookies* son utilizadas para proporcionar información de estado entre peticiones HTTP, aunque también ayudan a lo usuarios a navegar eficientemente y realizar ciertas funciones. A continuación se relacionan una serie de utilidades de las *cookies*.

1.- Carrito de compras virtual

La utilización de *cookies* permite al cliente navegar por el sitio *web* (tienda electrónica), seleccionar productos que serán añadidos o eliminados del carrito de compra y finalmente pagar con una tarjeta de crédito. El intercambio de mensajes entre el cliente y el sitio *web* permite actualizar el contenido del carrito. Cuando el cliente finaliza la compra y desea pagar, se recupera la *cookie* para poder calcular el precio total de la compra y poder proceder con el pago. El hecho de no utilizar una *cookie*, en este caso, implicaría que el cliente debería comprar cada producto individualmente introduciendo los mismos datos tantas veces como productos quisiera adquirir.

2.- Identificación y autenticación del cliente

Las *cookies* son utilizadas por numerosos sitios *web* como mecanismo de reconocimiento del cliente, de forma que se evita que este deba introducir sus credenciales (usuario y contraseña) cada vez que realice una petición al sitio *web*. Este ahorro que evita la introducción de las credenciales con cada petición, facilita la navegación al usuario y permite una mayor velocidad de respuesta a las peticiones. Adicionalmente, las *cookies* permiten a los clientes registrados acceder a servicios que proporciona el sitio *web* y que no son accesibles a clientes no registrados, por tanto, se utiliza la *cookie* como mecanismo que restringe el acceso a clientes autorizados.

3.- Personalización de las preferencias del usuario (portal *web*)

Algunos sitios *web* facultan al cliente para definir cuales son sus preferencias. En estos casos, las *cookies* permitirán al sitio *web* recordar cuáles son las preferencias del usuario y por tanto, una vez que un cliente se identifique, el sitio *web* personalizará las respuestas que se proporcione al cliente.

4.- Seguimiento de clientes

Un sitio *web* puede registrar todas las peticiones realizadas por un cliente de forma que el sitio puede aprender cuáles son los intereses del cliente. Por ejemplo, pueden quedar registradas todas las compras de un cliente determinado de forma que el propietario del sitio *web* puede conocer cuál es el interés o los hábitos de consumo de este.

5.- Perfiles de usuario

Existen sitios *web* que mediante la utilización de las llamadas "*cookies* de terceros" pueden crear perfiles de usuario más amplios, los cuales se pueden obtener mediante el rastreo de los clientes a través de varios sitios *web*. Esta opción es muy utilizada por empresas de publicidad, ya que tras el análisis de los sitios visitados por un cliente, se le puede ofrecer a través de anuncios, productos que pueden ser de su interés.

6.- Análisis de un sitio *web*

A partir del análisis de las actividades de los clientes en un sitio *web* se pueden obtener estadísticas de uso del sitio. Esta información puede ser muy relevante para los gestores de los sitios *web,* ya que pueden conocer cuáles son los intereses de los visitantes así como cuáles son las páginas que no son visitadas por estos. A partir de esta información los gestores pueden modificar los sitios *web* de forma que se adapten mejor a la necesidades de los clientes y por tanto sean más eficientes. El análisis de un sitio *web* es una herramienta que permite al propietario modificar y adaptar el contenido del sitio a los intereses de los clientes.

7.- Evitar ataques masivos por peticiones SYN al servidor

Existen varías técnicas cuya finalidad es evitar ataques masivos por peticiones SYN al servidor, como por ejemplo, limitar el número de peticiones que el servidor puede gestionar, no asignar recursos para atender peticiones de dirección IP desconocidas o no asignar recursos hasta que el servidor no reciba una *cookie* desde el cliente.

A continuación se procede a explicar en qué consiste la técnica en la cual el servidor no asigna recursos hasta que no reciba una *cookie*. TCP es un protocolo de capa de transporte orientado a conexión. El establecimiento de la conexión TCP entre un cliente y un servidor se realiza mediante el proceso de acuerdo en tres pasos (*three-way handshake*). Los tres pasos de la fase de establecimiento de la conexión son los siguientes:

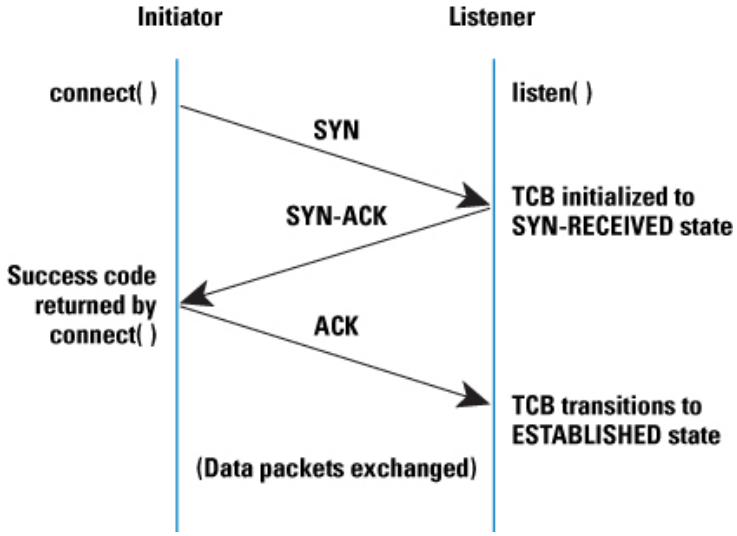

Figura 1 – Intercambio mensajes conexión TCP

1.- El cliente inicia la comunicación mediante el envío de un mensaje SYN, por tanto realiza una apertura activa.

2.- A continuación el servidor al recibir el mensaje SYN asigna recursos a la conexión (inicialización de buffers y variables) y envía un mensaje SYN-ACK hacia el cliente.

3.- Una vez que el cliente recibe el mensaje SYN-ACK contesta al servidor con un mensaje ACK y el servidor al recibir este último mensaje da por establecida la conexión. En el caso de que el cliente no envíe el mensaje ACK transcurrido un tiempo, el servidor procederá a liberar los recursos reservados.

El ataque masivo por peticiones SYN se basa en el envío masivo de peticiones a un servidor, el cual reservará recursos para cada uno de los mensajes SYN que recibe sin que los clientes completen el establecimiento de conexión al no enviar el mensaje ACK. Si el servidor recibe un gran número de peticiones en un breve espacio de tiempo este se puede quedar sin recursos y por tanto, denegará el servicio que sea solicitado por otros clientes no atacantes.

Una estrategia para combatir este tipo de ataque es mediante la utilización de las llamadas *cookies* SYN, y la no asignación de recursos a una conexión hasta que el servidor obtenga la *cookie* SYN enviada por el cliente, y este verifique que el ACK recibido corresponde a un cliente legítimo y no un atacante.

La *cookie* SYN corresponde con un número de secuencia inicial TCP creada por el servidor mediante una función de hash a la dirección IP origen, dirección IP destino, los puertos que intervienen en la comunicación y un valor secreto. El valor de SYN-ACK que enviará el servidor hacia el cliente corresponderá a la *cookie* SYN creada. Esta información no debe ser guardada por el servidor.

El cliente al recibir el mensaje SYN-ACK responderá con un mensaje ACK y el servidor al recibir el mensaje ACK calculará el valor de SYN-ACK utilizando la misma función hash y con los mismos elementos que se utilizaron para calcular la *cookie* SYN. Si el valor ACK es igual al valor de SYN-ACK más uno, el servidor habrá verificado que el cliente no es un atacante, asignará los recursos necesarios y abrirá una conexión. Sin embargo, si el cliente no envía el mensaje ACK, no provocará ningún daño al servidor ya que no han sido asignado recursos para la conexión.

2.3 Contenido de las *cookies*

Una *cookie* se compone de los siguientes atributos de acuerdo a la última especificación definida en el RFC: nombre, caducidad, edad máxima, ruta, dominio, seguridad y HttpOnly. A continuación se explica el significado de cada uno de ellos.

Nombre: Este campo identifica el nombre de la *cookie* asignado por el servidor.

Caducidad: Este campo es introducido por el servidor e indica cuando caduca la *cookie*. El navegador del cliente borrará la *cookie* en el momento en que esta haya caducado.

Las *cookies* de sesión no poseen campo de caducidad e implica que la *cookie* será borrada del directorio del navegador una vez el cliente haya cerrado la sesión.

Las *cookies* persistentes tienen fecha de caducidad y amplían el periodo de validez hasta que estas expiran. Al cliente puede no interesarle que el periodo de validez de la *cookies* sea muy grande para evitar problemas de seguridad, pero el cliente no puede modificar este valor ya que es determinado por el servidor.

Edad Máxima (Max-Age attribute): Este atributo determina el tiempo en segundos otorgado antes de que la *cookie* sea eliminada. Este atributo no es muy utilizado y en el caso de que no sea soportado por parte del navegador será ignorado.

Ruta: El alcance de cada *cookie* está limitado por un conjunto de rutas controladas por el atributo Ruta. Este campo indica la estructura del directorio del servidor y definirá qué partes del archivo del servidor puede utilizar la *cookie*.

Dominio: El atributo Dominio indica la dirección del servidor de la cual procede la *cookie*. Si no se indica explícitamente este campo en la *cookie*, indica por defecto el servidor que envió la *cookie* y por tanto, si se realiza una petición se enviará sólo al servidor de origen. Este campo es importante porque define que conjunto de servidores pueden recibir la *cookie* al realizar peticiones. De acuerdo a la especificación, las *cookies* sólo pueden ser asignadas y leídas por el dominio en el que están activas.

Seguridad: La marcación de una *cookie* con la bandera de seguridad implica que la transmisión de esta debe realizarse sólo mediante una conexión segura. Normalmente HTTPS es el protocolo utilizado en estos casos y su funcionamiento está basado en el protocolo HTTP pero añade seguridad.

HTTPS es utilizado normalmente cuando se solicita un servicio a un sitio y este requiere que exista una transferencia de datos personales y/o contraseñas entre el cliente y el sitio. La técnica utilizada para enviar esta información de forma segura se basa en utilizar el cifrado (SSL/TLS) para crear un canal que garantice que la información transferida no pueda ser utilizada por un atacante. El nivel de protección de la comunicación dependerá de los algoritmos de cifrado utilizados, la implementación del navegador y el *software* utilizado en el servidor *web*. Esta técnica nos protege de que la *cookie* sea descubierta por un atacante, y por tanto nos proporciona *confidencialidad*, pero no protege la *cookie* de ser interceptada cuando está almacenada en el directorio del navegador.

HttpOnly: Este atributo limita el alcance de la *cookie* a peticiones HTTP.

2.4 ¿Cómo son usadas las *cookies*?

El mecanismo de funcionamiento de las *cookies* es siempre el mismo independientemente de la implementación que se realice para crearlas y almacenarlas.

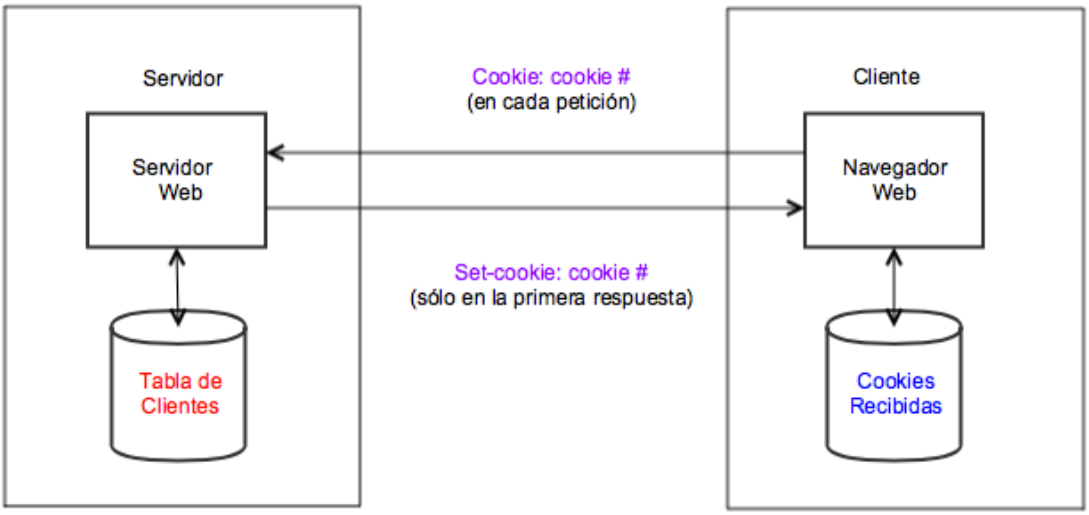

Figura 2 – Intercambio de *cookies* entre cliente y servidor

El primer paso es realizado por el cliente, el cual realiza una petición a un sitio *web* al clicar sobre un enlace en el navegador *web*. El sitio *web* comprobará si la petición incluye alguna *cookie*, y en caso de que la contenga comprobará el valor. Si coincide con el valor guardado por el sitio *web*, este entenderá que el cliente no es la primera vez que visita este sitio. En el caso de que la *cookie* recibida no coincida con los valores de ninguna *cookie* almacenada, el sitio procederá a ignorarla.

En el caso de que la petición no contenga ninguna *cookie* será interpretado por el sitio *web* como que es la primera vez que el cliente visita ese sitio. En este caso, el sitio *web* guarda la información del cliente, por ejemplo nombre, número de registro, marca de tiempo y otra información, junto con el valor de la *cookie* asociada que creará en ese momento. En el siguiente paso, el sitio *web* envía la respuesta al cliente junto con la *cookie* que ha creado. A continuación cuando el cliente recibe la respuesta del sitio *web*, recibirá la *cookie* y el navegador *web* del cliente la guardará en un directorio de *cookies* en el disco duro. En el momento en el que el navegador recibe la respuesta se desconecta del sitio *web*.

Una vez guardada la *cookie* y mientras que esta sea válida, el navegador *web* adjuntará la *cookie* junto a las peticiones realizadas por el cliente siempre y cuando la petición cumpla con las especificaciones de validez definida en la *cookie.* Por tanto, cuando el cliente realiza una petición a un sitio *web*, el navegador buscará en el directorio de *cookies* si hay alguna *cookie* almacenada que fue enviada por el sitio *web*, y en caso afirmativo la adjuntará, mientras que en caso negativo enviará la petición sin adjuntar nada.

Los cuatro elementos básicos necesarios para poder implementar *cookies* son: una línea de cabecera de la *cookie* en el mensaje respuesta HTTP desde el sitio *web* a una petición del cliente, una línea de cabecera en el mensaje de petición HTTP del cliente, una base de datos en el sitio *web* donde se almacenará toda la información del usuario (nombre, dirección correo electrónico, etc..) asociada a la *cookie* creada por el sitio *web* y un archivo de *cookies* gestionado por el navegador y guardado en el dispositivo del cliente.

El sitio *web* al responder al cliente incluirá como hemos mencionado la *cookie*, y por tanto introducirá en la línea de cabecera del mensaje respuesta HTTP "*Set-Cookie*" con los atributos y valores asignados por el sitio *web*. El navegador del cliente al detectar en la cabecera "*Set-Cookie*" guardará la *cookie* en el directorio de *cookies*. El cliente, al hacer una nueva petición al

sitio *web*, verá que dispone de una *cookie* vinculada al sitio *web* y por tanto en la cabecera HTTP del mensaje de petición incluirá la palabra "*Cookie*:" junto con su valor.

2.5 Tipo de *Cookies*

Las *cookies* pueden ser clasificadas siguiendo diferentes criterios, pero habitualmente la primera clasificación que se suele aplicar es la debida al tiempo que la *cookie* permanecerá almacenada por el navegador en el ordenador del usuario. Utilizando esta clasificación se pueden diferenciar las *cookies* de sesión de las *cookies* persistentes. El segundo criterio que se suele utilizar para clasificar las *cookies* es la utilidad que estas aportan. A continuación se proporciona la clasificación que será utilizada durante el presente trabajo.

2.5.1 *Cookies* de sesión

Las *cookies* de sesión son aquellas que son utilizadas durante una sesión del usuario y son eliminadas una vez que este ha cerrado el navegador. Si el sitio *web* marca la *cookie* con la bandera de persistente a falso indicará que la *cookie* es de sesión. Estas *cookies* evitan que un usuario permanezca registrado (*logged*) inintencionadamente.

2.5.2 *Cookies* persistentes

Las *cookies* persistentes son aquellas que siguen estando almacenadas en la memoria del ordenador cuando el usuario ha cerrado el navegador. Este tipo de *cookie* tiene definida una fecha de validez, la cual ha sido establecida por el sitio *web* que creó la *cookie*. De esta forma, estableciendo una fecha de validez, se permite a la *cookie* que "sobreviva" entre sesiones. Una vez que se ha superado la fecha de validez de la *cookie,* el navegador la eliminará de la memoria del ordenador.

Cookies de terceros

Las "*cookies de terceros*" permiten rastrear los sitios *web* visitados por un usuario. La *cookie* de rastreo es aquella que permite a los sistemas de los sitios *web* monitorizar el comportamiento *online* de los clientes, y por tanto se utilizan para investigar los hábitos de navegación de los usuarios. Este es un tipo específico de *cookie* que puede ser distribuida, compartida y leída por más de un sitio *web* con el propósito de recopilar información o proporcionar información personalizada al usuario.

En principio, las *cookies* sólo son enviadas por el cliente al servidor *web* que las creó, pero en el caso que la respuesta que proporcione un sitio *web* sea por ejemplo una página *web* que necesite de imágenes, el navegador al montar la página *web* que mostrará al cliente podría necesitar acceder a recursos que están ubicados en otros sitios *web*. El sitio *web* donde está ubicado el recurso necesario para mostrar al cliente la página *web*, puede enviar una *cookie* que también será guardada en el navegador del cliente; esta *cookie* es la llamada "*Cookie de terceros*". Por tanto, el cliente al realizar una petición a cualquier sitio *web* donde la "*Cookie* de terceros" tenga validez, enviará la *cookie* junto con la petición.

Las compañías de publicidad suelen utilizar estas "*Cookie* de terceros" para realizar un seguimiento de las actividades de los usuarios, registrando todas las páginas *web* donde la empresa de publicidad ha colocado su publicidad y que son visitadas por cada usuario. La recopilación de información a lo largo del tiempo, permitirá a la compañía de publicidad crear un perfil de los hábitos del cliente y por tanto, podrá enviarle publicidad personalizada.

El problema no está en que los sitios envíen publicidad personalizada, sino en que el usuario desconoce por completo que se esté realizando una recolección de información y que este pueda pensar que está a salvo su privacidad por el simple hecho de no clicar sobre ninguno de los anuncios que aparecen en las páginas *web* que se le muestran.

Adicionalmente, la *cookie* de terceros no tiene porqué ser visible. Si el recurso que se solicita a un servidor tercero es simplemente el valor del color de un píxel, este no será percibido probablemente por el cliente pero sin embargo, este píxel puede llevar asociada una *cookie* de terceros que será almacenada en el directorio del navegador del cliente, y que podrá ser utilizada para rastrear la actividad del cliente sobre todos aquellos sitios *web* que estén vinculados con la *cookie*.

Dentro de las *cookies* de terceros se podrían incluir las denominadas *cookies* funcionales, cuyo objetivo es adquirir información anónima sobre las actuaciones de los sitios *web* de forma que estos puedan ser mejorados. La mayoría de las compañías utilizan Google analytics en sus sitios *web* para rastrear el número de visitantes del sitio y analizar la forma en la que los usuarios navegan por él. Estos paquetes utilizan *cookies* para lograr sus objetivos, aunque son considerados menos intrusivos respecto de la privacidad en comparación con otros los cuáles permiten el rastreo de los usuarios a través de múltiples sitios *web*.

Logged-off *cookies*

Estas *cookies* son del tipo persistente y rastrean las actividades del usuario a pesar de que este se haya desconectado (*logged-out*). “Facebook” utiliza este tipo de *cookies* y justifica su utilización argumentando que son para un buen propósito (seguridad y protección). Esta organización niega que la utilización de este tipo de *cookies* tenga como fin la venta de información a terceros y defiende su uso al poder personalizar el uso del sitio, mejorar el servicio, y proporcionar seguridad y protección. Por último, “Facebook” afirma que los datos recopilados se tratan anónimamente y que 90 días después de su recogida son eliminados automáticamente por el sistema.

2.5.3 Otras clasificaciones

Dentro de la variedad de *cookies* existentes, pueden clasificarse no sólo por el tiempo que se almacenará por el navegador sino siguiendo otros criterios. A continuación se muestran algunos ejemplos.

Cookies seguras

Las *cookies* seguras son aquellas creadas siempre que la comunicación entre los dos extremos (cliente-sitio *web*) es realizada usando una sesión segura, por ejemplo utilizando el protocolo HTTPS donde la conexión estará cifrada.

Cookies certificadas

La idea de la utilización de *cookies* certificadas se basa en la creación de un mecanismo por el cual un usuario pueda configurar su navegador de forma que pueda aceptar el uso de *cookies* de sitios *web* que han sido auditados. Normalmente son originadas por un sitio *web* el cual en su declaración del uso de sus *cookies* cumple con los requisitos de privacidad del cliente, y por tanto pueden ser aceptadas automáticamente por este. Así, el uso de *cookies* certificadas puede aliviar posibles miedos que los usuarios puedan tener en relación al tratamiento que el sitio *web* pueda realizar de sus datos personales.

Las *cookies* certificadas son creadas utilizando técnicas criptográficas como por ejemplo, firmas digitales, códigos de autenticación, mensajes resumen y encriptación. La técnica utilizada dependerá de la implementación que se realice de este tipo de *cookies*. El sitio *web* obtendrá un certificado criptográfico por el cual se avala su identidad y que afirma cómo utilizará la información recopilada por la *cookie*.

Las *cookies* certificadas proporcionan: autenticación, integridad y confidencialidad. La autenticación verifica la identidad digital del remitente de la *cookie*, la integridad protege contra modificaciones no autorizadas de las *cookies* y la confidencialidad protege contra la revelación de los valores de la *cookie* a una entidad no autorizada.

Cookies dinámicas de reescritura

Las *cookies* dinámicas de reescritura (*Dynamic Cookies Rewriting Technique*) son utilizadas para proteger las *cookies* almacenadas en el directorio del navegador del ordenador del cliente de un ataque (*Cross Site Script Attacks*) por el cual un atacante roba las *cookies* del directorio de un navegador. Esta técnica está explicada más ampliamente en el apartado 3.5 – Robo de *cookies*.

Flash cookies

El método utilizado por las *flash cookies* es el mismo que el resto de *cookies* pero tienen la particularidad de que son específicas para ser utilizadas con el programa Adobe Flash Player. Este tipo de *cookies* son utilizadas principalmente para juegos o programas con contenido de vídeo. Este tipo de *cookies* no pueden ser controladas a través del navegador y la única forma de realizar un control es a través del sitio *web* de Adobe. Accediendo a este se podrá modificar su configuración.

Supercookies y *Cookies* zombie

Esta clasificación incluye todas aquellas *cookies* que son muy difíciles de ser detectadas y eliminadas. En el caso de que un sitio *web* utilice este tipo de *cookie*, se considera que se está cometiendo una infracción respecto de la nueva Directiva Europea aplicable al uso de las *cookies*.

2.6 Creación de una *cookie*

La creación y almacenaje de una *cookie* depende de la implementación. En algunos casos pueden existir limitaciones a la hora de la creación de las mismas, por ejemplo, limitaciones en el tamaño de la cabecera HTTP o no permitir que la *cookie* se establezca para un dominio diferente del que pertenece el sitio que la ha creado.

La transferencia de páginas *web* utiliza el protocolo HTTP, por lo que tras realizar una petición a un servidor *web*, este responderá proporcionando la página *web* solicitada. El protocolo utiliza un encabezado en el cual el cliente y el sitio *web*, extremos de la comunicación, se intercambian información relativa a la solicitud y transferencia de la información. El sitio *web* al responder a la petición del cliente enviará un mensaje "*Set-Cookie*" mediante el cual solicita al navegador del cliente que guarde la información contenida en la *cookie* que le está enviando, y que devuelva la *cookie* guardada cada vez que realice una petición al domino de validez de la *cookie*.

La estructuras de las cabeceras que se introducen vienen definidas en el RFC 6265 y establece que la cabecera que se insertará por el sitio *web* hacia el navegador cuando quiere introducir una *cookie* es la siguiente:

Set-Cookie: Nombre=VALOR; Caduca=FECHA; Ruta=RUTA; Dominio=NOMBRE_DOMINIO; Seguridad

El navegador del cliente al recibir la *cookie*, analizará las preferencias del cliente y en el caso de que el cliente haya aceptado la recepción de *cookies*, el navegador guardará la información que contiene y adjuntará el valor de la *cookie* en cada petición que realice al sitio *web*. Por tanto el navegador introducirá la siguiente cabecera:

Cookie: Nombre=VALOR;

Cabe destacar que los atributos de las *cookies* no son devueltos por el navegador en las peticiones al sitio *web*. El sitio *web* al recibir la *cookie* obtendrá el valor de la misma y podrá relacionar la petición actual del cliente con la peticiones anteriores que el cliente ha realizado al sitio *web* realizando una consulta a su base de datos.

2.7 Obtención del valor de una *cookie*

Para obtener los valores de una *cookie* no es necesario leer la cabecera HTTP de una *cookie*. Además muchas veces las *cookies* son transferidas utilizando HTTPS, lo cual imposibilita la capacidad de captación de la *cookie* al realizarse la transmisión de esta sobre un canal cifrado.

La información relativa a las *cookies* está almacenada en un directorio del navegador o en el sitio *web*. Por lo tanto, las *cookies* pueden ser leídas tanto en el lado del navegador como en el lado del sitio *web*. Para poder obtener los valores de una *cookie* es determinante el lenguaje que es utilizado. La mayoría de los lenguajes utilizados leen la cabecera de los mensajes y permiten el acceso al contenido a través de una variable o un objeto. Algunos navegadores permiten al usuario obtener toda la información relevante de los atributos de una *cookie* en concreto.

Las *cookies* que están almacenadas por el navegador pueden proceder de diferentes dominios, pero las *cookies* que están guardadas en un sitio *web* son aquellas que ha creado él mismo y no son pertenecientes a otros dominios.

2.8 Eliminar un valor de la *cookie*

Las razones por las cuales se deseen eliminar *cookies* tanto por el sitio *web* como por el cliente pueden ser diversas.

Las *cookies* de sesión, tal y como hemos comentado anteriormente, son eliminadas por el navegador al finalizar el cliente la sesión. Las *cookies* persistentes son eliminadas por el navegador una vez que se ha superado el periodo de validez de la misma. Una vez que las *cookies* han sido eliminadas, no se enviarán al sitio *web* junto con las peticiones realizadas por el cliente.

Las *cookies* no son enviadas al sitio *web* no sólo por la finalización de su validez, como ocurre con las *cookies* persistentes, o por cierre del navegador, en el caso de las *cookies* de sesión, sino también por los siguientes motivos:

- El usuario da la orden de borrar la *cookie* almacenada.
- El servidor cambia la fecha de validez a una fecha ya pasada de forma que esté ordenando al navegador que elimine la *cookie* almacenada.
- El servidor por alguna razón establece el campo valor a nulo (*null*).

3. CUESTIONES GENERALES – ADMINISTRACIÓN DE *COOKIES*

Este capítulo tiene como objetivo contestar a las preguntas más habituales que los usuarios tienen en relación al uso de las *cookies*.

3.1 ¿Son peligrosas las *cookies* para mi ordenador?

Desde que se dieron a conocer las *cookies* y sobre todo teniendo en cuenta que se habían estado utilizando sin el conocimiento de los ciudadanos, por ejemplo por la CIA durante la última década del siglo XX, se ha creado un rechazo entre los usuarios debido a las implicaciones que el uso de las *cookies* pueden tener en relación a su privacidad. Este hecho ha dado pie a diversas creencias no siempre ciertas acerca de las *cookies*. En el año 2005 Jupiter Research publicó los resultados de un estudio según el cual un importante porcentaje de los entrevistados creían que era cierta alguna de las siguientes afirmaciones:

- Las *cookies* son similares a gusanos y virus que pueden borrar la información de los discos duros de los usuarios.
- Las *cookies* son un tipo de *spyware* porque pueden leer información personal almacenada en el ordenador de los usuarios.
- Las *cookies* generan *popups*.
- Las *cookies* se utilizan para generar *spam*.
- Las *cookies* sólo se utilizan con fines publicitarios.

Las *cookies* son datos y no código, por lo tanto no pueden ni eliminar ni leer información del ordenador del usuario. El único efecto que tiene sobre el sistema el uso de las *cookies* es el almacenamiento de información de diversos sitios *web* por parte del navegador.

3.2 ¿Son las *cookies* una amenaza a mi privacidad?

Las *cookies* tienen implicaciones respecto de la privacidad de los usuarios ya que su uso por parte de los navegadores, especialmente las llamadas "*Cookies de terceros*", permite a compañías de publicidad realizar un seguimiento de las actividades de un usuario a través de diferentes sitios *web*. La posibilidad de crear un perfil de usuario, por ejemplo, utilizando las "*cookies de terceros*" se ha considerado un peligro en relación a la privacidad de los individuos. Como consecuencia de esta creciente preocupación, algunos países han desarrollado normativas relativas a la privacidad de las telecomunicaciones.

Uso de *cookies* en publicidad

Un sitio *web* implica un coste para el poseedor del mismo, sobre todo si quiere publicitar su sitio en sitios de terceros. Un método para financiar dicho coste es a través de la publicidad, permitiendo que una compañía de publicidad introduzca anuncios en su página *web*. Por este servicio la empresa de publicidad pagará una cantidad al propietario del sitio *web*.

El problema no radica en la transacción económica entre el propietario del sitio *web* y la empresa de publicidad, sino en que la publicidad introducida tiene asociada el envío de *cookies* desde la empresa de publicidad al cliente, lo cual permitirá a la empresa de publicidad identificar al cliente a través de la *cookie*. La empresa de publicidad introduce piezas de publicidad en numerosas páginas *web* de tal forma que a través de la *cookie* inicial que recibió el cliente, la empresa de publicidad podrá conocer qué páginas ha visitado el cliente y por tanto, podrá crear un perfil bastante detallado de sus intereses y aficiones a partir de las actividades de navegación. El problema radica en el hecho de que el usuario no es consciente de que se ha instalado una *cookie* mediante la cual se está creando un perfil suyo.

Inicialmente existían empresas que utilizaban la información recopilada para venderla a otras empresas, por ejemplo los Bancos en Sudáfrica, los cuales vendieron información personal de sus clientes a terceros. Otro ejemplo son las empresas *Infoseek* y *Lycon Inc.*, las cuales declararon su intención de crear sistemas de rastreo y mantener perfiles detallados de sus usuarios. La empresa *DoubleClick* es un ejemplo de una compañía de publicidad que utilizaba *cookies* para crear perfiles de usuario, proporcionar anuncios específicos a los usuarios y que incluso intentó enlazar los perfiles con la identidad de los usuarios.

¿Pero los usuarios están preocupados por el uso de las *cookies*? Algunos estudios han revelado que un porcentaje muy reducido de las *cookies* son rechazadas. Los motivos de este bajo índice no está muy claro pero quizás se deban a los siguientes motivos:

- Algunos usuarios desconocen la existencia de las *cookies*, su utilización por sitios *web* y las implicaciones que pueden tener su uso.
- Algunos usuarios conocen las *cookies* pero no relacionan que estas puedan ser utilizadas para rastrearlos.
- Algunos usuarios conocen las *cookies* y saben que mediante ellas pueden ser rastreados pero no les preocupa.
- Otros usuarios no saben diferenciar qué *cookies* deben aceptar y cuales rechazar y por tanto, optan por permitirlas todas.
- Otros conocen el uso de las *cookies*, son conscientes de la utilización de los datos pero consideran que estos serán protegidos y utilizados de forma discreta.
- Otros consideran que los organismos protegerán mediante regulación el uso adecuado de las *cookies*.

Independientemente del grado de preocupación de los clientes, la obtención de los perfiles de estos junto a la posibilidad de relacionarlo con la identidades de los mismos es una invasión seria a la privacidad de los individuos.

3.3 ¿Puedo borrar las *cookies*?

Los navegadores deben poder almacenar un número mínimo de *cookies* cuyo tamaño es reducido debido a la pequeña cantidad de información que contienen. Sin embargo, el navegador puede almacenar un número máximo de *cookies* por lo que en el caso de haber llegado al límite de almacenamiento este deberá aplicar su política de eliminación de *cookies*.

Las *cookies* no suelen permanecer eternamente en la memoria del ordenador ya que suelen ser eliminadas por el navegador dependiendo de su naturaleza, como se ha explicado anteriormente. Las *cookies* de sesión son eliminadas al cerrar el navegador, y las *cookies* persistentes son eliminadas por el navegador una vez ha llegado a la fecha máxima de validez que estableció el sitio *web*.

El servidor puede en cualquier momento eliminar una *cookie* que esté guardada en el disco duro de un cliente, enviando nuevamente la *cookie* indicando en el campo caducidad un valor que ya está caducado. Adicionalmente, el usuario dispone de la posibilidad de eliminar *cookies.* Para ello será necesario realizarlo mediante las opciones que nos permite el navegador *web*.

Algunos navegadores permiten el borrado de todas las *cookies* almacenadas en el directorio del disco duro con sólo una acción. En el caso de que el cliente seleccione esta opción se borrarán absolutamente todas las *cookies*, incluso aquellas que puedan interesarle. Sin embargo, algunos navegadores también permiten la eliminación de las *cookies* una a una. Esta opción permite al usuario eliminar sólo aquellas *cookies* que no desee tener almacenadas en su dispositivo.

3.4 ¿Cómo configuro mi navegador para rechazar *cookies*?

Actualmente la mayoría de los navegadores soportan el uso de *cookies* y permiten al usuario configurar el tratamiento que el navegador debe dar a estas. Dentro de las opciones más habituales de los navegadores se puede encontrar:

- No permitir el uso de *cookies*.
- Preguntar al usuario antes de aceptar una *cookie*.
- Aceptar *cookies* de sesión.
- Rechazar *cookies* persistentes.
- Rechazar *cookies* de terceros.
- Rechazar *cookies* de determinados dominios.

El cliente deberá configurar el navegador dependiendo de las opciones que este ofrezca en función de sus necesidades.

Las especificaciones P3P permiten a un servidor definir su política de privacidad mediante la cual indica el tipo de información que recoge y el tratamiento que hace de esta. Algunos navegadores permiten comparar las preferencias del usuario con las políticas establecidas por un sitio *web* de forma que el navegador automáticamente permita o deniegue el uso de las *cookies* de ese sitio *web*.

En el apartado 5 se muestran como ejemplo las opciones de configuración de tres navegadores.

3.5 Problemas asociados a las *cookies*

Como ya se ha mencionado, las *cookies* pueden proporcionar información sobre los hábitos de navegación del cliente, lo cual implica un problema de privacidad. Las principales interesadas en explotar esta capacidad de las *cookies* son las empresas de publicidad, ya que a partir de los hábitos de navegación se pueden crear perfiles de los clientes y proporcionar anuncios de acuerdo a los intereses de los mismos. El documento "*Cookie* Central" [*Cookie* Central 2008] proporciona mucha información en relación a la controversia que suscita la utilización de las *cookies*.

Adicionalmente el uso de la *cookies* puede ocasionar otros problemas como puede ser que al utilizarlas no se identifique correctamente a los usuarios o que puedan ser utilizadas para realizar ataques de seguridad. A continuación se detalla una serie de ejemplos de problemas asociados al uso de *cookies*.

Identificación de usuario

Las *cookies* no identifican a un usuario sino que identifican una combinación ordenador-navegador-usuario, lo cual implica que varios usuarios que utilicen el mismo navegador en un ordenador podrían utilizar una misma *cookie* para solicitar los servicios de un sitio *web* determinado. Una solución para evitar este problema de identificación de usuario es que los usuarios al utilizar un ordenador utilicen su cuenta de usuario de forma que se garantice la identificación y no permita que las *cookies* de un usuario sean utilizadas por otro usuario.

Robo de *Cookies*

Las *cookies* son almacenadas en el ordenador del usuario. Por tanto, un acceso al disco duro del usuario por un tercero (atacante) podría implicar el robo de estas y su posterior utilización. Este hecho podría provocar que el atacante que ha captado la *cookie* tras realizar un análisis, obtenga información sensible como pueda ser el nombre de usuario o un testigo "*token*" el cual se utiliza para autenticar al usuario legítimo de la *cookie*.

Las *cookies* son enviadas en las dos direcciones, desde el cliente al sitio *web* y viceversa, normalmente durante sesiones HTTP. En este tipo de sesiones la información viaja en claro y son visibles para aquellos usuarios que estén captando los paquetes que viajan por la red.

El *scripting* es un método que permite que el valor de la *cookies* almacenadas se envíen a servidores que normalmente no reciben esa información (robo). Esto es posible ya que existen navegadores que permiten la ejecución de parte de código recibido desde el servidor (script malicioso) y, por tanto, podrían permitir que las *cookies* fuesen captadas y enviadas a terceros servidores.

Es recomendable, para evitar la captación de información, que las *cookies* no contengan ninguna información sensible y que las transmisiones de las *cookies* se realicen utilizando el protocolo HTTPS, ya que este proporciona seguridad mediante el cifrado de la conexión establecida entre el cliente y el sitio *web*.

Adicionalmente, existe una técnica denominada "Dynamic *Cookies* Rewriting" cuyo objetivo es impedir los ataques tanto persistentes como no persistentes (*Cross Site Scripting Attack- XSS attack*), con los que se pueden suplantar a los usuarios mediante *cookies* robadas. Esta técnica suele ser implementada en el *web* proxy que es donde se realiza la reescritura de las *cookies* que son enviadas entre el sitio *web* al usuario y viceversa. Hay que destacar que se puede implementar sin necesidad de modificar el navegador *web* o el sitio *web*. De esta forma, en el caso de que se produjera un robo de *cookies* guardadas por el navegador en el ordenador de un usuario, estas no podrían ser utilizadas por el atacante ya que al no haber sido reescritas no serían reconocidas por el sitio *web*. El *web* proxy actúa modificando el valor de la *cookie* dependiendo del tramo donde se tenga que utilizar, siendo el primer tramo el establecido entre el sitio *web* y el *web* proxy; el segundo tramo es el establecido entre el *web* proxy y el cliente, y por tanto el *web* proxy actúa de traductor y evita la utilización de la *cookie* en caso de robo.

Falsificación de *cookies*

Las *cookies* pueden ser interceptadas en el proceso de intercambio de información entre el cliente y el sitio *web* si no se utiliza el protocolo HTTPS, el cual cifra la sesión. En el caso de que la *cookie* sea interceptada podría modificarse el valor de la misma provocando un falsificación de la *cookie* antes de que sea devuelta al sitio *web*.

Cookies entre sitios

Los sitios *web* establecen *cookies* que son enviadas a los usuarios una vez que reciben las peticiones. Cada sitio *web* debe tener sus propias *cookies* y no es conveniente que se produzca el intercambio de *cookies* entre diferente sitios *web*, ya que sino un sitio *web* (atacante) podría modificar el valor de la *cookie* o incluso definir *cookies* de otro sitio *web*.

Este tipo de problema relacionado con el envío de *cookies* entre sitios, se produce principalmente cuando los navegadores tienen alguna vulnerabilidad y esta es aprovechada por un atacante para realizar esta práctica. Las fronteras lógicas de las que disponen los navegadores proporcionan la seguridad que no permitirán que un sitio *web* pueda modificar o robar datos de otro.

3.6 Alternativas al uso de las *cookies*

Existen diversas alternativas al uso de las *cookies* que aparentemente podrían proporcionar resultados semejantes a los que se obtienen mediante el uso de estas, pero la utilización de las alternativas también conllevan inconvenientes, lo cual ha comportado que el uso de *cookies* sea la opción más utilizada. A continuación se muestra una alternativa, no efectiva, al uso de las *cookies* para el reconocimiento del usuario por parte de los sitios *web*.

Dirección IP

Aparentemente puede parecer que asociar un usuario a una dirección IP es una solución para que el servidor reconozca quién es el usuario con el que se está dialogando. Sin embargo, esta solución no es del todo correcta ya que la dirección IP puede identificar al ordenador que tiene la dirección IP asignada, siempre que esta asignación sea estática, pero no identifica al usuario. Por otro lado, hoy en día es habitual que un ISP (*Internet Service Provider*) proporcione una dirección IP pública de salida de la red de una empresa utilizando el protocolo NAT (*Network Address Translation*), mediante el cual miles de usuarios podrían estar utilizando simultáneamente una única dirección IP pública. Esto implica que la dirección IP no tiene porqué estar asociada a un usuario. Por tanto, la utilización de la dirección IP no es una solución válida para que un servidor *web* pueda reconocer a un usuario.

4. LEGISLACIÓN

El creciente interés que suscitó el conocimiento por parte de la opinión pública de las posibles implicaciones respecto de la privacidad de los usuarios al utilizar los servicios que proporcionan los sitios *web*, ocasionó que gobiernos de diferentes estados desarrollasen normativas relativas a la privacidad en las telecomunicaciones. Concretamente se han desarrollado reglas que deben ser cumplidas al utilizar *cookies*, por ejemplo, en la Directiva de la Unión Europea de 2002 sobre la privacidad en las telecomunicaciones (Directiva 2002/58/CE).

En la parte introductoria de la Directiva 2002/58/CE se establece lo siguiente:

Punto 5 – Actualmente se están introduciendo en las redes públicas de comunicación de la Comunidad nuevas tecnologías digitales avanzadas que crean **necesidades específicas en materia de protección de datos personales y de la intimidad de los usuarios**.

Punto 6 – Los servicios de comunicaciones electrónicas disponibles al público a través de Internet introducen nuevas posibilidades para los usuarios, pero también **nuevos riesgos para sus datos personales e intimidad**.

Punto 9 – Los Estados miembros, los proveedores y usuarios afectados y las instancias comunitarias competentes deben cooperar para el establecimiento y el desarrollo de las tecnologías pertinentes cuando sea necesario para aplicar las garantías previstas en la presente Directiva y teniendo especialmente en cuenta el **objetivo de reducir al mínimo el tratamiento de los datos personales** y de tratar la información de forma anónima o mediante seudónimos cuando sea posible.

Punto 21 – Deben adoptarse medidas para **evitar el acceso no autorizado** a las comunicaciones a fin de proteger la confidencialidad de las mismas.

Punto 23 – **La confidencialidad de las comunicaciones debe garantizarse también en el curso de las prácticas comerciales lícitas**.

Punto 24 – Los denominados “programas espía” (*spyware*), *web* bugs, identificadores ocultos y otros dispositivos similares pueden introducirse en el terminal del usuario sin su conocimiento para acceder a información, archivar información oculta o rastrear las actividades del usuario, lo que puede suponer **una grave intrusión en la intimidad de dichos usuarios.** Sólo debe permitirse la utilización de tales dispositivos con fines legítimos y con el conocimiento de los usuarios afectados.

En el punto 25 se hace alusión expresa a las *cookies* y dice lo siguiente: No obstante, los dispositivos de este tipo, por ejemplo **los denominados “chivatos” (*cookies*), pueden constituir un instrumento legítimo y de gran utilidad, por ejemplo, para analizar la efectividad del diseño y de la publicidad de un sitio *web* y para verificar la identidad de usuarios participes en una transacción en línea**. En los casos en que estos dispositivos, por ejemplo los denominados “chivatos” (*cookies*), tengan un propósito legítimo, como el de facilitar el suministro de servicios de la sociedad de la información, debe autorizarse su uso a condición de que se facilite a los usuarios información clara y precisa al respecto, de conformidad con la Directiva 95/46/CE, para garantizar que los usuarios están al corriente de la información que se introduce en el equipo terminal que están utilizando. Los usuarios deben tener la posibilidad de impedir que se almacene en su equipo terminal un “chivato” (*cookie*) o dispositivo semejante. Esto es particularmente importante cuando otros usuarios distintos al usuario original tienen acceso al equipo terminal y, a través de este, a cualquier dato sensible de carácter privado almacenado en dicho equipo. La información sobre la utilización de distintos dispositivos que se vayan a instalar en el equipo terminal del usuario en la misma conexión y el derecho a impedir la instalación de tales dispositivos se pueden ofrecer en una sola vez durante una misma conexión y abarcar asimismo cualquier posible utilización futura de dichos dispositivos en conexiones posteriores. La presentación de la información y del pedido de consentimiento o posibilidad de negativa debe ser tan asequible para el usuario como sea posible. No obstante, **se podrá supeditar el acceso a determinados contenidos de un sitio *web* a la aceptación**

fundada de un "chivato" (*cookie*) o dispositivo similar, en caso de que este tenga un propósito legítimo.

En el párrafo 3 del artículo 5 se establece: Los Estados miembros velarán por que únicamente se permita el uso de las redes de comunicaciones electrónicas con fines de almacenamiento de información o de obtención de acceso a la información almacenada en el equipo terminal de un abonado o usuario a condición de que **se facilite a dicho abonado o usuario información clara y completa, en particular sobre fines del tratamiento de los datos,** con arreglo a lo dispuesto en la Directiva 95/46/CE y de que el responsable del tratamiento de los datos le ofrezca el derecho a negarse a dicho tratamiento. La presente disposición no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar o facilitar la transmisión de una comunicación a través de una red de comunicaciones electrónicas, o en la medida de lo estrictamente necesario a fin de proporcionar a una empresa de información un servicio expresamente solicitado por el usuario o el abonado.

Esta normativa no requiere que sea el usuario quien deba deshabilitar "*Cookies de terceros*" al configurar su navegador *web* sino que sea el usuario que deba realizar una acción consciente para su activación.

El desarrollo e implantación de la Directiva 2002/58/CE no fue seguida por todos los países pertenecientes a la Unión Europea lo cual implicó que se recomendase un análisis de la situación de cada uno de los Estados miembros.

4.1 Directiva 2009/136/CE y normativa de 26 de Mayo de 2011

En el año 2009 se publicó una nueva Directiva Europea 2009/136/CE por la cual se modificaba la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) nº 2006/2004 sobre la cooperación en materia de protección de los consumidores.

El objetivo de la normativa Europea de 26 de Mayo de 2011 sobre las *cookies* en los sitios *web*, es aumentar la protección de la privacidad de los individuos dentro de la Unión Europea al navegar por Internet independientemente del tipo de dispositivo utilizado. Esta directiva es aplicable a todos los sitios *web* independientemente de la ubicación de estos, siempre que den servicios a ciudadanos europeos. Así por ejemplo, sitios ubicados en EEUU también tienen la obligación de cumplir con esta directiva. Aunque es difícil forzar el cumplimiento de la normativa a aquellas empresas que no tienen "presencia legal" dentro de la Unión Europea.

4.2 ¿Qué necesitan los sitios *web* para cumplir con la normativa actual?

Todos los propietarios de sitios *web*, con el fin de cumplir con la nueva normativa europea "*EU Cookie Law*", es necesario que realicen una auditoria a sus sitios con el fin de garantizar que las *cookies* que utilizan cumplen con la regulaciones establecidas.

El ICO (*Information Commission Office*) considera que muchos navegadores no están preparados para cumplir con la nueva legislación europea. En consecuencia el ICO ha modificado la normativa por la cual se requiere que cada sitio *web* deba preguntar directamente al visitante si desea o no que se descarguen *cookies* en su ordenador. De esta manera, son los usuarios los que tienen que dar permisos a los sitios *web* que estén visitando a utilizar *cookies*. Así se cumple con el punto que indica que los sitios *web* necesitarán específicamente obtener un consentimiento del usuario para poder almacenar *cookies* en sus dispositivos. Adicionalmente, es necesario que los sitios *web* proporcionen información a sus usuarios de forma que sean conscientes de las *cookies* que se están utilizando y una explicación relativa a lo que el sitio *web* realiza con las *cookies*.

4.3 ¿Qué tipo de consentimiento del cliente es requerido?

La normativa comunitaria de septiembre de 2012, que regula la utilización de las *cookies* por parte de los sitios *web*, requiere un consentimiento por parte del usuario mediante el cual se asegura que este es consciente del uso que el sitio *web* hará de sus datos y las finalidades de los mismos.

El consentimiento del usuario permite la utilización y el almacenamiento de *cookies* en el ordenador del usuario. El consentimiento puede obtenerse de diferentes formas, como por ejemplo, haciendo clic sobre el texto "acepto", "permito", etc. Se considera aceptable lo que se conoce como "consentimiento implícito", el cual será utilizado cuando el usuario no rellena un formulario *online* o utiliza un *pop-up* y continua utilizando el sitio *web* como siempre. Se considera que el consentimiento es implícito porque el usuario no ha dejado claros sus deseos y continua navegando.

4.4 Auditorías de las *cookies*

Actualmente se requiere a los propietarios de los sitios *web* que demuestren evidencias del cumplimiento de la nueva normativa relacionada con el uso de las *cookies*. Una forma de evidenciar dicho cumplimiento es mediante la realización de auditorías de las *cookies*.

Diversas empresas han desarrollado *software* específico para ayudar a los propietarios de los sitios *web* a conocer la situación actual del uso de las *cookies* por parte de sus sitios, y ayudar en la adaptación de los mismos a los requerimientos de la nueva normativa. También se ha desarrollado *software* específico para realizar las auditorías a las *cookies* de los sitios *web*. En Internet se puede encontrar *software* que se puede descargar gratuitamente. Incluso existen empresas que se publicitan con la intención de ayudar a las empresas en el cumplimiento de la legislación actual ofreciendo diversas opciones a los clientes.

5. ANALISIS PRÁCTICO

Una vez realizado un análisis teórico de lo que es una *cookie* y para qué son utilizadas, se ha realizado un estudio práctico en el cual se ha procedido a analizar el comportamiento de los tres navegadores más utilizados, que son los siguientes: Google Chrome (versión 51.0.2704.103), Firefox (3.6.22) y Safari (9.1.1). Las versiones de los navegadores utilizados para realizar este análisis práctico son las indicadas anteriormente. Para realizar el análisis se ha utilizado un ordenador MacBook Pro con un procesador Intel Core 2 Duo a 2.53GHZ, Memoria 4 GB 1067 MHZ DDR3 y sistema operativo versión 10.9.5 OS Mavericks.

Tal y como se ha explicado anteriormente, las *cookies* son almacenadas en la base de datos de los sitios *web* y en el navegador del usuario. Se ha optado por realizar un análisis de las *cookies* que son almacenadas en el lado del cliente, ya que no es posible acceder a la base de datos de los sitios *web* que se utilizarán en el estudio. Por otro lado también se ha descartado hacer un análisis de las *cookies* que viajan entre el cliente y el servidor mediante capturas de tráfico, ya que normalmente circulan sobre canales seguros y no se posible descifrar la información que circula sobre estos canales. Además el trabajo tiene por objetivo analizar la privacidad que nos proporcionan los navegadores más utilizados y hacer recomendaciones a los usuarios sobre las opciones más convenientes para proporcionar una mayor privacidad.

La metodología que se ha aplicado para el análisis de los navegadores ha sido la misma y los pasos realizados han sido los siguientes:

1.- Análisis de las opciones de seguridad que proporciona el navegador.
2.- Aplicar las diferentes opciones de seguridad que proporciona el navegador a tres tipos diferentes de sitios *web*.
3.- Analizar el comportamiento de los navegadores en relación a las opciones seleccionadas y tratamiento de las *cookies* que estos realizan, sobre todo en aquello relativo a la privacidad de los usuarios.

El último paso que se ha realizado tras el análisis es realizar una recomendación de las opciones que debe seleccionar el cliente sobre el navegador que habitualmente utiliza para obtener el mayor grado de privacidad, dependiendo del tipo de sitios *web* a las cuales suele requerir sus servicios.

Los sitios *web* que se han utilizado para realizar el análisis han sido “El País”, “Facebook” y “Amazon”. Se ha optado por realizar un análisis de estos sitios *web* al proporcionar servicios totalmente diferentes para el usuario. “El País” es un diario digital al cual los usuarios acceden para obtener información actualizada. Este diario adicionalmente muestra publicidad a la cual los usuarios podrán acceder simplemente clicando sobre el enlace o las imágenes. El segundo sitio *web* utilizado es la conocida red social “Facebook” mediante la cual principalmente los usuarios comparten información con el resto de usuarios, permitiéndoles adjuntar imágenes. Adicionalmente permite el intercambio de mensajes de forma privada entre dos miembros registrados en la aplicación. Este sitio *web* también permite que otros sitios *web* puedan mostrar publicidad a la cual los usuarios pueden acceder fácilmente. Por último, se ha utilizado “Amazon” al ser un sitio *web* que proporciona el servicio del comercio electrónico, a través del cual los usuarios pueden acceder y comprar los diversos productos que son ofertados.

5.1 Opciones de configuración de los navegadores

En este apartado 5 se mostrarán las opciones de seguridad relacionadas con el uso de las *cookies* y por tanto con la privacidad que ofrecen los tres navegadores más usados.

5.1.1 Navegador Google Chrome (Versión 51.0.2704.103)

A pesar de ser uno de los navegadores de Internet que ha sufrido más fallos de seguridad, es al mismo tiempo de los más seguros, ya que es muy complejo realizar un ataque o aprovechar

las vulnerabilidades de este navegador. Este navegador ha implementado medidas para aumentar la seguridad mientras navegamos por Internet.

Nos centraremos en la configuración del navegador sobre privacidad y más concretamente sobre la gestión de las *cookies*. Para acceder a la configuración del navegador se seleccionará:

Menú> Configuración> Mostrar configuración avanzada> Privacidad

Figura 3 – Opciones de configuración de privacidad navegador Google Chrome

a) La pestaña "Configuración de contenido" mostrada en la figura 3 permite administrar cómo gestiona Chrome el contenido y los permisos de los sitios *web*. A continuación se pueden observar las opciones disponibles:

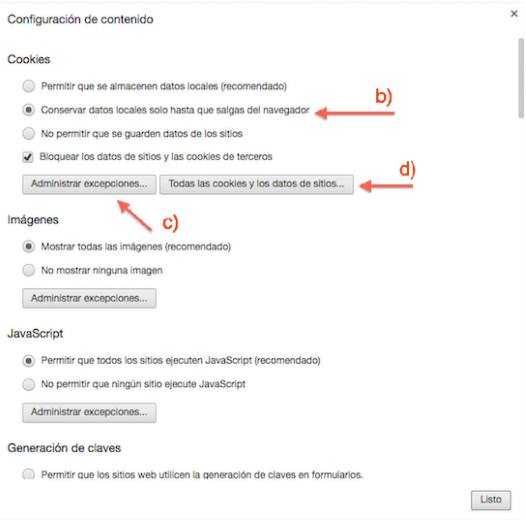

Figura 4 – Opciones de configuración de contenido navegador Google Chrome

b) Por tanto las opciones de configuración de las *cookies*, tal y como se puede observar en la figura 4, son las siguientes:

- Permitir que se almacenen datos locales (recomendado)
- Conservar datos locales hasta que salgas del navegador
- No permitir que se guarden datos de los sitios
- Bloquear los datos de sitios y las *cookies* de terceros
- Administrar excepciones

c) Al clicar el usuario sobre el botón “Administrar excepciones…” de la figura 4, el navegador mostrará una ventana como se muestra en la figura 5.

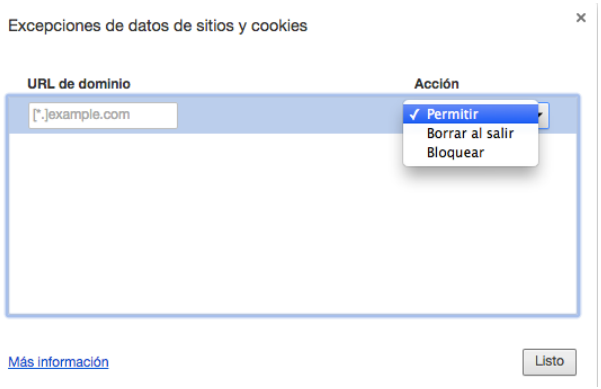

Figura 5 – Excepciones de datos de sitos y *cookies* navegador Google Chrome

d) Al clicar el usuario sobre el botón “Todas las *cookies* y los datos de sitios” de la figura 4, el navegador mostrará una ventana como se muestra en la figura 6.

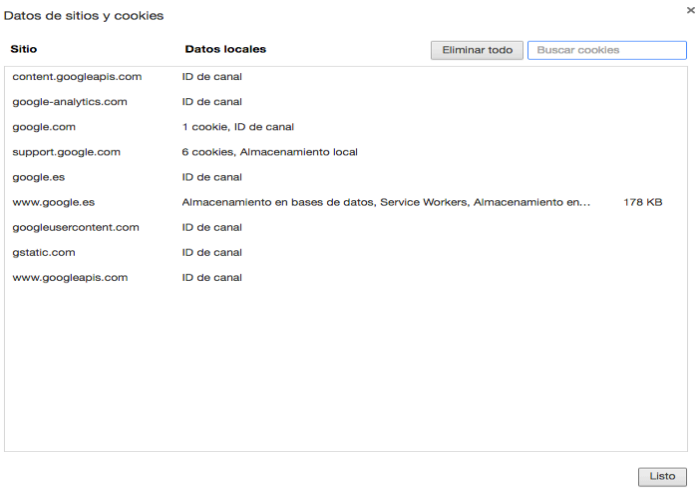

Figura 6 – Ejemplo *cookies* almacenadas por el navegador Google Chrome

e) La pestaña “Borrar datos de navegación”, mostrada en la figura 3, permite eliminar información de la actividad de navegación, como son el historial, las *cookies* o contraseñas guardadas.

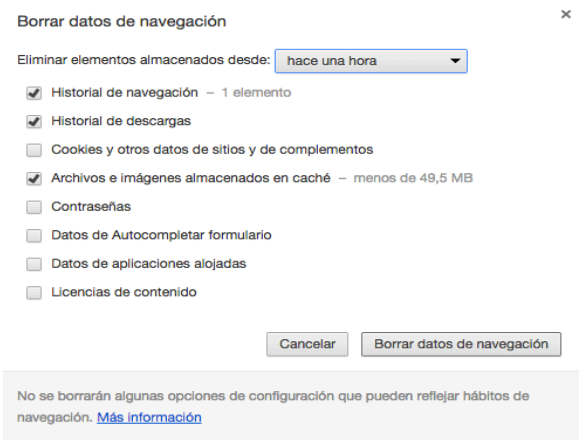

Figura 7 – Opciones borrar datos de navegación del navegador Google Chrome

A continuación se muestra el texto de ayuda que proporciona "Google" en relación a las opciones de configuración del navegador respecto de la privacidad:

- **Utilizar un servicio *web* para intentar resolver errores de navegación:** si no puede conectarse a una página *web*, puedes obtener sugerencias de otras páginas similares a la que intentas acceder. Chrome envía a "Google" la dirección *web* de la página que intentas visitar para ofrecer sugerencias.

- **Utilizar un servicio de predicción para completar las búsquedas y las URL introducidas en la barra de direcciones o en el cuadro de búsqueda del menú de aplicaciones:** estas sugerencias se basan en búsquedas *web* relacionadas, en tu historial de navegación y en sitios *web* populares. Si tu motor de búsqueda predeterminado ofrece un servicio de sugerencias, el navegador puede enviar el texto que escribes en la barra de direcciones al motor de búsqueda. Obtén más información sobre el servicio de predicciones de la barra de direcciones.

- **Cargar recursos previamente para que las páginas se carguen de forma más rápida:** los navegadores utilizan una dirección IP para cargar una página *web*. Al acceder a un sitio *web*, Chrome puede buscar las direcciones IP de todos los enlaces de las páginas y cargar las que podrías visitar a continuación. Si activas esta opción, los sitios *web* y los contenidos insertados que se carguen previamente pueden establecer y leer sus propias *cookies* como si los hubieras visitado (aunque no lo hayas hecho).

- **Enviar a "Google" automáticamente información sobre posibles incidentes de seguridad:** si activas la casilla, estos datos se enviarán cada vez que Chrome detecte una descarga o un sitio *web* sospechosos. Obtén más información sobre *software* malicioso y advertencias de descargas no habituales.

- **Obtener protección para ti y para tu dispositivo frente a sitios *web* peligrosos:** recibe una alerta instantánea cuando Chrome detecte que el sitio *web* al que intentas acceder puede ser dañino. Al acceder a un sitio *web*, Chrome comprueba si aparece en una lista de sitios *web* maliciosos que se almacena en tu ordenador. Si el sitio *web* coincide con algunos de los elementos de la lista, el navegador envía una copia parcial de la dirección a "Google" para averiguar si el sitio *web* al que quieres acceder es peligroso. Obtén más información sobre la protección con la función de Navegación Segura.

- **Utilizar un servicio *web* para revisar la ortografía:** utiliza la misma tecnología de corrección ortográfica que la Búsqueda de "Google". Chrome envía el texto que has escrito a los servidores de "Google".

- **Enviar automáticamente estadísticas de uso e informes sobre fallos a "Google":** permite que Chrome envíe a "Google" estadísticas de uso e informes sobre fallos automáticamente para ayudarnos a priorizar las funciones y las mejoras en las que tenemos que trabajar. Obtén más información sobre las estadísticas de uso y los informes sobre fallos.

- **Enviar una solicitud de no seguimiento con tu tráfico de navegación:** puedes incluir una solicitud de no seguimiento con tu tráfico de navegación. No obstante, muchos sitios *web* seguirán recopilando y utilizando tus datos de navegación para mejorar la seguridad, proporcionar contenido, servicios, anuncios y recomendaciones sobre sus sitios *web*, y generar estadísticas de informes.

5.1.2 Navegador Mozilla Firefox (Versión 3.6.22)

A pesar de los problemas iniciales que tuvo Firefox en su lanzamiento, una versión con todas las correcciones necesarias fue lanzada convirtiendo a Firefox en uno de los navegadores más seguros del mercado. Los desarrolladores de Firefox trabajan continuamente para corregir las

vulnerabilidades detectadas teniendo una tasa de corrección del 100%, lo cual significa que la totalidad de las vulnerabilidades son corregidas aunque con el transcurso del tiempo siguen apareciendo nuevas vulnerabilidades que son tratadas y solucionadas.

El usuario a través de los ajustes seleccionados en la configuración del navegador puede aumentar el nivel de seguridad respecto de la configuración por defecto que proporciona el navegador.

Para acceder a la configuración del navegador Mozilla Firefox el usuario deberá seleccionar:

Menú> Herramientas> Opciones> Seguridad

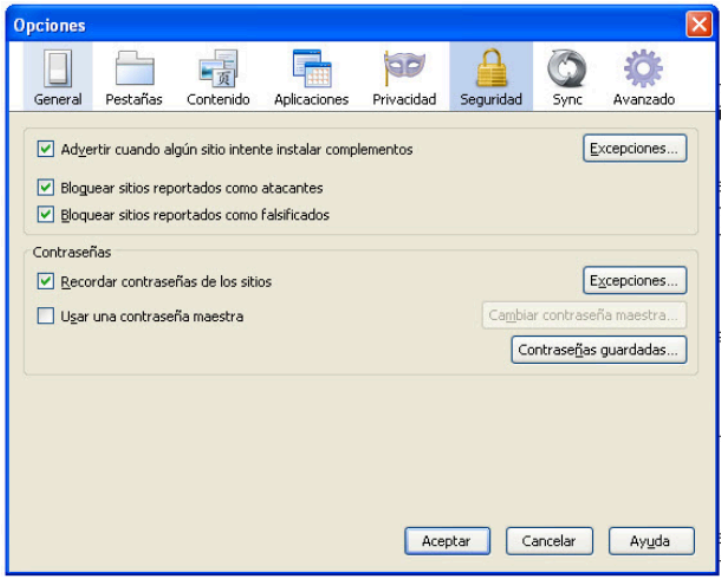

Figura 8 – Opciones de Seguridad del navegador Mozilla Firefox

Si se selecciona la opción de privacidad se muestra la siguiente pantalla:

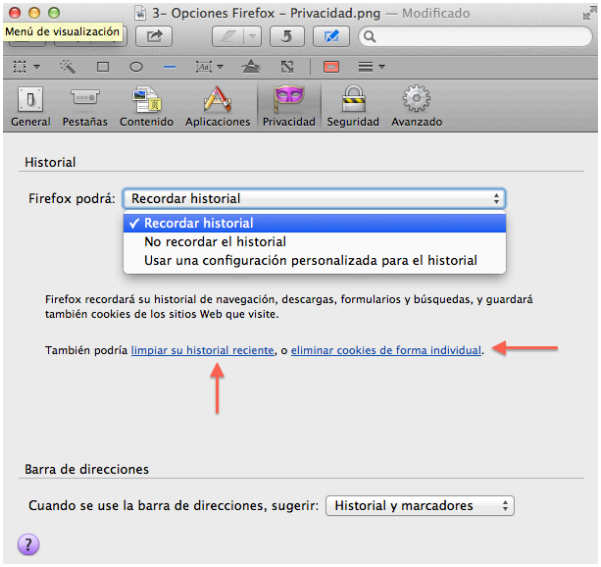

Figura 9 – Opciones de Privacidad del navegador Mozilla Firefox

Al clicar sobre “Recordar historial” el navegador mostrará un desplegable con las opciones que se muestran en la figura 9. En la parte central de la pantalla se pueden observar las opciones “limpiar su historial reciente” o “eliminar *cookies* de forma individual”.

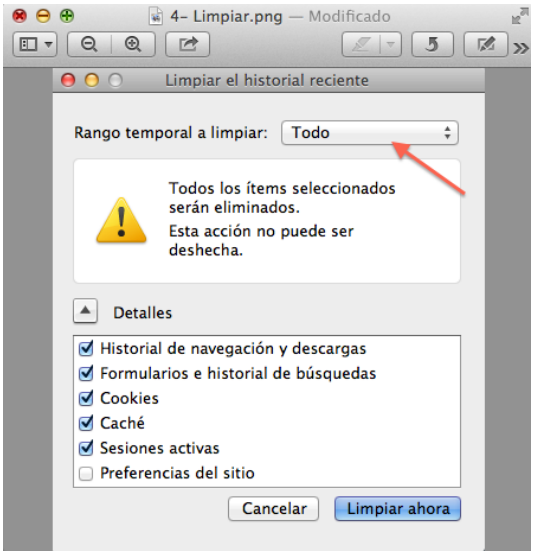

Figura 10 – Opción Limpiar historial reciente del navegador Mozilla Firefox

Si se clica sobre el enlace “limpiar su historial reciente” se mostrará la pantalla de la figura 10 y permitirá al usuario eliminar: “Todo”, que implicará eliminar todo el historial de los elementos seleccionados sin tener en cuenta el tiempo que llevan almacenados; “Última hora”, con lo cual se eliminarán elementos del historial seleccionados de la última hora; “Última dos horas”, con lo cual se eliminarán elementos del historial seleccionados en las últimas dos horas; “Última cuatro horas”, lo que implicará eliminar elementos seleccionados de las últimas cuatro horas; y “Hoy”, con lo cual se eliminarán todos los elementos del historial seleccionados en el día de hoy.

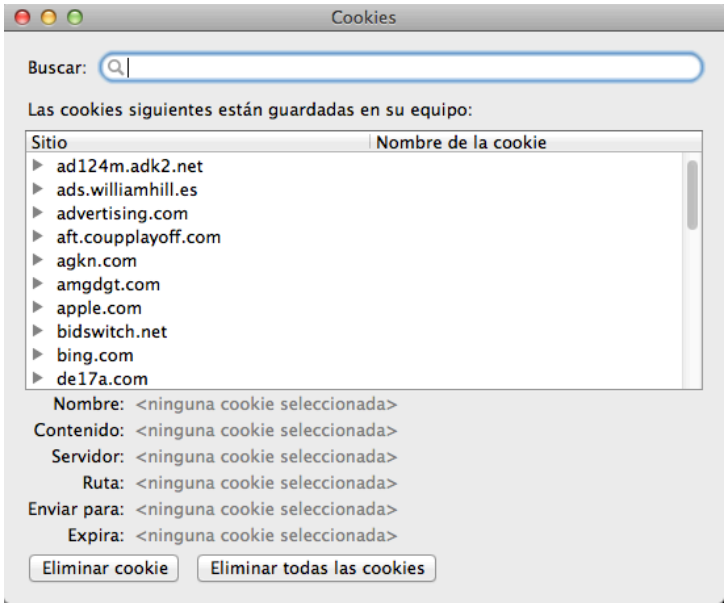

Figura 11 – Opción Eliminar *cookie* de forma individual del navegador Mozilla Firefox

Al seleccionar “eliminar *cookies* de forma individual” el navegador proporcionará la pantalla mostrada en la figura 11 y el usuario podrá elegir entre las opciones de “Eliminar *cookie*” mediante la cual se eliminará la *cookie* seleccionada, o “Eliminar todas las *cookies*” mediante la cual, al clicar sobre el botón, eliminará todas las *cookies* almacenadas.

Si seleccionamos uno de los sitios que han almacenado *cookies*, mostrará todas las *cookies* que se han almacenado de ese sitio en concreto. Si el usuario se sitúa sobre una de las *cookies* obtendrá toda la información de esta. La información obtenida es: Nombre, Contenido, Servidor, Ruta, Enviar para y Expira. En la figura 12 se puede ver un ejemplo de una *cookie* almacenada por el sitio "Google".

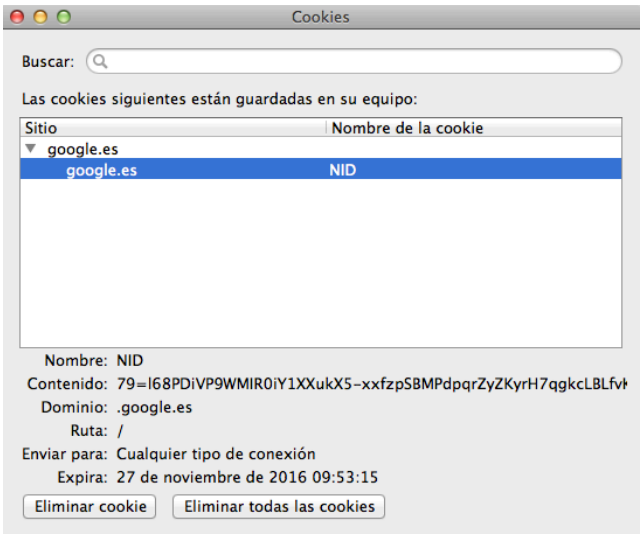

Figura 12 – Ejemplo información almacenada de una *cookie* por el navegador Mozilla Firefox

Si en la pantalla de privacidad se selecciona "No recordar el historial", el navegador mostrará la pantalla mostrada en la figura 13 y permitirá al usuario seleccionar "Limpiar todo el historial". Las opciones que proporcionará la opción de "Limpiar todo el historial" son las mismas que se han descrito anteriormente.

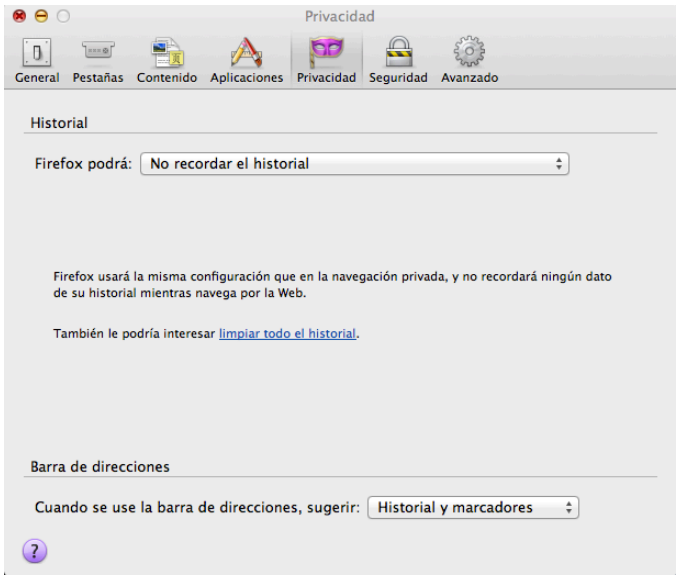

Figura 13 – Opción No recordar el historial del navegador Mozilla Firefox

Por último, si en la pantalla de privacidad se selecciona "Usar una configuración personalizada para el historial", el navegador mostrará la pantalla mostrada en la figura 14 y permitirá al usuario seleccionar varias opciones. La primera opción permite al usuario "Abrir automáticamente Firefox en una sesión de navegación privada". En el caso de que el usuario seleccione esta opción, cada vez que abra el navegador estará utilizando una navegación privada que no registrará el historial de búsquedas, de descargas, ni de formularios, y por tanto

no será necesario limpiar el historial cuando Firefox se cierre. Sin embargo, si el usuario no selecciona “Abrir automáticamente Firefox en una sesión de navegación privada”, podrá seleccionar qué quiere recordar. Las opciones de recordar el historial son: “Búsqueda al menos un número seleccionado de días”, “Descargas” y “Formularios y búsquedas”.

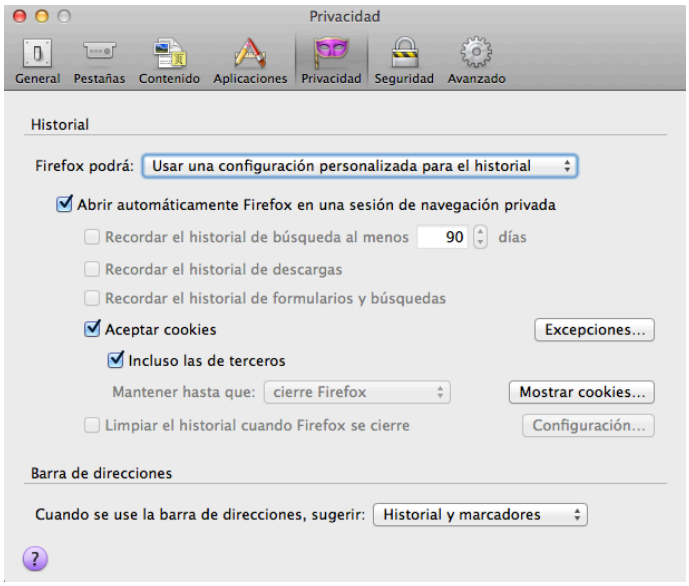

Figura 14 – Opción Configuración personalizada para el historial navegador Mozilla Firefox

Adicionalmente, el usuario podrá seleccionar “Limpiar el historial cuando Firefox se cierre”. Las opciones que el usuario puede elegir en este caso son las que se muestran en la figura 15.

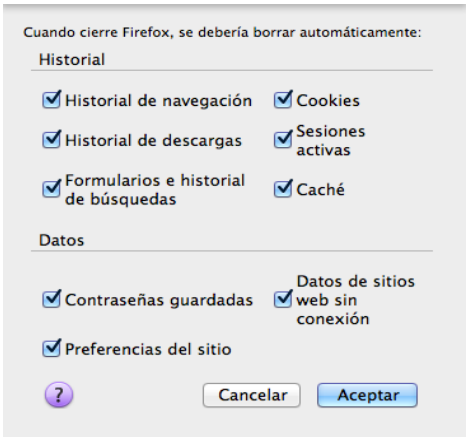

Figura 15 – Opción Limpiar el historial al cerrar navegador Mozilla Firefox

Independientemente de la configuración seleccionada por el usuario en relación a los elementos que desea recordar del historial, este podrá configurar el tratamiento que el navegador realizará de las *cookies*. Las opciones posibles son: No aceptar *cookies*, Aceptar *cookies* sin excepciones y Aceptar *cookies* con excepciones. Si se selecciona “Aceptar *cookies”*, el usuario podrá decidir si quiere aceptar *cookies* de terceros o no. Por último, el usuario podrá decidir la duración de almacenaje de la *cookie* por el navegador. Las opciones disponibles son “Mantener hasta” que: “Caduquen”, “Cierre Firefox” o “Preguntar siempre”. La última opción implicará que siempre que un sitio desee instalar una *cookie* preguntará al usuario, tal como muestra el mensaje de la figura 16, qué quiere hacer con la *cookie*.

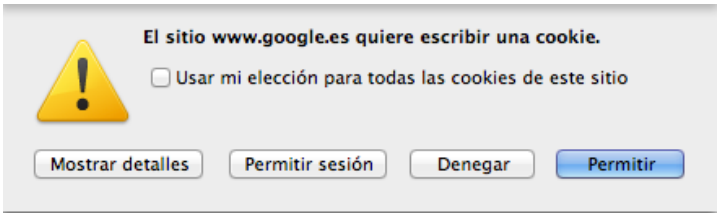

Figura 16 – Opción preguntar tratamiento a la *cookie* del navegador Mozilla Firefox

El navegador Firefox permite al usuario gestionar las excepciones en relación al tratamiento que debe hacer de las *cookies*. Tal y como muestra la pantalla de la figura 17, el usuario podrá especificar los sitios *web* que nunca o siempre podrán utilizar *cookies* mediante las opciones de: Bloquear, Permitir durante la sesión o Permitir.

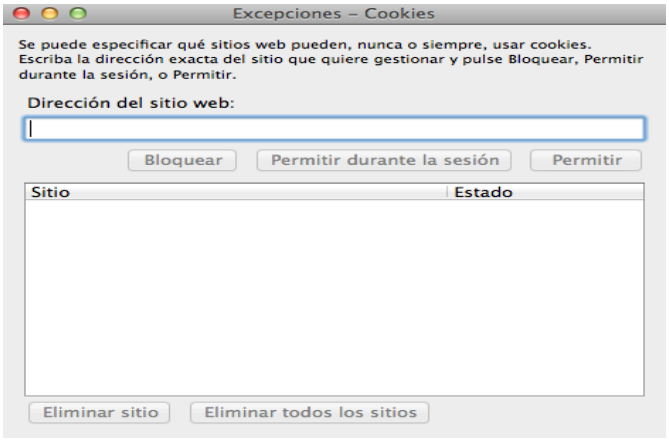

Figura 17 – Opción gestión excepciones *cookies* Mozilla Firefox

El usuario al clicar sobre la opción "Mostrar *cookies*" que aparece en la figura 14, se presenta la misma pantalla que el navegador proporciona al seleccionar "Recordar *cookies*" y clicar sobre el enlace "Eliminar *cookies* de forma individual".

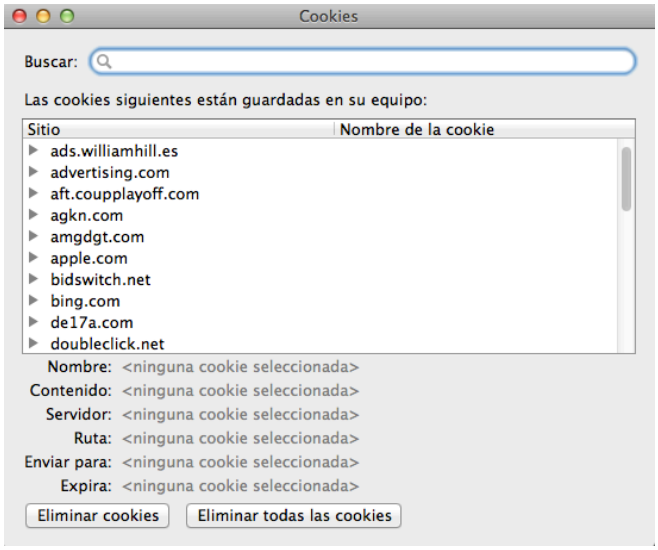

Figura 18 – Opción mostrar *cookies* Mozilla Firefox

5.1.3 Navegador Safari (Versión 9.1.1)

Este navegador es el más utilizado por los usuarios de Apple. Está considerado el mejor navegador que el usuario puede utilizar si utiliza un Mac, ya que es más rápido, eficiente y por lo tanto carga los contenidos a gran velocidad provocando que la batería del portátil dure más. Este navegador ha implementado medidas de seguridad necesarias para salvaguardar la información de los usuarios. Por ejemplo, ha implementado la opción de navegación privada mediante la cual Safari no recuerda las páginas que el usuario ha visitado, tampoco el historial de búsquedas ni los datos de auto-relleno. Las pestañas de navegación privada son independientes, de forma que ningún sitio pueda acceder a las *cookies* de otro sitio.

Safari fue el primer navegador que bloqueó por defecto las *cookies* de terceros de forma que evita que los sitios *web* de terceros almacenen datos en la caché, en el sistema o la base de datos. Al igual que otros navegadores, los desarrolladores de Safari trabajan continuamente para corregir las vulnerabilidades detectadas. También igual como ocurre con otros navegadores disponibles en el mercado, el usuario de Safari, a través de los ajustes seleccionados en la configuración del navegador, puede aumentar el nivel de seguridad que se aplica cuando el usuario está navegando por Internet.

Este estudio se centra en las opciones de configuración que ofrece el navegador sobre la privacidad y más concretamente sobre la gestión de las *cookies*. Para acceder a la configuración del navegador seleccionaremos:

Safari> Preferencias> Privacidad

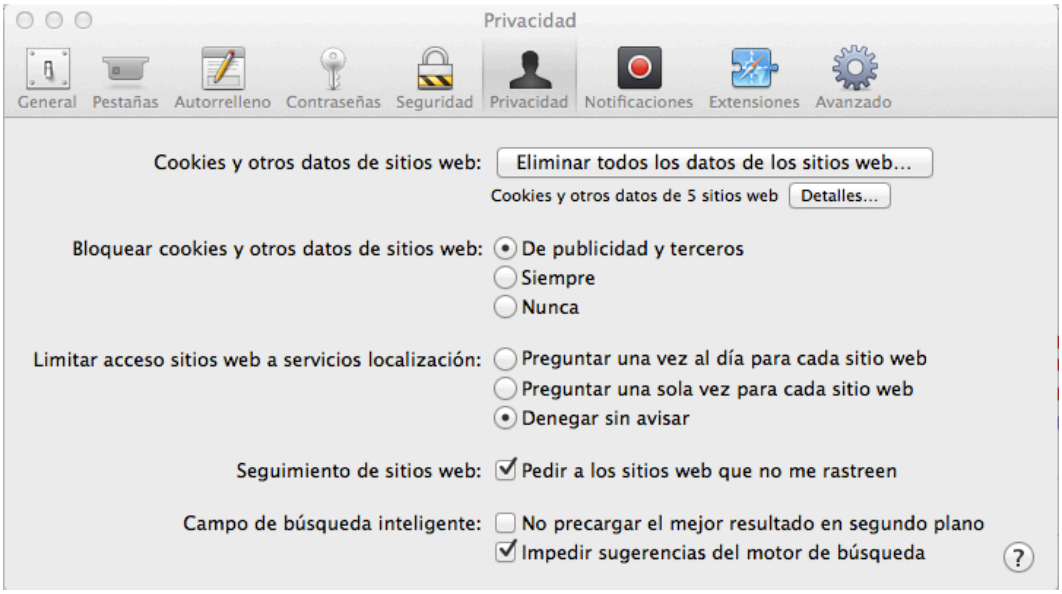

Figura 19 – Opción mostrar *cookies* del navegador Safari

La ventana de privacidad del menú de configuración de preferencias del navegador nos permite principalmente gestionar las *cookies*, limitar el acceso a los sitios *web* a servicios de localización y evitar el seguimiento de los sitios *web*.

Las opciones proporcionadas por el navegador respecto de las *cookies* y otros datos de sitios *web* que almacena el navegador pueden verse en la figura 19 y son:

- *Cookies* y otros datos de sitios *web*: Si se clica sobre "Eliminar todos los datos de los sitios *web*" el usuario deberá confirmar que desea eliminar todos los datos guardados en el ordenador por los sitios *web*.

- Detalles: Si se clica sobre “Detalles” se mostrará la pantalla de la figura 20 y el usuario puede ver qué sitios *web* han almacenado *cookies* o datos y puede eliminarlos todos o eliminarlos uno a uno.

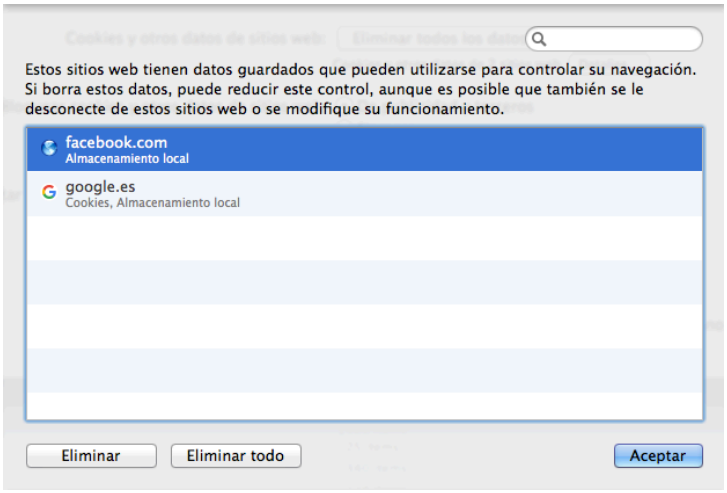

Figura 20 – Opción Detalles del navegador Safari

El usuario puede cambiar la manera en que se bloquean las *cookies* y los datos de sitios *web*. Las opciones disponibles son las siguientes:

- Bloquear *cookies* y otros datos de sitios *web* de publicidad y terceros.
- Bloquear *cookies* y otros datos de sitios *web* siempre.
- Bloquear *cookies* y otros datos de sitios *web* nunca.

El usuario puede adicionalmente definir el límite de acceso de los sitios *web* a los servicios de localización. Las opciones disponible son las siguientes:

- Permitir servicios de localización y preguntar una vez al día para cada sitio *web*.
- Permitir servicios de localización y preguntar una sola vez para cada sitio *web.*
- Denegar servicios de localización sin avisar.

El usuario puede seleccionar que no desea que se rastreen sus actividades, pero a pesar de que el usuario seleccione esta opción, no queda garantizado que los sitios *web* no obtengan información desde el navegador sin su autorización. Existen varios sitios *web* que se comprometen a no realizar un rastreo de las actividades de un usuario si este ha indicado expresamente que no desea que se realice tal rastreo, pero esta opción es voluntaria y no de obligado cumplimiento por parte de los sitios.

Por último, el usuario puede optar por realizar una navegación privada, la cual se activa accediendo al menú de Safari y clicando sobre la pestaña “Navegación Privada…”. El navegador Safari en este caso puede mantener el historial de navegación en privado y no recordará ni las páginas que visita, ni su historial de búsqueda, ni la información de auto-relleno. Para finalizar la Navegación Privada deberá acceder de nuevo al menú de Safari y clicar sobre “ ✓ Navegación Privada…”.

5.2 Análisis del comportamiento de los navegadores

Una vez analizadas las opciones de configuración de los navegadores respecto de la privacidad, se ha procedido a aplicar las diferentes opciones de seguridad de los navegadores al visitar tres sitios web diferentes. Tal y como se comentó en la introducción de este capítulo 5, los sitios *web* que se han utilizado para realizar el análisis han sido “El País”, “Facebook” y “Amazon”. A continuación se describen los resultados obtenidos con cada opción de configuración de los navegadores al visitar cada uno de los sitios *web*.

Los tres navegadores han sido configurados de forma que la página de inicio que muestran al abrirlos sea la página de "Google".

El análisis realizado proporciona detalles de las *cookies* que han sido almacenadas por los navegadores en el momento de realizar las pruebas. Las *cookies* almacenadas pueden variar incluso utilizando un determinado navegador con una configuración determinada y visitando el mismo sitio.

5.2.1 Navegador Google Chrome – Sitio *web* "El País"

En este apartado 5.2.1 se utilizará el navegador Google Chrome y se analizarán los resultados obtenidos al ir seleccionando las diferentes opciones que el navegador nos permite respecto de la privacidad a través de la configuración del contenido.

Las tres primeras pruebas se realizarán teniendo en común que no se bloqueen los datos de los sitios y las *cookies* de terceros y no permitiendo que ningún sitio ejecute JavaScript. Las pruebas se diferenciarán en el tratamiento que el navegador realizará sobre las *cookies* y las opciones de configuración que se analizarán serán en primer caso "Permitir que se almacenen datos locales (recomendado)", el segundo caso "Conservar datos locales sólo hasta que el usuario salga del navegador" y, por último, "No permitir los datos de sitios y las *cookies* de terceros".

5.2.1.1 Permitir que se almacenen datos locales (recomendado) - No bloquear los datos de sitios y las *cookies* de terceros - No Permitir que ningún sitio ejecute JavaScript

Al abrir el navegador aparece una *cookie* e información adicional de "Google", ya que tal y como se ha mencionado el navegador tiene configurada la página de "Google" como página de inicio de la navegación del usuario.

Al acceder al sitio "El País" no se muestran las imágenes asociadas a las noticias en la portada al no tener activado JavaScript y aparecen almacenadas las siguientes *cookies*: "elpais", "207.net", "doubleclick.net", "prisa.com2" y "scorecardresearch.com". Las *cookies* de "elpais" y "prisa.com" están vinculadas directamente con el sitio *web* visitado, pero las *cookies* "207.net", "doubleclick.net" y "scorecardresearch.com" son *cookies* de terceros y cada una de ellas tienen el siguiente objetivo:

- Doubleclick.net: Empresa de publicidad, adquirida por "Google". Rastrea las actividades del usuario, registra los anuncios comerciales visitados mientras se navega.
- 207.net: Rastrea las actividades del usuario y obtiene información de los hábitos del mismo.
- Scorecardresearch.com: Recopila datos que ayudan a las empresas a suministrar productos y servicios que satisfagan las necesidades del usuario a través del uso de *cookies*.

Al navegar por "El País" se obtienen otras *cookies* como por ejemplo, "youtube" y "i.ytimg.com" a pesar de no haber clicado sobre ningún link que esté vinculado a Youtube ni al servidor de vistas en miniatura Youtube. Hay que mencionar que Youtube es una compañía que fue adquirida por "Google" con lo cual todas estas *cookies* pertenecen al mismo grupo empresarial.

Al cerrar el navegador y volverlo a abrir, aparecen todas las *cookies* persistentes que han sido almacenadas por el navegador. Las *cookies* de sesión "elpais" y "youtube.com" han sido eliminadas.

Tal y como se ha comentado, al no permitir JavaScript, al acceder al sitio *web* de "El País" no aparecen las imágenes de la portada y tampoco permite la descarga de los videos mostrados en los artículos.

5.2.1.2 Conservar datos locales sólo hasta salir del navegador - No bloquear los datos de sitios y las *cookies* de terceros - No Permitir que ningún sitio ejecute JavaScript

Inicialmente, el comportamiento del navegador es el mismo que en el caso anterior. Al abrir el navegador la *cookie* que aparece es la de "Google", al acceder al sitio *web* de "El País" se obtienen las mismas *cookies* que anteriormente, y al navegar el navegador va almacenando nuevas *cookies*.

En este caso al haber seleccionado en el menú de configuración de contenido del navegador "Conservar datos locales sólo hasta que salgas del navegador", el navegador ha procedido a borrar todas las *cookies* tanto persistentes como de sesión una vez que el usuario ha cerrado la sesión de navegación. En este caso al abrir el navegador, la única *cookie* que aparece es la de "Google", ya que es una sesión nueva de navegación del usuario y tal y como hemos comentado anteriormente "Google" es la página inicial del navegador.

5.2.1.3 No permitir que se guarden datos de los sitios - No bloquear los datos de sitios y las *cookies* de terceros - No Permitir que ningún sitio ejecute JavaScript

En este caso la única diferencia con los casos anteriores es que se ha seleccionado "No permitir que se guarden datos de los sitios" en las opciones de configuración de contenido del navegador. Las *cookies* que el navegador iba almacenando en el ordenador en los casos anteriores ahora no son almacenadas, y por tanto el navegador, al seleccionar esta opción, no permite que ni las *cookies* persistentes ni las de sesión sean almacenadas por el navegador. Así, la navegación por el sitio *web* de "El País" sigue siendo igual que en los dos casos anteriores con la única diferencia de que no se le permite al navegador que almacene ningún tipo de *cookie*.

A continuación se mostrarán los resultados obtenidos tras ir modificando las opciones de configuración del navegador respecto de la configuración del contenido, siguiendo el mismo proceso que en los tres apartados anteriores con la única variación de configuración del navegador que ahora se ha seleccionado "Bloquear los datos de sitios y las *cookies* de terceros".

5.2.1.4 Permitir que se almacenen datos locales (recomendado) - Bloquear los datos de sitios y las *cookies* de terceros - No Permitir que ningún sitio ejecute JavaScript

Este caso es muy semejante al expuesto en el apartado 5.2.1.1. La única diferencia es que se ha marcado la casilla por la cual se bloquean los datos de sitios y las *cookies* de terceros.

Inicialmente, no se aprecia ningún cambio ya que "Google" vuelve a almacenar una *cookie* antes de acceder a ningún sitio *web*. Al acceder a "El País" sólo son almacenadas la *cookie* de "Google" y tres de "El País", dos de ellas de sesión y una persistente, con lo cual si comparamos esta opción con las pruebas realizadas en el aparatado 5.2.1.1, se consigue que las *cookies* de terceros de "207.net", "doubleclick.net" y "scorecardresearch.com" no sean almacenadas por el navegador.

Si se sigue navegando por el sitio *web* "El País", el navegador va almacenando *cookies* pero en este caso sólo del sitio "El País". Las *cookies* que siguen almacenadas, una vez se ha salido del navegador y se vuelve acceder a él, son la *cookie* de "Google" y una única *cookie* persistente de "El País".

Una vez realizada la prueba con las opciones del navegador definidas en este apartado, se puede observar que esta configuración es mejor que la definida en el apartado 5.2.1.1, ya que la navegación de cara al usuario ha sido la misma y sin embargo se ha evitado que el navegador almacene *cookies* de terceros, las cuales no mejoran la navegación de los usuarios pero sí que pueden proporcionar información privada del usuario a sitios terceros.

5.2.1.5 Conservar datos locales sólo hasta salir del navegador - Bloquear los datos de sitios y las *cookies* de terceros - No Permitir que ningún sitio ejecute JavaScript

Este caso es muy semejante al apartado 5.2.1.2 anteriormente expuesto. La única diferencia es que se ha marcado la casilla por la cual se bloquea los datos de sitios y las *cookies* de terceros.

Las *cookies* que son almacenadas por el navegador son las mismas que en el caso anterior descrito en el apartado 5.2.1.4 ya que el navegador guarda una *cookie* de "Google" y tres *cookies* de "El País". Adicionalmente, al navegar no se detectan diferencias respecto del almacenamiento de *cookies* del expuesto en el punto 5.2.1.4.

Al cerrar la sesión de navegación y volver a abrir una nueva, se detecta que todas las *cookies* que fueron almacenadas durante la navegación anterior han sido eliminadas, con lo cual esta opción de configuración es mejor que la expuesta en el caso anterior 5.2.1.4, ya que el usuario puede acceder a los contenidos sin ningún tipo de problema y evita que las *cookies* persistentes sean guardadas entre una sesión y otra.

5.2.1.6 No permitir que se guarden datos de los sitios - Bloquear los datos de sitios y las *cookies* de terceros - No Permitir que ningún sitio ejecute JavaScript

En este caso no se detecta ningún tipo de diferencia en cuanto a la navegación y el almacenamiento de *cookies* por parte de navegador entre las opciones seleccionadas de configuración en este caso y las opciones seleccionadas en el punto 5.2.1.3, ya que en ambos casos no permiten que se guarden datos de los sitios independientemente de que sean del sitio *web* que se visita o de terceros.

A continuación se mostrarán los resultados obtenidos tras ir modificando las opciones de configuración del navegador respecto de la configuración del contenido, siguiendo el mismo proceso que en los apartados 5.2.1.1, 5.2.1.2 y 5.2.1.3 con la única variación de configuración del navegador que ahora se ha seleccionado en el apartado JavaScript "Permitir que todos los sitios ejecuten JavaScript (recomendado)".

5.2.1.7 Permitir que se almacenen datos locales (recomendado) - No bloquear los datos de sitios y las *cookies* de terceros - Permitir que todos los sitios ejecuten JavaScript (recomendado)

En este caso al abrir navegador este guarda la *cookie* de "Google", tal y como ocurría en el supuesto del punto 5.2.1.1. A continuación se accede al sitio "El País" y en este caso al permitir que se ejecute JavaScript aparecen en la portada del diario digital numerosas imágenes, que en el supuesto 5.2.1.1 no aparecían. Al permitir que los sitios ejecuten JavaScript implica que muchas más *cookies* sean almacenadas por el navegador en el ordenador. Estas *cookies* mayoritariamente son *cookies* de terceros cuyo objetivo es publicitar productos y realizar un rastreo de las actividades del usuario. El número de *cookies* que son almacenadas por el sitio *web* visitado "El País" también se incrementan.

Al cerrar el navegador y volver a abrirlo, se detecta que se ha incrementado el número de *cookies* persistentes almacenadas por el navegador. Este hecho provoca que muchos más sitios *web* puedan obtener información de la navegación que es efectuada por el usuario, lo cual implica un mayor riesgo respecto de la privacidad del usuario.

Cabe destacar que al permitir que los sitios ejecuten JavaScript, aparece el mensaje por el cual el sitio *web* informa al usuario del uso y tratamiento que hace de las *cookies*. El mensaje que muestra es el siguiente: "Uso de *Cookies*. Utilizamos "*Cookies*" propias y de terceros para elaborar información estadística y mostrarle publicidad personalizada a través del análisis de su navegación. Si continúa navegando acepta su uso. Más información y política de *cookies*". Este mensaje se muestra en la portada del diario digital y si el usuario

continúa la navegación, el mensaje no vuelve a aparecer y el sitio *web* entiende que acepta las condiciones impuestas por este. Es lo que se explicó en el apartado 4.3: la denominada aceptación implícita.

Por último, si se compara este supuesto con el descrito anteriormente en el apartado 5.2.1.1, el usuario en este caso además de poder visualizar las imágenes relacionadas con las noticias que proporciona el sitio *web* también puede detectar el aumento en el número de anuncios que se le muestran al navegar por el sitio.

5.2.1.8 Conservar datos locales sólo hasta salir del navegador - No bloquear los datos de sitios y las *cookies* de terceros - Permitir que todos los sitios ejecuten JavaScript (recomendado)

Inicialmente el comportamiento del navegador es el mismo que en los casos anteriores ya que al abrir el navegador la única *cookie* que se almacena es la de "Google". En el momento que se visita el sitio *web* y se accede a la portada ocurre exactamente igual que el caso anterior 5.2.1.7: numerosas *cookies* son almacenadas por el navegador y muestra el mensaje de la política de *cookies* nada más acceder al sitio *web*. A medida que se navega, el navegador va almacenando más *cookies* tanto del sitio "El País" como de terceros.

Al cerrar el navegador y volver a abrirlo se detecta que todas las *cookies* que fueron almacenadas durante la navegación anterior han sido eliminadas. Por tanto, esta opción de "Conservar datos locales sólo hasta salir del navegador" es más recomendable ya que no permite almacenar ni utilizar las *cookies* almacenadas por los sitios *web,* y por tanto proporcionar información acerca de los sitios visitados por el usuario a terceros. La única información que obtendrán los sitios *web* será toda aquella debida a las visitas por los distintos sitios *web* que realiza el usuario mientras el navegador está abierto.

5.2.1.9 No permitir que se guarden datos de los sitios - No bloquear los datos de sitios y las *cookies* de terceros - Permitir que todos los sitios ejecuten JavaScript (recomendado)

El único cambio respecto del caso anterior es que en este caso se ha seleccionado "No permitir que se guarden datos de los sitios". Igual como ocurría en los casos anteriores descritos en el supuesto 5.2.1.3 y en el 5.2.1.6, a medida que se navega no se almacena ningún tipo de información por parte del navegador.

El hecho de no guardar ninguna *cookie* implica que el navegador tampoco almacena la *cookie* que utiliza para mostrar la política del sitio *web*, con lo cual a medida que el usuario visita cada una de las páginas correspondientes a las noticias, el sitio *web* vuelve a mostrar el mensaje de la política del sitio *web*. Esta configuración proporciona más privacidad que los dos últimos casos expuestos al no almacenar ningún tipo de información, pero el hecho de mostrar en cada página la política del sitio *web* puede ser molesto para el usuario.

A continuación se mostrarán los resultados obtenidos tras ir modificando las opciones de configuración del navegador respecto de la configuración del contenido, siguiendo el mismo proceso que en los apartados 5.2.1.4, 5.2.1.5 y 5.2.1.6 con la única variación de configuración del navegador que ahora se ha seleccionado en el apartado JavaScript "Permitir que todos los sitios ejecuten JavaScript (recomendado)".

5.2.1.10 Permitir que se almacenen datos locales (recomendado) - Bloquear los datos de sitios y las *cookies* de terceros - Permitir que todos los sitios ejecuten JavaScript (recomendado)

La configuración realizada en este caso es igual que la del caso 5.2.1.7 pero se ha seleccionado que se bloqueen a los datos de sitios y las *cookies* de terceros, con lo cual al acceder a la portada del sitio *web* "El País" se puede observar que las únicas *cookies* almacenadas por el navegador corresponden a la *cookie* de "Google" y las *cookies* de "El

País". El resto de *cookies* de terceros no son almacenadas, lo cual implica que sitios terceros no puedan obtener información de los hábitos de navegación de los usuarios.

Al cerrar una sesión del navegador y volver a acceder a él, se puede observar que las *cookies* que son almacenadas sólo son aquellas de sitios visitados directamente por el usuario. En este caso se siguen mostrando mensajes publicitarios pero sólo se almacenarán *cookies* de sitios terceros si el usuario accede al enlace del sitio que se publicita.

5.2.1.11 Conservar datos locales sólo hasta salir del navegador - Bloquear los datos de sitios y las *cookies* de terceros - Permitir que todos los sitios ejecuten JavaScript (recomendado)

La única diferencia que se aprecia respecto del caso anterior 5.2.1.10 es que igual como ocurría en casos descritos anteriormente, una vez se cierra el navegador toda la información almacenada es borrada, no permitiendo que los sitios obtengan información del usuario de sesiones de navegación anteriores.

5.2.1.12 No permitir que se guarden datos de los sitios - Bloquear los datos de sitios y las *cookies* de terceros - Permitir que todos los sitios ejecuten JavaScript (recomendado)

Esta opción de configuración es prácticamente igual que la configuración seleccionada en el apartado 5.2.1.9, ya que en ambos casos no se permite que se guarden datos de los sitios tanto si se selecciona adicionalmente bloquear o no bloquear los datos de sitios y *cookies* de terceros. Por tanto, el resultado de la navegación es el mismo que el descrito en el apartado 5.2.1.9., con lo cual a medida que el usuario visita cada una de las páginas correspondientes a las noticias, el sitio *web* vuelve a mostrar el mensaje de la política del sitio *web*.

A continuación se mostrarán los resultados obtenidos tras ir modificando las opciones de configuración del navegador respecto de la configuración del contenido, siguiendo el mismo proceso que en los apartados 5.2.1.7, 5.2.1.8 y 5.2.1.9 con la única variación de configuración del navegador respecto de esos casos que ahora se ha seleccionado en el apartado Ubicación "Permitir que todos los sitios realicen un seguimiento de la ubicación física del usuario". Esta opción permitirá a algunos sitios *web* proporcionar información personalizada a los usuarios ya que sus servicios pueden variar dependiendo de la ubicación del usuario.

5.2.1.13 Permitir que se almacenen datos locales (recomendado) – No bloquear los datos de sitios y las *cookies* de terceros - Permitir que todos los sitios ejecuten JavaScript (recomendado) - Permitir que todos los sitios realicen un seguimiento de tu ubicación física

En relación con los resultados obtenidos con la configuración seleccionada en el supuesto 5.2.1.7, no se detecta ninguna variación respecto del almacenamiento de las *cookies* por parte del navegador. Al ser el resultado obtenido de la navegación el mismo, la opción de habilitar o no al navegador para que haga un seguimiento de la ubicación física del usuario para poderle proporcionar los servicios ofrecidos, no proporciona nada adicional al usuario al visitar el sitio "El País", pero puede proporcionar información a los sitios sobre la ubicación física, lo cual implica obtener información privada de los usuarios.

5.2.1.14 Conservar datos locales sólo hasta salir del navegador – No bloquear los datos de sitios y las *cookies* de terceros - Permitir que todos los sitios ejecuten JavaScript (recomendado) - Permitir que todos los sitios realicen un seguimiento de tu ubicación física

El comportamiento del navegador respecto del almacenamiento de *cookies* es el mismo que en el supuesto anterior 5.2.1.13 y por tanto, el usuario al acceder al sitio "El País" no

obtiene nada adicional que facilite su navegación, y tampoco es un requisito necesario para que el sitio *web* pueda proporcionar sus servicios.

5.2.1.15 No permitir que se guarden datos de los sitios – No bloquear los datos de sitios y las *cookies* de terceros - Permitir que todos los sitios ejecuten JavaScript (recomendado) - Permitir que todos los sitios realicen un seguimiento de tu ubicación física

En esta última prueba, realizada con el navegador Google Chrome, se han obtenido exactamente los mismos resultados que en los supuestos anteriores 5.2.1.3, 5.2.1.6, 5.2.1.9 y 5.2.1.12 en los que independientemente del resto de opciones seleccionadas, no se permite que se guarden datos de los sitios ni durante toda la navegación, ni cuando el navegador se cierra.

Tras realizar un análisis sobre el comportamiento del navegador Google Chrome al seleccionar unas opciones determinadas relacionadas con la privacidad, al configurar el contenido tanto de las *cookies* como JavaScript o Ubicación, se han obtenido los siguientes resultados:

- Al deshabilitar JavaScript no es posible visualizar las imágenes relacionadas con los artículos ni anuncios publicitarios que pueden proporcionar el sitio "El País", con lo cual es recomendable habilitar del menú de configuración de contenido JavaScript para "Permitir que todos los sitios ejecuten JavaScript (recomendado)" a pesar de que almacene muchas más *cookies* en el navegador.
- La opción de configuración del contenido respecto de la ubicación no proporciona una mejora en la navegación para el usuario y al no ser requerido por el sitio *web* "El País" para poder proporcionar sus servicios, se recomienda "No permitir que ningún sitio pueda hacer un seguimiento de tu ubicación física".
- Respecto de la opción de configuración de contenido sobre las *cookies* es recomendable seleccionar "Bloquear los datos de sitios y las *cookies* de terceros", ya que esta opción en caso de no ser marcada permite a sitios *web* terceros obtener información de la navegación del usuario, afectando a la privacidad de estos.
- Por último, en relación a la configuración del contenido sobre las *cookies*, de las tres opciones posibles que ofrece el navegador, teniendo en cuenta que se han bloqueado los datos de sitios y las *cookies* de terceros, son:

    - "No permitir que se guarden datos de los sitios" lo cual implicaba una repetición del mensaje de la política sobre las *cookies* que tiene establecido el sitio *web* "El País" al ir navegando entre las páginas.
    - "Permitir que se almacenen datos locales (recomendado)" que en este caso el navegador guardará sólo *cookies* de sitios *web* que se han visitado, aunque las *cookies* persistentes guardadas por los sitios *web* se mantienen en el navegador hasta la fecha de caducidad de la *cookie*.
    - "Conservar datos locales sólo hasta que el usuario salga del navegador" y por tanto, borrar todas las *cookies* de sesión o persistentes al cerrar el navegador.

    El usuario puede seleccionar cualquiera de las tres opciones, las cuales si son listadas por orden de mayor restricción a menor respecto de la posibilidad de que las *cookies* sean almacenadas, y por tanto proporcionando de más a menos privacidad al usuario: la primera opción "No permitir que se guarden datos de los sitios", la segunda opción "Conservar datos locales sólo hasta que el usuario salga del navegador" y la tercera opción "Permitir que se almacenen datos locales (recomendado)".

    La recomendación sería utilizar la opción de "Conservar datos locales sólo hasta que el usuario salga del navegador" a pesar de que se pueda perder comodidad en la navegación, ya que seleccionando esta opción se evita la repetición de la política del sitio en relación a las *cookies* y elimina todo tipo de *cookies* al cerrar el navegador.

5.2.2 Navegador Google Chrome – Sitio *web* "Facebook"

La metodología que se ha realizado para analizar el comportamiento del navegador Google Chrome al visitar el sitio *web* "Facebook" ha sido la misma que en el caso anterior en el que se realizaba un análisis al visitar el sitio *web* "El País". Sin embargo, "Facebook" requiere que esté habilitado JavaScript, por lo que de entrada en el menú de configuración de contenido del navegador en el apartado JavaScript se ha tenido que seleccionar "Permitir que todos los sitios ejecuten Java Script (recomendado)". El navegador, en la opción de configuración, ya indica esta opción como recomendada. Este hecho ha provocado que el número de casos que deben analizarse al visitar el sitio *web* "Facebook" sea menor en comparación con los realizados en el apartado 5.2.1 al visitar el sitio *web* "El País".

Las dos primeras pruebas se realizarán teniendo en común que no se bloqueen los datos de los sitios y las *cookies* de terceros, y permitiendo que todos los sitios ejecuten JavaScript. Las opciones de configuración del navegador que se analizarán se diferencian en el tratamiento que el navegador realizará sobre las *cookies*. Así, en el primer caso se seleccionará "Permitir que se almacenen datos locales (recomendado)", en el segundo caso "Conservar datos locales sólo hasta que el usuario salga del navegador" y en el último caso "No permitir que se guarden datos de los sitios".

5.2.2.1 Permitir que se almacenen datos locales (recomendado) - No bloquear los datos de sitios y las *cookies* de terceros - Permitir que todos los sitios ejecuten JavaScript (recomendado)

Una vez configurado el navegador, se detecta que al abrirlo este sólo muestra una *cookie* de "Google" e información adicional de este sitio *web*. Al acceder a la aplicación "Facebook" el navegador guarda una *cookie* de "Facebook" (facebook.com). "Facebook" requiere que el usuario se autentique frente al sitio *web* para permitirle el acceso. Al autenticarse con las credenciales frente a la aplicación "Facebook", el navegador almacena las *cookies*: atdmt.com (2), Facebook (11) y liverail.com (2). El número entre el paréntesis indica el número de *cookies* que el navegador almacena de cada sitio.

Las *cookies* de Atdmt.com son de rastreo y son servidas por "Facebook" a través de la empresa subsidiaria Atlas Solutions y son usadas como *cookies* de terceros por numerosos sitios *web*.

Liverail.com es una compañía de "Facebook" cuya tecnología es utilizada por cientos de los mayores publicistas, los cuales se benefician de análisis sofisticados y controles avanzados, generando el rendimiento máximo de cada anuncio. Adicionalmente gestiona anuncios de acuerdo a las selecciones del usuario.

Al navegar por el sitio *web* de "Facebook" el navegador va almacenando nuevas *cookies* en el ordenador del usuario, por ejemplo, se ha detectado que el sitio Groupalia almacena 14 *cookies* diferentes entre las de sesión y las persistentes.

Al cerrar la sesión de navegación y volver a abrir el navegador, se observa que han quedado almacenadas todas aquellas *cookies* persistentes, sin embargo las *cookies* de sesión han sido eliminadas. Por ejemplo, si se accede a las *cookies* de Groupalia que ha almacenado el navegador, se puede observar que las siguientes *cookies* de sesión han desaparecido: BIInfo, gat, dcgtm_UA-15758073-6 y degtm_UA-62250942-1 y cbarsess_pv.

Al abrir de nuevo el navegador sin haber eliminado las *cookies* y acceder a la aplicación "Facebook", no es necesario volver a introducir las credenciales porque una *cookie* persistente proporciona las credenciales del usuario al sitio *web*.

5.2.2.2 Conservar datos locales sólo hasta salir del navegador - No bloquear los datos de sitios y las *cookies* de terceros - Permitir que todos los sitios ejecuten JavaScript (recomendado)

Al igual como ocurría en el caso anterior 5.2.2.1 al abrir el navegador sólo muestra una *cookie* de "Google" e información adicional de este sitio *web*. Al acceder al sitio "Facebook" el navegador almacena información local de "Facebook". Finalmente el usuario al autenticarse frente al sitio *web*, se detecta que el navegador ha almacenado *cookies* de atdmt.com (2), Facebook (11) y liverail.com (2). Comparando esta opción de configuración y la seleccionada en el apartado 5.2.2.1, no se ha detectado ninguna diferencia entre ambos casos.

El usuario, al navegar, provoca que el navegador vaya almacenando nuevas *cookies*. Este hecho ocurría también anteriormente en el caso 5.2.2.1. En un momento dado, al navegar por el sitio "Facebook", este muestra información personalizada al usuario de la empresa Iberia. Lo sorprendente de este caso es que "Facebook" muestra información no sólo basándose en *cookies* que tenga almacenadas en ese momento en el navegador que se está utilizando, sino que al haber utilizado otro navegador, por ejemplo Safari, "Facebook" puede registrar la visita que se realizó a la página de Iberia y al acceder desde otro navegador, en este caso Google Chrome, "Facebook" sigue mostrando información de Iberia. Al clicar sobre Iberia, el navegador Google Chrome almacena las *cookies* de Iberia. Esta situación se ha podido reproducir en otra ocasión, pero esta vez "Facebook" mostró publicidad de la empresa de alquiler de coches Sixt.

Al igual que ocurría con la configuración del navegador expuesta en el apartado 5.2.1.8, al analizar el comportamiento del navegador al visitar el sitio *web* "El País", una vez que el usuario ha cerrado el navegador, este ha borrado todas las *cookies* que fueron almacenadas mientras que el usuario navegaba. Esta configuración de las opciones de privacidad del navegador sólo proporcionará información de los sitios visitados por el usuario a terceros durante la sesión de navegación.

5.2.2.3 No permitir que se guarden datos de los sitios - No bloquear los datos de sitios y las *cookies* de terceros - Permitir que todos los sitios ejecuten JavaScript (recomendado)

Inicialmente el navegador no guarda ninguna *cookie* de la prueba anterior y se ha seleccionado la opción "No permitir que se guarden datos de los sitios". Al abrir el navegador se comprueba que no existe ninguna información guardada por el navegador.

Al visitar la página de "Facebook", el sitio *web* muestra, como es habitual, su política en relación al tratamiento que este realizada de la *cookies*. Para poder acceder al sitio es necesario introducir las credenciales del usuario tal y como se ha explicado anteriormente, pero al introducir las credenciales en "Facebook", este nos avisa mediante un mensaje: "Se requieren *cookies*: Las *cookies* no están habilitadas en tu navegador. Habilítalas en las preferencias del navegador para continuar." Por tanto, no debe seleccionarse la opción de privacidad de configuración de contenido "No permitir que se guarden datos de los sitios" si se pretende acceder al sitio *web* de "Facebook".

A continuación se muestran los resultados al modificar la configuración de las opciones de privacidad del navegador, cambiando respecto de las pruebas realizadas en los apartados 5.5.2.1, 5.2.2.2 y 5.2.2.3 la opción de "No bloquear los datos de sitios y las *cookies* de terceros", en este caso sí que se ha seleccionado "Bloquear los datos de sitios y las *cookies* de terceros".

5.2.2.4 Permitir que se almacenen datos locales (recomendado) - Bloquear los datos de sitios y las *cookies* de terceros - Permitir que todos los sitios ejecuten JavaScript (recomendado)

Al abrir el navegador, como en todos los casos anteriores, sólo ha almacenado una *cookie* de "Google" e información adicional de este sitio *web*. Al acceder al sitio *web* de "Facebook" se detecta que el navegador ha almacenado información local de "Facebook" (es-es.facebook.com). Y al introducir las credenciales del usuario se detecta que el navegador sólo ha almacenado *cookies* de "Facebook" (12) y por tanto, no aparecen las *cookies* de terceros de atdmt.com (2) y liverail.com (2) tal y como ocurría en el supuesto 5.2.2.1.

Al navegar se ha clicado sobre un anuncio de la compañía Sixt, almacenando el navegador 3 *cookies* de sixt.com, 10 *cookies* de sixt.es, 7 *cookies* de www.sixt.es y 3 *cookies* de terceros refinedads.com, con lo cual, al seleccionar esta opción el navegador no está bloqueando realmente todas las *cookies* de terceros ya que no se ha accedido a esta página voluntariamente en ningún momento.

Refineads.com es una empresa ubicada en Alemania, al igual que la compañía Sixt, y realiza análisis del uso a través de "Facebook" de los anuncios de las empresas que les contratan.

Al cerrar el navegador y volver a acceder a este, se detecta que el navegador sigue almacenando todas las *cookies* persistentes que han sido almacenadas en sesiones de navegación anteriores, y las *cookies* de sesión han sido eliminadas.

5.2.2.5 Conservar datos locales sólo hasta salir del navegador - Bloquear los datos de sitios y las *cookies* de terceros - Permitir que todos los sitios ejecuten JavaScript (recomendado)

El navegador se comporta exactamente igual que en el caso anterior 5.2.2.4 hasta el momento en el cual el usuario se autentica mediante credenciales frente a "Facebook".

Igual que anteriormente, a medida que se clica sobre los anuncios que se muestran por el sitio *web* "Facebook", el navegador empieza a almacenar *cookies* de los sitios de las diferentes empresas. En este caso se ha clicado sobre la publicidad de Iberia, Movistar y Sixt. Como ocurrió en el caso anterior, a pesar de haber seleccionado "Bloquear los datos de sitios y las *cookies* de terceros", el navegador sigue almacenando *cookies* del sitio refinedads.com.

En este caso, al cerrar el navegador y volver a acceder a él, se detecta que se han borrado todas las *cookies* que el navegador había almacenado en la sesión de navegación anterior, apareciendo sólo las *cookies* de la nueva sesión de navegación, más concretamente de "Google", ya que recordemos que el navegador tiene este sitio como dirección a la cual debe acceder cuando este se abre.

5.2.2.6 No permitir que se guarden datos de los sitios - Bloquear los datos de sitios y las *cookies* de terceros - Permitir que todos los sitios ejecuten JavaScript (recomendado)

Esta configuración del navegador no ha podido ser analizada, ya que tal y como se ha descrito en el apartado 5.2.2.3, la aplicación "Facebook" requiere que se habiliten las *cookies* para que el usuario pueda autenticarse frente al sitio *web* "Facebook".

Las tres pruebas que se muestran a continuación se realizaron utilizando las mismas opciones de configuración sobre la privacidad del navegador que las utilizadas en los apartados 5.5.2.1, 5.2.2.2 y 5.2.2.3, con la única diferencia que en este caso se seleccionó adicionalmente que se permitiera a todos los sitios realizar un seguimiento de la ubicación física del usuario.

5.2.2.7 Permitir que se almacenen datos locales (recomendado) – No bloquear los datos de sitios y las *cookies* de terceros - Permitir que todos los sitios ejecuten JavaScript (recomendado) - Permitir que todos los sitios realicen un seguimiento de tu ubicación física

Como en todos los casos en los que se ha seleccionado "Permitir que se almacenen datos locales (recomendado)" al abrir el navegador este almacena una *cookie* de "Google" e información adicional. En el momento que se accede a la aplicación mediante credenciales, el navegador almacena 11 *cookies* de "Facebook", de las cuales 9 son persistentes y 2 son de sesión. El nombre utilizado para cada una de ellas es el mismo que en casos anteriores. Las *cookies* de sesión tienen el nombre "p" y "presence" y las *cookies* persistentes tienen el mismo nombre que en casos anteriores, datr, fr, lu, sb y xs, pero en este caso cambian sus valores.

El usuario al navegar y acceder a los anuncios, estos van almacenando sus *cookies* en el navegador. Al salir del navegador y volver a acceder, se obtendrán todas las *cookies* persistentes que el navegador ha ido almacenando.

No se ha detectado ninguna mejora de la navegación del usuario al seleccionar "Permitir que todos los sitios realicen un seguimiento de tu ubicación física".

5.2.2.8 Conservar datos locales sólo hasta salir del navegador – No bloquear los datos de sitios y las *cookies* de terceros - Permitir que todos los sitios ejecuten JavaScript (recomendado) - Permitir que todos los sitios realicen un seguimiento de tu ubicación física

En este caso, al navegar por los sitios *web* que se publicitan a través de "Facebook" han guardado sus *cookies* en el navegador cuando se ha clicado sobre ellos. Al cerrar el navegador y volverlo a abrir, como en caso anteriores, se ha eliminado toda la información sobre *cookies* tanto persistentes como de sesión.

Al igual que en el caso anterior 5.5.2.7, no se ha detectado ninguna mejora de cara a la navegación del usuario al configurar el navegador con "Permitir que todos los sitios realicen un seguimiento de tu ubicación física".

5.2.2.9 No permitir que se guarden datos de los sitios – No bloquear los datos de sitios y las *cookies* de terceros - Permitir que todos los sitios ejecuten JavaScript (recomendado) - Permitir que todos los sitios realicen un seguimiento de tu ubicación física

Esta configuración del navegador no ha podido ser analizada ya que tal y como se ha descrito en los supuestos 5.2.2.3 y 5.2.2.6, la aplicación "Facebook" requiere que se habiliten las *cookies* para que el usuario pueda autenticarse frente al sitio *web*.

Durante las pruebas realizadas para ver el tipo de información que es guardada por el navegador al visitar el sitio *web* "Facebook", se ha detectado que las empresas publicitarias e incluso noticias que aparentemente no deberían representar un "peligro", y que no son de empresas de publicidad, utilizan "Facebook" para almacenar sus *cookies* en el navegador del usuario.

En este caso, tras realizar un análisis sobre el comportamiento del navegador Google Chrome al visitar el sitio de "Facebook", al seleccionar unas opciones determinadas relacionadas con la privacidad al configurar el contenido tanto de las *cookies* como JavaScript o Ubicación, se han obtenido los siguientes resultados:

- El sitio *web* "Facebook" requiere habilitar JavaScript ya que no es posible acceder a "Facebook" si no está habilitado en el menú de configuración de contenido JavaScript para "Permitir que todos los sitios ejecuten JavaScript (recomendado)".

- No se ha detectado ninguna restricción o mejora al visitar el sitio *web* "Facebook" si se ha seleccionado la opción "Ubicación - Permitir que todos los sitios realicen un seguimiento de tu ubicación física" o la opción "Ubicación – No permitir que ningún sitio pueda hacer un seguimiento de tu ubicación física". Por tanto, para evitar que pueda realizarse un seguimiento de nuestra ubicación física, ya que es información que se puede considerar privada, se recomienda seleccionar la opción "No permitir que ningún sitio pueda hacer un seguimiento de tu ubicación física".
- Respecto de la opción de configuración de contenido sobre las *cookies* es recomendable seleccionar "Bloquear los datos de sitios y las *cookies* de terceros" ya que a pesar de haberse marcado esta opción, en un par de ocasiones se ha detectado que sí se ha almacenado alguna *cookie* de terceros. También es cierto que limita enormemente el número de *cookies* de terceros que se guardan en el ordenador del usuario a través del navegador.
- Por último, en relación a la configuración del contenido sobre las *cookies*, de las tres opciones posibles que ofrece el navegador, y teniendo en cuenta que la opción "No permitir que se guarden datos del sitio" no es válida para el correcto funcionamiento de "Facebook", sólo quedan dos opciones que pueda elegir el usuario: "Permitir que se almacenen datos locales (recomendado)" o "Conservar datos locales sólo hasta que el usuario salga del navegador". Ante estas dos opciones se recomienda "Conservar datos locales hasta que salgas del navegador" ya que esta opción no permite a los sitios *web* obtener información del usuario una vez cerrada la ventana de navegación, con lo cual es mejor de cara a la privacidad de los usuarios en comparación con la primera opción.

5.2.3 Navegador Google Chrome – Sitio *web* "Amazon"

La metodología que se ha realizado para analizar el comportamiento del navegador Google Chrome al visitar el sitio *web* "Amazon" ha sido la misma que en los casos anteriores en el que se realizó un análisis al visitar el sitio *web* "El País" y "Facebook".

Las tres primeras pruebas han sido realizadas utilizando exactamente las mismas opciones de configuración del navegador respecto de la privacidad que se usaron en los casos 5.2.1.1, 5.2.1.2 y 5.2.1.3, con la única variación que en este caso se ha visitado el sitio "Amazon" en lugar de "El País".

5.2.3.1 Permitir que se almacenen datos locales (recomendado) - No bloquear los datos de sitios y las *cookies* de terceros - No Permitir que ningún sitio ejecute JavaScript

Antes de acceder al sitio *web* de "Amazon", la *cookie* que es almacenada por el navegador es la correspondiente a "Google" (la que el navegador tiene configurada como página de inicio).

Al acceder al sitio *web* de "Amazon", el navegador almacena 6 *cookies* persistentes provenientes de "Amazon". Una vez que el usuario se autentica frente a la aplicación, el navegador almacena 4 *cookies* adicionales, dos ellas persistentes, una de sesión y otra persistente con 14 minutos de validez.

Al navegar por el sitio *web*, el navegador almacena una *cookie* de rastreo que proviene de omtrdc.net. Este dominio es usado por Adobe, que utiliza la compañía de publicidad para rastrear las actividades de los usuarios al navegar desde un sitio a otro. A lo largo del tiempo creará un perfil del usuario, el cual puede ser utilizado o incluso vendido a otros publicistas o empresas de venta *online*.

Al cerrar la sesión de navegación y al volver a abrir el navegador, se puede observar que este ha eliminado todas aquellas *cookies* de sesión pero sigue almacenando las *cookies* persistentes, las cuales corresponden a los sitios “Amazon”, “Google” y “omtrdc.net”.

5.2.3.2 Conservar datos locales sólo hasta salir del navegador - No bloquear los datos de sitios y las *cookies* de terceros - No Permitir que ningún sitio ejecute JavaScript

El comportamiento respecto del almacenaje de las *cookies* al abrir el navegador, autenticarse frente al sitio “Amazon” y navegar a través de él, es exactamente el mismo que en el caso descrito anteriormente en el apartado 5.2.3.1. La única diferencia se detecta cuando se cierra el navegador, ya que en este caso este ha eliminado todas las *cookies* que había almacenado durante la sesión anterior, tanto si son de sesión como persistentes. La única *cookie* que aparece es la de “Google” que se corresponde a la apertura de una nueva ventana de navegación.

5.2.3.3 No permitir que se guarden datos de los sitios - No bloquear los datos de sitios y las *cookies* de terceros - No Permitir que ningún sitio ejecute JavaScript

Al seleccionar “No permitir que se guarden datos de los sitios”, el navegador no almacenará ningún tipo de *cookie*.

Al acceder al sitio *web* “Amazon”, el navegador no almacena ninguna *cookie,* pero el sitio muestra la portada con información de los artículos que ofrece a los clientes y permite navegar visualizando los detalles de los mismos. Al intentar acceder a la cuenta del usuario, “Amazon” muestra el siguiente mensaje: “Habilita las *cookies* para continuar. Para continuar comprando en “Amazon”, habilita las *cookies* en tu navegador. Una vez habilitadas las *cookies* en tu navegador, haz clic en el botón de abajo para volver a la página anterior. <Volver a la página anterior”. Por tanto, si el usuario desea entrar en su cuenta es necesario que este habilite las *cookies,* bien sea “Permitiendo que se almacenen datos locales (recomendado)” o “Conservar datos locales sólo hasta salir navegador”. Sin embargo, si el usuario sólo desea consultar los productos ofertados no será necesario habilitar las *cookies*.

Una vez que se cierra el navegador, y si no se ha modificado la opción “No permitir que se guarden datos de los sitios”, este seguirá sin almacenar ningún tipo de *cookie*.

A continuación se mostrarán los resultados obtenidos tras ir modificando las opciones de configuración del navegador respecto de la configuración del contenido, siguiendo el mismo proceso que en los apartados 5.2.3.1, 5.2.3.2 y 5.2.3.3, con la única variación de configuración del navegador que ahora se ha seleccionado “Bloquear los datos de sitios y las *cookies* de terceros”.

5.2.3.4 Permitir que se almacenen datos locales (recomendado) - Bloquear los datos de sitios y las *cookies* de terceros - No Permitir que ningún sitio ejecute JavaScript

Esta prueba es muy semejante a la expuesta anteriormente en el apartado 5.2.3.1. Inicialmente, no se aprecia ningún cambio ya que “Google” vuelve a almacenar una *cookie* antes de acceder a ningún sitio *web*. Al acceder a “Amazon” sólo son almacenadas la *cookie* de “Google” y tres *cookies* persistentes de “Amazon”, con lo cual si se compara esta opción con los resultados obtenidos en el aparatado 5.2.3.1, se detecta que el número de *cookies* almacenadas por el navegador se reduce, al no permitir al navegador almacenar *cookies* de terceros.

Si el usuario utiliza sus credenciales para autenticarse, el navegador almacena 10 *cookies*, las mismas que se almacenaron en la prueba realizada en el apartado 5.2.3.1. La única diferencia es que al navegar, en este caso no se almacena ninguna *cookie* adicional y la

cookie de omtrdc.net que se almacenaba por el navegador con la configuración descrita en el apartado 5.2.3.1 no aparece, lo cual indica que el navegador realmente está bloqueando los datos de sitios y *cookies* de terceros.

Las *cookies* que el navegador sigue almacenando, una vez se ha cerrado la sesión de navegación y se vuelve acceder a él, son la *cookie* de "Google" y 9 *cookies* persistentes de "Amazon". En este caso no es necesario que el usuario vuelva a introducir sus credenciales, ya que al acceder de nuevo al sitio "Amazon" este está directamente autenticado, pues este sitio utiliza una de sus *cookies* persistentes para almacenar las credenciales del usuario.

5.2.3.5 Conservar datos locales sólo hasta salir del navegador - Bloquear los datos de sitios y las *cookies* de terceros - No Permitir que ningún sitio ejecute JavaScript

La primera diferencia que se ha podido apreciar en comparación con las pruebas realizadas en el caso anterior 5.2.3.4 es que al salir del navegador, este no guarda las *cookies*, tal y como se ha seleccionado en el menú de preferencias. La segunda diferencia es que al acceder al sitio "Amazon" y no almacenar las *cookies* de la navegación anterior, es necesario que el usuario introduzca su dirección de e-mail o número de teléfono y contraseña para autenticarse frente a "Amazon".

5.2.3.6 No permitir que se guarden datos de los sitios - Bloquear los datos de sitios y las *cookies* de terceros - No Permitir que ningún sitio ejecute JavaScript

El resultado de las pruebas realizadas con la configuración de bloquear los datos de sitios y las *cookies* de terceros en el navegador es exactamente igual al descrito en la prueba 5.2.3.3. "Amazon" requiere que las *cookies* estén habilitadas para poder autenticar un usuario y por tanto poderle ofrecer todos sus servicios.

A continuación se mostrarán los resultados obtenidos tras ir modificando las opciones de configuración del navegador respecto de la configuración del contenido, siguiendo el mismo proceso que en los apartados 5.2.3.1, 5.2.3.2 y 5.2.3.3 con la única variación de configuración del navegador que ahora se ha seleccionado en el apartado JavaScript "Permitir que todos los sitios ejecuten JavaScript (recomendado)".

5.2.3.7 Permitir que se almacenen datos locales (recomendado) - No bloquear los datos de sitios y las *cookies* de terceros - Permitir que todos los sitios ejecuten JavaScript (recomendado)

Al configurar el navegador de forma que permita que todos los sitios ejecuten Java Script se detecta que nada más acceder al sitio de "Amazon" el número de *cookies* que almacena el navegador, en comparación con el que almacenaba cuando no se permitía que se ejecutará JavaScript, aumenta considerablemente: aparecen 26 *cookies* adicionales, la mayoría de ellas de terceros.

Al acceder al sitio de "Amazon" mediante autenticación se observa que el sitio vuelve a utilizar las 10 *cookies* que siempre almacena a través del navegador. Al navegar, igual como ocurría anteriormente con otras configuraciones, no implica que el navegador almacene más *cookies*.

Una vez cerrado el navegador y volver a abrirlo, se puede ver que todas las *cookies* persistentes siguen estando almacenadas. La mayoría de estas *cookies* son de terceros y tienen por finalidad rastrear los sitios visitados por el usuario. Esta opción implica un mayor riesgo para la privacidad del usuario. Adicionalmente, cabe destacar que para obtener los servicios que proporciona "Amazon" y navegar a través de este, no es necesario permitir que todos los sitios ejecuten JavaScript.

5.2.3.8 Conservar datos locales sólo hasta salir del navegador - No bloquear los datos de sitios y las *cookies* de terceros - Permitir que todos los sitios ejecuten JavaScript (recomendado)

El resultado de este caso es igual que el descrito en el apartado 5.2.3.7 con la única diferencia que al cerrar el navegador se eliminan todas las *cookies* almacenadas.

5.2.3.9 No permitir que se guarden datos de los sitios - No bloquear los datos de sitios y las *cookies* de terceros - Permitir que todos los sitios ejecuten JavaScript (recomendado)

A pesar de haber configurado el navegador de forma que permita que se ejecute JavaScript, el hecho de haber configurado la opción de privacidad indicando que no se permitan guardar los datos de los sitios implica que el resultado de esta configuración sea exactamente igual que los casos descritos anteriormente en los apartados 5.2.3.3 y 5.2.3.6.

A continuación se mostrarán los resultados obtenidos tras ir modificando las opciones de configuración del navegador respecto de la configuración del contenido, siguiendo el mismo proceso que en los apartados 5.2.3.4, 5.2.3.5 y 5.2.3.6 con la única variación de configuración del navegador que ahora se ha seleccionado en el apartado JavaScript “Permitir que todos los sitios ejecuten JavaScript (recomendado)”.

5.2.3.10 Permitir que se almacenen datos locales (recomendado) - Bloquear los datos de sitios y las *cookies* de terceros - Permitir que todos los sitios ejecuten JavaScript (recomendado)

El resultado de la configuración es el mismo que en la prueba realizada descrita en el apartado 5.2.3.4. En este caso a pesar de haber configurado el navegador para permitir que los sitios ejecuten JavaScript, lo cual implicaba un aumento considerable de las *cookies* que almacena el navegador tal y como se ha descrito en el apartado 5.2.3.7, el hecho de haber seleccionado en las opciones de configuración bloquear los datos de sitios y las *cookies* de terceros implica que el navegador sólo almacena *cookies* de los sitios visitados.

Al cerrar el navegador y volverlo a abrir, se puede apreciar como todas las *cookies* persistentes almacenadas durante navegaciones anteriores siguen estando almacenadas.

5.2.3.11 Conservar datos locales sólo hasta salir del navegador - Bloquear los datos de sitios y las *cookies* de terceros - Permitir que todos los sitios ejecuten JavaScript (recomendado)

El resultado al utilizar esta configuración es el mismo que el expuesto en el apartado anterior 5.2.3.10, con la diferencia de que al cerrar el navegador todas las *cookies* son eliminadas, por tanto, el usuario en una sesión de navegación posterior deberá introducir sus credenciales de nuevo para poderse autenticar frente a “Amazon”.

5.2.3.12 No permitir que se guarden datos de los sitios - Bloquear los datos de sitios y las *cookies* de terceros - Permitir que todos los sitios ejecuten JavaScript (recomendado)

El resultado de la configuración seleccionada es el mismo que se describió anteriormente en los apartados 5.2.3.3, 5.2.3.6 y 5.2.3.9, por tanto, el usuario no ha podido autenticarse frente al sitio *web*, con lo cual no será posible acceder a todos lo servicios ofrecidos por el sitio “Amazon”.

A continuación se mostrarán los resultados obtenidos tras ir modificando las opciones de configuración del navegador respecto de la configuración del contenido, siguiendo el mismo proceso que en los apartados 5.2.3.7, 5.2.3.8 y 5.2.3.9 con la única variación de configuración del navegador que ahora se ha seleccionado en el apartado Ubicación "Permitir que todos los sitios realicen un seguimiento de la ubicación física del usuario".

5.2.3.13 Permitir se almacenen datos locales (recomendado) – No bloquear los datos de sitios y las *cookies* de terceros - Permitir que todos los sitios ejecuten JavaScript (recomendado) - Permitir que todos los sitios realicen un seguimiento de tu ubicación física

La configuración utilizada para realizar esta prueba es la misma que la utilizada descrita en el apartado 5.2.3.10 pero en este caso se ha seleccionado que el navegador permita que todos los sitios realicen un seguimiento de la ubicación física del usuario. El resultado es que no se ha detectado ningún cambio a la hora de navegar por el sitio de "Amazon", ni tampoco se ha detectado que el navegador almacene ninguna *cookie* adicional.

5.2.3.14 Conservar datos locales sólo hasta salir del navegador – No bloquear los datos de sitios y las *cookies* de terceros - Permitir que todos los sitios ejecuten JavaScript (recomendado) - Permitir que todos los sitios realicen un seguimiento de tu ubicación física

La configuración utilizada en este apartado es la misma que en el caso anterior con la única diferencia que en el navegador se ha seleccionado que se conserven los datos locales sólo hasta salir del navegador. Una vez se ha cerrado el navegador, se eliminan todas las *cookies* de sesión y persistentes. No se detecta que el navegador almacene ninguna *cookie* adicional debida al hecho de haber configurado este de forma que se permita que todos los sitios realicen un seguimiento de la ubicación física del usuario.

5.2.3.15 No permitir que se guarden datos de los sitios – No bloquear los datos de sitios y las *cookies* de terceros - Permitir que todos los sitios ejecuten JavaScript (recomendado) - Permitir que todos los sitios realicen un seguimiento de tu ubicación física

El resultado de la configuración seleccionada es el mismo que se describió anteriormente en los apartados 5.2.3.3, 5.2.3.6, 5.2.3.9 y 5.2.3.12, por tanto, el usuario no ha podido autenticarse frente al sitio *web* con lo cual, con lo cual como en casos anteriores el usuario no podrá acceder a todos lo servicios ofrecidos por el sitio "Amazon".

Tras realizar un análisis sobre el comportamiento del navegador Google Chrome al seleccionar unas opciones determinadas relacionadas con la privacidad al configurar el contenido tanto de las *cookies* como JavaScript o Ubicación, se han obtenido los siguientes resultados:

- El sitio *web* "Amazon" no requiere habilitar JavaScript para proporcionar su servicios a los usuarios, por lo tanto es recomendable no seleccionar la opción Permitir que todos los sitios ejecuten JavaScript (recomendado).
- Igual como ocurría en los casos anteriores, no se ha detectado ninguna restricción o mejora al visitar el sitio *web* "Amazon" si se ha seleccionado la opción "Ubicación - Permitir que todos los sitios realicen un seguimiento de tu ubicación física" frente a la opción "Ubicación – No permitir que ningún sitio pueda hacer un seguimiento de tu ubicación física". Por tanto, se recomienda seleccionar la opción "No permitir que ningún sitio pueda hacer un seguimiento de tu ubicación física".
- Respecto de la opción de configuración de contenido sobre las *cookies* es recomendable seleccionar "Bloquear los datos de sitios y las *cookies* de terceros" ya que el navegador no permitirá que se almacenen *cookies* de sitios no visitados.
- Por último, en relación a la configuración del contenido sobre las *cookies* se recomienda "conservar datos locales hasta que salgas del navegador" ya que

esta opción permite acceder al usuario acceder a su cuenta para realizar compras o gestionar su cuenta en “Amazon” y no permite a los sitios *web* obtener información del usuario una vez cerrada la ventana de navegación.

5.2.4 Navegación Privada Google Chrome

La opción de la Navegación privada mejora la seguridad y privacidad de los usuarios en la red. Si el usuario utiliza el navegador Google Chrome deberá apretar las teclas Ctrl+Mayúsculas+N o pulsar sobre las tres rayas que aparecen en las esquina superior derecha al abrir el navegador y seleccionar “Nueva ventana de incógnito”.

Al seleccionar la ventana de incógnito, el navegador mostrará el siguiente mensaje: “Las páginas que aparezcan en las pestañas de incógnito no se guardarán en el historial del navegador, en el almacén de *cookies* ni en el historial de búsquedas una vez que hayas cerrado todas tus pestañas de incógnito. Se mantendrán los archivos que descargues o los marcadores que crees. Ten en cuenta que tus acciones no serán totalmente invisibles. El uso del modo incógnito no te permite ocultar tu actividad de navegación a tu empresa, a tu proveedor de servicios de Internet o a los sitios *web* que visites.”

Tal y como dice el mensaje, una vez que el usuario cierra la ventana de navegación, las *cookies*, las contraseñas y otros datos locales de la sesión son eliminados de forma automática. Por tanto, este modo de navegación es recomendable de cara a la seguridad y privacidad del usuario, sobre todo si realiza el acceso a Internet a través de un ordenador público o a través de un ordenador que es compartido por más usuarios, ya que las contraseñas serán eliminadas al cerrar la pestaña de navegación privada y no podrán ser captadas por el siguiente usuario.

Por otro lado, cabe destacar que tal y como advierte el mensaje que proporciona el navegador al abrir la pestaña en modo privado, la privacidad no es total, ya que la actividad del usuario puede ser registrada y analizada por el propietario de la empresa, por el proveedor de servicios de Internet o por los sitios *web* visitados.

En relación al resultado obtenido al utilizar el navegador Google Chrome mediante la ventana de incógnito, cabe destacar que las pruebas que se han realizado utilizando la ventana de sesión de incógnito del navegador Google Chrome han sido las mismas que se realizaron mediante no de incógnito. No se ha detectado que las *cookies* que han sido utilizadas por los sitios *web* “El País”, “Facebook” y “Amazon” hayan sido almacenadas por el navegador. Al tener abierta la ventana de incógnito, el navegador permite al usuario que sólo tenga que autenticarse una vez frente a los sitios visitados recordando el usuario y la contraseña a través de *cookies* almacenadas. Al finalizar la sesión cerrando la ventana de navegación, el navegador no guarda ninguna *cookie* de los sitios visitados ni ninguna contraseña utilizada por el usuario.

La opción de Navegación privada es una opción cómoda que no requiere configuración por parte del usuario y que le proporciona mayor privacidad.

5.2.5 Navegador Mozilla Firefox – Sitio *web* “El País”

En los siguientes apartados se realizarán una serie pruebas utilizando el navegador “Mozilla Firefox” y se analizarán los resultados obtenidos al ir seleccionando las diferentes opciones que el navegador nos permite respecto de la privacidad a través de la configuración del contenido.

Las tres primeras pruebas realizadas utilizando el navegador Mozilla Firefox tendrán en común que el navegador aceptará *cookies* incluso de terceros. Las pruebas se diferencian en el tratamiento que el navegador realizará sobre las *cookies* respecto del tiempo de almacenamiento. En el primer caso el navegador se ha configurado para almacenar las *cookies* hasta que Caduquen, en el segundo caso hasta que se Cierre Firefox y por último la opción seleccionada es Preguntar siempre.

5.2.5.1 Aceptar *cookies* - Aceptar *cookies* de terceros – Mantener hasta que caduquen

Antes de acceder a la página del sitio *web* de "El País" una *cookie* es almacenadas por el navegador del sitio "Google". Esto es debido a que tal y como se comentó anteriormente "Google" es la página que se ha establecido como página de inicio al abrir la ventana del navegador.

Una vez se accede al sitio de "El País" el navegador almacena cerca de 200 *cookies*. La inmensa mayoría son *cookies* de terceros ya que sólo se ha accedido a la portada sin navegar por el sitio. De estas 200 *cookies*, 16 corresponden a *cookies* de sesión, la cuales serán eliminadas por el navegador al cerrar la sesión de navegación.

Al navegar por el sitio *web* se detecta que nuevas *cookies* son almacenadas por el navegador, por ejemplo, durante la navegación se clicó sobre un anuncio de la empresa Toyota y el sitio *web* de Toyota almacenó 14 *cookies*.

Al cerrar la ventana de navegación y volver a abrir una nueva sesión de navegación, se verifica que todas las *cookies* de sesión han sido eliminadas. Un ejemplo lo podemos ver con las *cookies* almacenadas por el sitio *web* de "El País". Este sitio almacenó un total de 18 *cookies* durante la navegación. Una vez cerrada la sesión del navegador y volver a abrirlo, se detecta que el número total de *cookies* almacenadas es 14. Este número se corresponde con las *cookies* persistentes almacenadas, ya que las otras 4 *cookies* correspondían a *cookies* de sesión.

Esta opción de configuración no es muy adecuada de cara a la privacidad del usuario ya que permite que numerosos sitios terceros utilicen sus *cookies* para obtener información del usuario, y además permite que las *cookies* sigan estando almacenadas después de cerrar una sesión de navegación.

5.2.5.2 Aceptar *cookies* - Aceptar *cookies* de terceros – Mantener hasta que cierre Firefox

La diferencia de configuración del navegador respecto del tratamiento de las *cookies*, entre este caso y el descrito en el apartado anterior 5.2.5.1, es que en este caso se ha seleccionado "Mantener hasta que cierre Firefox" mientras que en el caso anterior fue "Mantener hasta que caduquen". A la hora de navegar no se detecta ninguna diferencia respecto del caso anterior, ya que el navegador sigue almacenando *cookies* de sesión y *cookies* persistentes a medida que el usuario navega.

La diferencia aparece en el momento en el que el navegador es cerrado y se vuelve a abrir. En este caso al haber seleccionado la opción de las *cookies* "Mantener hasta que cierre Firefox" se han eliminado todas las *cookies* de la navegación anterior y la única *cookie* que se ha almacenado es de "Google" y es debido a la nueva sesión de navegación.

Esta opción de navegación es mejor que la expuesta en el caso anterior ya que a pesar de aceptar *cookies* de terceros, las *cookies* son eliminadas una vez que se cierra la sesión de navegación.

5.2.5.3 Aceptar *cookies* - Aceptar *cookies* de terceros – Mantener hasta que preguntar siempre (1)

Este tercer caso se diferencia de los dos anteriores porque se le ha indicado al navegador "Preguntar siempre". En los dos casos anteriores nada más abrir el navegador, este almacenaba una *cookie* de "Google". En este caso antes de que se abra la página aparece un mensaje en el cual se informa "El sitio www.google.es quiere escribir una *cookie*" y aparece información relativa a la *cookie*. El usuario podrá seleccionar: Ocultar detalles, Permitir sesión, Denegar o Permitir. Adicionalmente puede clicar sobre "usar mi elección para todas las *cookies* de este sitio".

(1) Al analizar comportamiento del navegador Mozilla Firefox, una de las elecciones de configuración corresponden a la opción de preguntar siempre al usuario si desea almacenar cookies de un determinado sitio. El texto del título del apartado es el que muestra la opción del navegador "mantener hasta que: preguntar siempre".

Al acceder al sitio “El País”, antes de mostrar la portada del diario digital, empiezan a aparecer numerosos mensajes sobre *cookies* que terceros desean almacenar en el ordenador del usuario. El primer mensaje proviene del sitio “Doubleclick” y se probó denegar el almacenamiento de la *cookie* sin haber clicado sobre la opción “usar mi elección para todas las *cookies* de este sitio”. El siguiente mensaje que aparece vuelve a ser del sitio “Doubleclick” y también se denegó el almacenamiento, pero en este caso se probó clicar sobre “usar mi elección para todas las *cookies* de este sitio”. Los siguientes mensajes que se muestran al usuario son de otros sitios *web* que también quieren almacenar *cookies*. En este caso lo sorprendente, y que no ocurre sólo una vez, es que a pesar de que el usuario seleccione “usar mi elección para todas las *cookies* de este sitio”, los sitios siguen enviando mensajes de almacenamiento de *cookies*. Este hecho ocurrió con los sitios “Ad.Doubleclick.net”, “bs.serving-sys.com” y “t.qservz.com”.

Al denegar todas las *cookies* de terceros, el navegador sólo almacena las *cookies* que se han permitido, las cuales en la prueba fueron de los sitios de “Google” y “El País”.

A continuación el usuario, al navegar por el sitio “El País”, recibe numerosos mensajes de solicitud de almacenamiento de *cookies* de sitios terceros. Se probó a denegar a todos los sitios que podrían almacenar *cookies* y se seleccionó “Usar mi elección para todas las *cookies* de este sitio”. Al finalizar la navegación se obtuvo que el único sitio que almacenó más *cookies* fue “El País”, ya que al haber seleccionado “Usar mi elección para todas las *cookies* de este sitio” se permitió que este sitio siguiera almacenando nuevas *cookies*.

Una vez cerrado el navegador y al volver a abrirlo, se detecta que el navegador continua teniendo almacenadas todas aquellas *cookies* persistentes de los sitios “Google” y “El País” de la sesión de navegación anterior. Adicionalmente, todos los mensajes recibidos de sitios terceros a los cuales se les denegó que pudieran almacenar *cookies* aparecen como bloqueadas al clicar sobre “Excepciones – *Cookies*”. Por tanto, al volver a acceder al sitio “El País” no vuelve a mostrar los mensajes de los sitios que aparecen como bloqueados por el usuario.

Esta opción de navegación es mejor que las anteriores, ya que se notifica al usuario de la intención de un sitio de almacenar *cookies*, con lo cual el usuario decidirá qué quiere hacer con las *cookies* de cada sitio *web* y, por tanto, el navegador actuará en consecuencia con las decisiones tomadas por el usuario.

A continuación se realizarán las mismas pruebas que las realizadas en los apartados 5.2.5.1, 5.2.5.2 y 5.2.5.3 pero habiendo modificado la configuración del navegador respecto de la aceptación de *cookies,* ya que en las siguientes pruebas se ha configurado el navegador para que no acepte *cookies* de terceros.

5.2.5.4 Aceptar *cookies* – No aceptar *cookies* de terceros – Mantener hasta que caduquen

Al abrir el navegador, igual como ocurría en todos los casos anteriores, el navegador almacena una *cookie* del sitio “Google”. Posteriormente al acceder al sitio *web* “El País” se han reducido considerablemente el número de *cookies* almacenadas por el navegador. En el caso más semejante al analizado aquí, el cual es el 5.2.5.1, se almacenaron casi 200 *cookies* entre las *cookies* de “Google”, “El País” y el resto de *cookies* de terceros. En este caso, sólo se han almacenado 30 *cookies* del sitio “El País”.

Al seguir navegando por el sitio “El País”, el navegador continúa almacenando *cookies* de “El País” y del sitio “As”, el cual almacena 16 *cookies* al acceder a una noticia de deportes.

Al cerrar el navegador y volverlo a abrir, se detecta que el navegador sigue almacenando todas las *cookies* persistentes de los sitios visitados “El País”, “As” y “Google”.

Esta opción de configuración es más adecuada, de cara a la privacidad, que la seleccionada en el apartado 5.2.5.1, ya que al no permitir *cookies* de terceros se limita que sitios terceros puedan obtener información privada de los usuarios.

5.2.5.5 Aceptar *cookies* – No aceptar *cookies* de terceros – Mantener hasta que cierre Firefox

El resultado obtenido es semejante al expuesto en el apartado 5.2.5.2, pero en este caso se han reducido el número total de *cookies* almacenadas, ya que no se permite que el navegador almacene *cookies* de terceros.

Al navegar por el sitio de "El País" el navegador va almacenando *cookies* provenientes de "El País" principalmente, pero cabe destacar que al acceder a una noticia relacionada con viajes, el navegador ha almacenado *cookies* del sitio "Skyscanner", que es un buscador de viajes, y del sitio "Outbrain", que es un sitio dedicado a recomendar contenidos a los usuarios e incluir contenidos externos, con lo cual a pesar de haber seleccionado en las opciones de configuración del navegador que no acepte *cookies* de terceros, el navegador ha insertado una *cookie* de "Outbrain" la cual es una *cookie* de terceros.

Al cerrar el navegador y volverlo a abrir, se detecta que todas las *cookies* han sido eliminadas por el navegador. Esta opción de navegación mejora la privacidad del usuario ya que no permite que *cookies* de terceros sean almacenadas por el navegador y también mejora la privacidad del usuario al almacenar las *cookies* sólo durante la sesión de navegación, y por tanto al cerrar el navegador todas las *cookies* son borradas.

5.2.5.6 Aceptar *cookies* – No aceptar *cookies* de terceros – Mantener hasta que preguntar siempre

Las opciones de configuración del navegador son prácticamente las mismas que las utilizadas en el apartado 5.2.5.3, con la única diferencia que ahora se ha seleccionado la opción de no aceptar *cookies* de terceros. El resultado de la navegación es prácticamente el mismo pero evidentemente con la reducción del número de *cookies* almacenadas por el navegador, ya que no almacena *cookies* de terceros.

En este caso igual como ocurría en el caso descrito en el apartado 5.2.5.3, el navegador pregunta cada vez que el sitio visitado desea almacenar una *cookie*. En este caso se ha permitido al navegador almacenar *cookies* de "Google" y de "El País".

El número de mensajes de peticiones de sitios para almacenar *cookies* se han reducido sustancialmente, ya que en este supuesto se ha configurado el navegador para no aceptar *cookies* de terceros. Prácticamente no se han mostrado mensajes al usuario. Sólo se han mostrado mensajes cuando el usuario ha accedido a páginas de publicidad. Al acceder a un anuncio de una naviera, ha mostrado dos mensajes, uno de la propia naviera y otro del sitio "doubleclick.net". Al denegar el almacenamiento de *cookies*, el sitio de la naviera muestra un mensaje por el cual indica que requiere *cookies* para poder prestar sus servicios, y recomienda al usuario verificar si tiene la última versión del navegador actualizada.

Todas las excepciones quedan almacenadas en el navegador, y aparece que se ha permitido el acceso a las *cookies* de los sitios "Google" y "El País", y por el contrario están bloqueados los sitios "Grimaldi-lines" y "Doubleclick".

Al cerrar el navegador y volverlo a abrir se detecta que todas las *cookies* de sesión han sido eliminadas. Sin embargo el navegador sigue almacenando todas las *cookies* persistentes guardadas durante sesiones de navegación previas.

Respecto de las excepciones de las *cookies* que el usuario ha seleccionado durante navegaciones anteriores, siguen estando almacenadas. En el caso de que el usuario lo desee puede eliminar un sitio en concreto o todos los sitios listados en el apartado de las excepciones de las *cookies*.

Igual como ocurría en el caso 5.2.5.3, el usuario controla qué sitios *web* almacenan *cookies*, y por tanto decidirá qué sitios pueden obtener información de sus hábitos de navegación. Además, en este caso, al no permitir las *cookies* de terceros, se reduce el número de preguntas que el usuario recibirá de sitios terceros.

5.2.5.7 No aceptar *cookies*

Al configurar el navegador para que no permita que almacene *cookies* se detecta que al abrir el navegador y acceder a "Google", este no almacena ninguna *cookie*.

Al navegar por el sitio *web* de "El País", no se detectan diferencias importantes respecto de las navegaciones realizadas en los casos anteriores, excepto que al navegar, cada vez que se selecciona una página, se muestra el mensaje con la política que el sitio "El País" aplica sobre las *cookies*. En el momento que el usuario se mueve por la página, el mensaje desaparece al entenderse implícitamente que el usuario acepta la política del sitio sobre el uso de *cookies.*

En el caso de que el usuario acceda a algún sitio *web* clicando sobre un anuncio mostrado por "El País", el sitio de la empresa anunciante tampoco almacenará ninguna *cookie*.

Al cerrar y volver a abrir el navegador, se comprueba que no se ha almacenado ninguna *cookie* por parte de este.

Esta opción de configuración del navegador Firefox es la más segura de cara a la privacidad del usuario al visitar el sitio "El País", ya que no permite que se utilicen *cookies*, y que por tanto estas puedan proporcionar información privada sobre los usuarios a los sitios.

5.2.6 Navegador Mozilla Firefox – Sitio *web* "Facebook"

La metodología que se ha realizado para analizar el comportamiento del navegador Firefox al visitar el sitio *web* "Facebook" ha sido la misma que en el caso anterior en el que se realizaba un análisis al visitar el sitio *web* "El País".

Igual como en las pruebas realizadas en el apartado 5.2.5, las tres primeras pruebas que se realizarán tienen en común que el navegador aceptará *cookies* incluso de terceros. Las pruebas se diferencian en el tratamiento que el navegador realizará sobre las *cookies* respecto del tiempo de almacenaje. En el primer caso el navegador se ha configurado para almacenar las *cookies* hasta que caduquen, en el segundo caso hasta que se cierre Firefox y por último preguntar siempre.

5.2.6.1 Aceptar *cookies* - Aceptar *cookies* de terceros – Mantener hasta que caduquen

Inicialmente, el sitio "Google" almacena una *cookie* persistente. Al acceder a la página de "Facebook", el sitio *web* muestra la política sobre el tratamiento de las *cookies*.

Una vez que el usuario se ha autenticado y accede al sitio de "Facebook", el navegador almacena 12 *cookies*, 8 de ellas persistentes y 4 de ellas de sesión. Al navegar por el sitio de "Facebook" aparecen una *cookie* de rastreo del sitio Atdmt.com y una *cookie* del sitio Liverail.com, igual como ocurría al navegar por "Facebook" utilizando el navegador Google Chrome.

Al cerrar el navegador, las *cookies* de sesión son eliminadas y siguen estando almacenadas aquellas *cookies* persistentes de los sitios "Google", "Facebook", "Atdmt.com" y "Liverail.com".

Esta opción de configuración tal y como ya se explicó en el apartado 5.2.5.1 no es muy adecuada de cara a la privacidad del usuario, ya que permite que numerosos sitios terceros utilicen sus *cookies* para obtener información del usuario y además permite que las *cookies* sigan estando almacenadas después de cerrar una sesión de navegación.

5.2.6.2 Aceptar *cookies* - Aceptar *cookies* de terceros – Mantener hasta que cierre Firefox

La diferencia entre la configuración seleccionada durante la prueba 5.2.6.1 y la utilizada en este caso, es que el navegador ha sido configurado para mantener las *cookies* hasta que se cierre Firefox. En el caso anterior el navegador mantenía *cookies* hasta que alcanzaban la fecha límite de validez.

El resultado ha sido que el navegador sólo almacena *cookies* de sesión de los sitios. Al aceptar *cookies* de terceros, el navegador sigue almacenando *cookies* de los sitios "Atdmt.com" y "Liverail.com" como en el caso anterior.

Al cerrar el navegador, y al no haber almacenado *cookies* persistentes durante la sesión de navegación anterior, este eliminará todas las *cookies* de sesión. Una vez que el navegador se vuelve a abrir de nuevo se detecta que efectivamente no se ha almacenado ninguna *cookie*.

Igual como ocurría en el apartado 5.2.5.2, esta opción de navegación es mejor que la expuesta en el caso anterior ya que a pesar de aceptar *cookies* de terceros, las *cookies* son eliminadas una vez que se cierra la sesión de navegación.

5.2.6.3 Aceptar *cookies* - Aceptar *cookies* de terceros – Mantener hasta que preguntar siempre

En este apartado se mostrarán los resultados una vez que el navegador Firefox ha sido configurado para que se pregunte al usuario si quiere almacenar *cookies* de un determinado sitio. Tal y como se describió en el apartado 5.2.5.3, el navegador, al preguntar al usuario, muestra una opción que le permite que su elección sea aplicable a todas aquellas *cookies* que provengan del sitio por el cual se le está realizando la pregunta de aceptación. Para realizar las pruebas, se ha seleccionado la casilla mencionada en todos los casos para evitar que el navegador pregunte al usuario por cada una de las *cookies* que desea almacenar. Aceptando o denegando una *cookie* de un sitio implicará la aceptación o denegación de todas las *cookies* de ese sitio.

Al navegar por el sitio de "Facebook" el navegador va preguntando al usuario qué acción desea en relación al almacenamiento de *cookies*. En la navegación realizada se ha permitido que el navegador almacene *cookies* de los sitios "Facebook" y "Google". Al aparecer *cookies* de "Liverail" y "Atdmt" se ha denegado el almacenamiento. Todas las preguntas contestadas por el usuario son almacenadas por el navegador y se pueden mostrar al usuario si clica sobre el botón "Excepciones-*Cookies*". Las decisiones tomadas por el usuario pueden ser cambiadas en cualquier momento a través de la ventana Excepciones-*Cookies*, pudiendo ser las opciones: Bloquear sitio permitido, Permitir durante la sesión *cookies* bloqueada o Permitir para permitir un sitio que está bloqueado o que está permitida durante la sesión. Adicionalmente, el usuario puede seleccionar Eliminar un sitio o Eliminar todos los sitios incluidos en el listado de Excepciones-*Cookies*.

Al cerrar el navegador y volverlo a abrir se detecta que el navegador tiene almacenadas todas las *cookies* persistentes que pertenecen a los sitios *web* cuyo estado en la pantalla de "Excepciones-*Cookies*" aparecen como Permitir. Al navegar de nuevo por el sitio "Facebook" no se almacenan *cookies* de aquellos sitios que aparecen como "Bloquear". Cabe destacar que al abrir una nueva sesión de navegación no es necesario volver a introducir las credenciales del usuario para autenticarse frente a "Facebook", ya que una *cookie* de "Facebook" almacenada recordará a la aplicación las credenciales del usuario.

Igual como se destacó en el apartado 5.2.5.3, esta opción de navegación es mejor que las anteriores 5.2.6.1 y 5.2.6.2 ya que el usuario es notificado de la intención de un sitio de almacenar *cookies*, con lo cual el usuario decidirá qué quiere hacer con las *cookies* de cada sitio *web* y, por tanto, el navegador actuará en consecuencia con las decisiones tomadas por el usuario.

A continuación se mostrarán los resultados tras modificar respecto de las pruebas realizadas en los apartados 5.2.6.1, 5.2.6.2 y 5.2.6.3 que el navegador No acepte *cookies* de terceros.

5.2.6.4 Aceptar *cookies* – No aceptar *cookies* de terceros – Mantener hasta que caduquen

En comparación con los resultados obtenidos y expuestos en el apartado 5.2.6.1, la gran diferencia radica en que el navegador, tal y como ha sido configurado, no acepta *cookies* de terceros, y por tanto no aparece una *cookie* de rastreo del sitio Atdmt.com, ni la *cookie* del sitio Liverail.com.

Al cerrar el navegador y volverlo a abrir se detecta que las tres *cookies* de sesión de "Facebook" han sido eliminadas, y las *cookies* persistentes de "Google" y "Facebook" siguen siendo almacenadas por el navegador.

La opción de configuración utilizada en este caso es mejor que la que permitía al navegador que almacenase *cookies* de terceros, ya que las *cookies* de terceros no proporcionan mejoras de cara a la navegación de los usuarios al visitar el sitio "Facebook" y, sin embargo, el uso de *cookies* de terceros puede implicar que sitios terceros obtengan información privada de los usuarios.

5.2.6.5 Aceptar *cookies* – No aceptar *cookies* de terceros – Mantener hasta que cierre Firefox

El análisis de configuración del navegador seleccionada para esta prueba nos confirma que el navegador no almacena *cookies* de terceros, igual como ocurría en el caso 5.2.6.4. Las *cookies* almacenadas sólo son *cookies* de sesión ya que el navegador ha sido configurado para que no acepte *cookies* que tengan una validez superior al tiempo que dure la sesión. Al navegar, el navegador almacena *cookies* de los sitios "Google" y "Facebook", así como de otros sitios relacionados con noticias que se muestran en "Facebook" y que en la prueba realizada han sido seleccionados por el usuario como puedan ser "Cuatro" o "KLM".

Al cerrar el navegador y volverlo a abrir se detecta que el navegador no tiene almacenadas las *cookies* de sesión de la sesión anterior, con lo cual se comprueba que las opciones seleccionadas por el usuario son realmente implementadas por el navegador.

En relación a la privacidad del usuario, esta opción es mejor que la descrita en el apartado 5.2.6.4, ya que no permite que las *cookies* tengan validez al cerrar una sesión de navegación. Por tanto, si un nuevo usuario inicia una sesión de navegación, no podrá utilizar información de la sesión anterior. Un ejemplo de la información a la que se podría acceder con otra configuración del navegador podrían ser credenciales del usuario anterior para acceder a un sitio determinado. Con esta opción de configuración aumenta la privacidad de los usuarios.

5.2.6.6 Aceptar *cookies* – No aceptar *cookies* de terceros – Mantener hasta que preguntar siempre

Este caso es muy semejante al expuesto en el apartado 5.2.6.3. El navegador pregunta al usuario si este desea almacenar las *cookies* de los sitios. La mayor diferencia detectada es que en este caso el navegador realiza un filtrado de los sitios que pretenden almacenar *cookies,* y si las *cookies* provienen de sitios terceros directamente son rechazadas y no se

le realiza al usuario la pregunta por la cual podría permitir almacenar *cookies* de un sitio determinado.

Al navegar a través de "Facebook" y acceder a noticias de determinados sitios, el navegador realizará preguntas para saber qué debe hacer con las *cookies* que provienen de un sitio determinado. Las decisiones tomadas por el usuario quedan almacenadas en el registro de excepciones de *cookies*. En el caso de que el usuario desee almacenar *cookies* de un determinado sitio, el navegador permitirá y almacenará *cookies* tanto de sesión como persistentes.

Una vez finalizada la sesión, cerrado el navegador y vuelta a iniciar una sesión, se puede detectar que todas las *cookies* persistentes de los sitios que el usuario ha decidido permitir el almacenamiento siguen estando almacenadas por el navegador.

Igual como se destacó en el apartado 5.2.6.3, esta opción de navegación es mejor que las anteriores ya que el usuario decidirá qué quiere hacer con las *cookies* de cada sitio *web* y, por tanto, el navegador actuará en consecuencia con las decisiones tomadas por el usuario.

La última configuración que se utilizará para analizar el comportamiento del navegador al visitar el sitio "Facebook", es que el navegador no acepte *cookies*.

5.2.6.7 No aceptar *cookies*

Al acceder al sitio de "Facebook", este muestra su portada incluyendo el mensaje de la política respecto de las *cookies* aplicada por "Facebook". Al introducir las credenciales del usuario para autenticarse frente a la aplicación *web*, el sitio de "Facebook" muestra el siguiente mensaje al usuario: "Se requieren *cookies*. Las *cookies* no están habilitadas en tu navegador. Habilítalas en las preferencias del navegador para continuar:"

Este hecho implica que si el usuario desea utilizar "Facebook" deberá optar entre el resto de opciones pero permitiendo que el navegador almacene *cookies*.

5.2.7 Navegador Mozilla Firefox – Sitio *web* "Amazon"

La metodología que se ha realizado para analizar el comportamiento del navegador Firefox al visitar el sitio *web* "Amazon" ha sido la misma que en los casos anteriores, en el que se realizaba un análisis al visitar los sitios *web* "El País" y "Facebook".

Las tres primeras pruebas han sido realizadas seleccionado en las opciones de configuración del navegador aceptar *cookies* y aceptar *cookies* de terceros. La opción de configuración del navegador que se ha ido modificando ha sido la relativa al tiempo que el navegador debe almacenar las *cookies*.

5.2.7.1 Aceptar *cookies* - Aceptar *cookies* de terceros – Mantener hasta que caduquen

Inicialmente el sitio "Google" almacena una *cookie* persistente. Al acceder a la página de "Amazon" se detecta que el navegador almacena numerosas *cookies* de terceros.

Al navegar por el sitio de "Amazon" aparecen más *cookies* de terceros todas ellas utilizadas por empresas de publicidad con la finalidad de recopilar información del usuario y optimizar las inversiones en marketing.

Al cerrar el navegador, las *cookies* de sesión son eliminadas y siguen estando almacenadas todas las *cookies* persistentes.

Esta opción de configuración del navegador, tal y como se analizó en los casos anteriores 5.2.5.1 y 5.2.6.1, no es la más adecuada de cara a la privacidad de los usuarios, ya que el uso de *cookies* de terceros puede poner en riesgo información privada de los usuarios. Además la información almacenada por el navegador entre sesiones respecto de las *cookies* es mantenida.

5.2.7.2 Aceptar *cookies* - Aceptar *cookies* de terceros – Mantener hasta que cierre Firefox

Las opciones configuradas en el navegador respecto de las *cookies* en este caso permiten que el navegador sólo almacene *cookies* de sesión. Por tanto, el navegador sigue aceptando y almacenando *cookies* de terceros ya que este ha sido configurado con esa opción.

Al navegar por el sitio "Amazon" el navegador va almacenando *cookies* de sesión de sitios visitados y de terceros.

Una vez se ha cerrado el navegador, todas las *cookies* de sesión han sido eliminadas.

Esta opción de navegación es más conveniente que la seleccionada en el apartado 5.2.7.1, ya que garantiza que no se almacenen *cookies* entre sesiones de navegación.

5.2.7.3 Aceptar *cookies* - Aceptar *cookies* de terceros – Mantener hasta que preguntar siempre

Al abrir el navegador, el usuario recibe una pregunta solicitando si permite el almacenamiento de una *cookie* de "Google.es". Al aceptar, el navegador almacena una *cookie* persistente del sitio "Google.es" y en la pestaña de excepciones de *cookies* aparecerá que el sitio "Google.es" tiene permitido almacenar *cookies*.

A continuación se accede al sitio de "Amazon", y al recibir la pregunta sobre el permiso de almacenamiento de una *cookie*, se acepta el almacenamiento de *cookies* por parte de este sitio, con lo cual, igual como ocurría con "Google.es", el estado del sitio "Amazon.es" es Permitir.

Al navegar a través del sitio "Amazon.es" se ha denegado el almacenamiento de *cookies* de cualquier sitio que no sea "Google.es" y "Amazon.es". El navegador almacena por tanto las *cookies* de "Google.es" y "Amazon.es" y el resto de sitios a los cuales no se le permite almacenar *cookies* aparecen en el listado de Excepciones-*Cookies* como Bloqueado.

Al cerrar el navegador y volverlo a abrir se detecta que el navegador sigue almacenando *cookies* de los sitios a los que se les ha permitido almacenar *cookies*, y siguen apareciendo en el listado de Excepciones-*Cookies* aquellos sitios a los cuales el usuario no ha permitido el almacenamiento de *cookies*.

En el caso de que el usuario permita el almacenamiento de un sitio para una sesión, el navegador almacenará la *cookie* del sitio y en las excepciones de *cookies* aparecerá el sitio con el estado "Permitir para la sesión".

Al cerrar el navegador y volverlo a abrir se detecta que las *cookies* del sitio para el cual el usuario había permitido el almacenamiento para una sesión han desaparecido. Sin embargo, en el listado de Excepciones-*Cookies* sigue apareciendo el sitio indicando "Permitir para la sesión".

En relación a la privacidad esta opción permite al usuario decidir qué sitios pueden almacenar *cookies*, con lo cual, sólo los sitios que haya permitido el usuario almacenarán *cookies* y podrán obtener información de los usuarios.

A continuación se mostrarán los resultados tras modificar respecto de las pruebas realizadas en los apartados 5.2.7.1, 5.2.7.2 y 5.2.7.3 que el navegador No acepte *cookies* de terceros.

5.2.7.4 Aceptar *cookies* – No aceptar *cookies* de terceros – Mantener hasta que caduquen

La configuración del navegador en este caso implica que a medida que el usuario navegue por los sitios, este almacena *cookies* de los sitios visitados pero no de sitios terceros. En el momento en que el usuario se autentica frente al sitio "Amazon.es", el navegador almacena más *cookies* de este sitio y a medida que se visualizan los productos ofertados, el navegador almacena más *cookies*.

Una vez cerrado el navegador y debido a que se ha seleccionado que las *cookies* se mantengan hasta que caduquen, el navegador ha eliminado todas las *cookies* de sesión. Por tanto, al abrir el navegador se detecta que el navegador sigue almacenando sólo todas las *cookies* persistentes de los sitios visitados.

La gran diferencia de este caso con el descrito en el apartado 5.2.7.1 es el aumento del nivel de privacidad, ya que los sitios terceros no podrán recopilar información del usuario, y el número de *cookies* que almacena el navegador se reduce significativamente al no aceptar *cookies* de terceros.

5.2.7.5 Aceptar *cookies* – No aceptar *cookies* de terceros – Mantener hasta que cierre Firefox

Las opciones de configuración seleccionadas en este caso son prácticamente las mismas que las seleccionadas en el apartado anterior 5.2.7.4, con la diferencia de que en este caso las *cookies* almacenadas por el navegador son *cookies* de sesión y no persistentes.

El navegador durante la sesión va almacenando *cookies* de sesión de los sitios visitados por el usuario. Una vez cerrado el navegador, todas las *cookies* son eliminadas garantizando que no se guarda información de la navegación de los usuarios entre sesiones, y por tanto esta opción mejora la privacidad respecto del caso anterior.

5.2.7.6 Aceptar *cookies* – No aceptar *cookies* de terceros – Mantener hasta que preguntar siempre

En este caso la modificación realizada sobre las opciones de configuración descritas en el apartado 5.2.7.3 es la misma que la realizada en el apartado 5.2.7.4 y 5.2.7.5, por la cual el navegador no aceptará *cookies* de terceros. Este cambio implicará que el usuario no recibirá numerosas preguntas de sitios terceros sobre el almacenamiento de sus *cookies*.

A medida que el usuario navega a través de los sitios *web* para los que ha aceptado el almacenamiento de *cookies*, el navegador irá almacenando *cookies* tanto persistentes como de sesión, pero únicamente de estos sitios.

Tal como ocurría en el caso descrito en el apartado 5.2.7.3, a medida que el usuario acepta o no las *cookies* de los sitios, la información se registra en el apartado "Estado" de la ventana de Excepciones-*Cookies*.

Una vez cerrado el navegador, todas las *cookies* de sesión almacenadas por el navegador serán eliminadas y sólo seguirá almacenando las *cookies* persistentes de los sitios autorizados por el usuario. En la ventana Excepciones-*Cookies* se mantendrán las opciones respecto del almacenamiento de las *cookies* elegidas por el usuario en sesiones anteriores.

La última configuración que se utilizará para analizar el comportamiento del navegador al visitar el sitio “Amazon” es que el navegador no acepte *cookies*.

5.2.7.7 No aceptar *cookies*

El navegador ha sido configurado en esta ocasión para que no acepte las *cookies* de los sitios que el usuario visita. Al acceder al sitio “Amazon.es”, la portada del sitio informa al usuario que “Amazon” utiliza *Cookies*. Habiendo seleccionado que el navegador no pueda almacenar *cookies*, no se impedirá al usuario que pueda visualizar todas las ofertas que el sitio *web* muestra, sin ningún tipo de problema.

En el caso de que el usuario desee autenticarse frente al sitio *web*, este muestra el siguiente mensaje: “Habilita las *cookies* para continuar”. Si el usuario intenta iniciar la sesión introduciendo sus credenciales sin haber habilitado las *cookies*, el sitio *web* muestra el siguiente mensaje: “Habilita las *cookies* para continuar. Para continuar comprando en “Amazon.es”, habilita las *cookies* en tu navegador. Una vez habilitadas las *cookies* en tu navegador, haz clic en el botón de abajo para volver a la página anterior.” Por tanto, es necesario habilitar las *cookies* para poder acceder a los servicios proporcionados por el sitio “Amazon.es”.

5.2.8 Navegación Privada Mozilla Firefox

En el caso de que un usuario que utilice el navegador Mozilla Firefox desee acceder a la Navegación privada deberá seleccionar del menú de herramientas “Iniciar navegación privada” y confirmar “Comenzar navegación privada”. Como se comentó anteriormente, este tipo de navegación permite al usuario navegar por Internet sin guardar ningún tipo de información sobre las páginas *web* que visita. Firefox proporciona, al seleccionar esa opción, protección contra el rastreo por distintas compañías. Tal y como ocurría con el navegador Google Chrome, el hecho de seleccionar Navegación privada no asegura el anonimato en Internet, ya que el proveedor de Servicios de Internet o la organización a la que pertenece el usuario pueden rastrear las páginas que visita.

Una vez que el usuario ha seleccionado la Navegación privada podrá acceder a los sitios *web* almacenando las *cookies* de sesión que sean necesarias para poder ofrecerle sus servicios. En este caso se han visitado los sitios “El País”, “Facebook” y “Amazon”, e igual que en los casos anteriores “Facebook” y “Amazon” requieren que el usuario se autentique con correo electrónico y contraseña. Una vez autenticado el usuario, este puede ir de una página a otra de diferentes sitios sin tener que autenticarse de nuevo. Como en otras ocasiones esto es posible debido a que los sitios almacenan sus *cookies* con las credenciales del usuario en el navegador.

Una vez que el usuario desea finalizar la sesión de navegación privada deberá seleccionar del menú de herramientas “Detener navegación privada”. En este momento el navegador elimina de forma automática todas las *cookies* de sesión almacenadas durante la sesión de navegación privada. Adicionalmente, se detecta que no han quedado registradas las páginas visitadas en el historial.

Igual como se explicó al analizar el comportamiento de Google Chrome, respecto de la navegación privada, este modo de navegación es recomendable de cara a la seguridad y privacidad del usuario, sobre todo si realiza el acceso a Internet a través de un ordenador público o que es compartido por más usuarios, ya que las contraseñas serán eliminadas al cerrar la pestaña de navegación privada.

5.2.9 Navegador Safari – Sitio *web* "El País"

Las tres primeras pruebas del comportamiento del navegador Safari se diferencia en el tratamiento que el navegador realizará sobre las *cookies*. El navegador Safari ha sido configurado seleccionando entre las diferentes opciones que este proporciona en relación al bloqueo de las *cookies* y otros datos de sitios *web*.

A continuación mostraremos los resultados obtenidos tras analizar el comportamiento del navegador al visitar el sitio "El País".

5.2.9.1 Nunca bloquear *cookies* y otros datos de sitios *web*

El navegador inicialmente almacena una *cookie* de "Google", al haber configurado en el navegador que "Google" sea la página de inicio. A continuación, al acceder a la página de "El País" el navegador almacena las *cookies* de este sitio, las cuales son necesarias para ofrecer sus servicios al usuario, pero adicionalmente almacena numerosas *cookies* de terceros.

Una vez que el usuario cierra el navegador y vuelve a abrirlo, se detecta que todas las *cookies* persistentes que habían sido almacenadas durante la sesión anterior siguen estando almacenadas.

Igual como ocurría con la configuración de no bloquear los datos de sitios y las *cookies* de terceros al utilizar el navegador Google Chrome, o la configuración de aceptar cookies al utilizar el navegador Mozilla Firefox, la opción de no bloquear las *cookies* y otros datos de sitios *web* al utilizar el navegador Safari, no es aconsejable de cara a la privacidad de los usuarios.

5.2.9.2 Bloquear *cookies* y otros datos de sitios *web* de publicidad y terceros

El navegador, en este caso, reduce significativamente el número de *cookies* que almacena, debido a que el usuario ha seleccionado que no desea almacenar *cookies* de terceros. Igual como ocurría en el caso anterior, el navegador almacena las *cookies* del sitio "Google" y "El País".

En este caso hay que destacar que a pesar de haber seleccionado no almacenar *cookies* de terceros, el navegador almacena *cookies* del sitio "Outbrain", las cuales pertenecen a un sitio de publicidad cuya finalidad es analizar el comportamiento del usuario y recomendar artículos, fotos, videos, blogs, etc, al lector. Los sitios recomendados por Outbrain pagan por este servicio y Outbrain paga a los sitios donde el enlace aparece, en este caso a "El País".

Una vez que se cierra el navegador y se vuelve a abrir, se detecta que las *cookies* persistentes de los sitios visitados "Google", "El País", "Huffingtonpost" siguen estando almacenadas, así como *cookies* del sitio tercero "Outbrain".

Adicionalmente, también se detecta que el navegador almacena información que clasifica como "Almacenamiento local" de los sitios "Cxense.com" y "Youtube.com" aunque no lo clasifica como "*Cookie"*. "Cxense" es una compañía que proporciona publicidad, gestión de datos y servicios de recomendación de contenido y análisis de los mismos.

Por tanto, a pesar de que el usuario haya configurado el navegador para que bloquee *cookies* y otros datos de sitios *web* de publicidad y terceros, se ha detectado que el navegador sí que almacena información de sitios no deseados.

5.2.9.3 Siempre bloquear *cookies* y otros datos de sitios *web*

El navegador ha sido configurado en este caso para que siempre bloquee todas las *cookies* y otros datos de sitios. Al abrir el navegador, este accede a la página de "Google" y no almacena información de la sesión, ni local ni *cookies*.

Al acceder al sitio "El País" la portada muestra el mensaje con la política del uso de *cookies* que aplica el sitio. En este caso se detecta que el navegador tampoco almacena ningún tipo de información ni al acceder a la portada ni al navegar por las páginas del sitio. Al no almacenar ningún tipo de *cookies*, el navegador entiende que al acceder a cualquier página del sitio es como si la mostrase a un nuevo usuario y por tanto cada página que es visitada por el usuario muestra la política que aplica "El País" en relación al uso de las *cookies.*

Una vez que el usuario cierra el navegador y vuelve a abrirlo, se detecta que el navegador no ha guardado ninguna *cookie* entre sesiones.

Esta configuración de navegación es la que proporciona más privacidad a las navegaciones realizadas por los usuarios de las tres analizadas hasta el momento, y en el caso de acceso a "El País" no se requiere el uso de *cookies* para proporcionar sus servicios al usuario.

5.2.10 Navegador Safari – Sitio *web* "Facebook"

La metodología que se ha realizado para analizar el comportamiento del navegador Safari al visitar el sitio *web* "Facebook" ha sido la misma que en el caso anterior, en el que se realizaba un análisis al visitar el sitio *web* "El País".

Tal como en las pruebas realizadas en el apartado 5.2.9, las pruebas hechas se diferencian en el tratamiento que el navegador realizará sobre el bloqueo de *cookies* y otros datos de sitios *web*.

5.2.10.1 Nunca bloquear *cookies* y otros datos de sitios *web*

Inicialmente, el sitio "Google" almacena una *cookie* persistente. Al acceder a la página de "Facebook" almacena información localmente y la aplicación muestra la política de tratamiento de las *cookies*.

Una vez que el usuario se ha autenticado y accede al sitio de "Facebook" el navegador almacena información de la sesión, información local y *cookies*. Todas las *cookies* almacenadas son persistentes. Al navegar por el sitio de "Facebook" aparecen una *cookie* de rastreo del sitio Atdmt.com y una *cookie* del sitio Liverail.com, tal como ocurría al navegar por "Facebook" al utilizar los navegadores Google Chrome y Firefox.

Al cerrar el navegador, las *cookies* de sesión son eliminadas y siguen estando almacenadas aquellas *cookies* persistentes de los sitios "Google", "Facebook", "Atdmt.com" y "Liverail.com".

Esta opción de configuración del navegador, tal como ocurría al visitar el sitio "El País", no es la más adecuada ya que permite que sitios terceros como "Atdmt.com" y "Liverail.com" puedan obtener información del usuario.

5.2.10.2 Bloquear *cookies* y otros datos de sitios *web* publicidad y terceros

La diferencia entre la configuración seleccionada en la prueba 5.2.10.1 y la utilizada en este caso es que el navegador ha sido configurado para bloquear *cookies* y otros datos de sitios *web* de publicidad y terceros.

El navegador almacena tanto *cookies* de sesión como *cookies* persistentes de los sitios visitados, sin embargo, no almacena *cookies* de terceros. Esta configuración, por tanto, reduce el número de *cookies* que son almacenadas, no permitiendo a terceros la obtención de información del usuario.

Al cerrar el navegador todas las *cookies* de sesión son eliminadas y sólo quedan almacenadas las *cookies* persistentes de los sitios visitados. En este caso no es necesario volver a introducir las credenciales de los usuarios y por tanto el acceso al sitio "Facebook" es directo. Esto es debido a que las credenciales del usuario han sido guardadas por el navegador a través de una *cookie* del sitio "Facebook" en el ordenador.

5.2.10.3 Siempre bloquear *cookies* y otros datos de sitios *web*

El usuario, al abrir el navegador, accede al sitio "Google" y no almacena información de la sesión, ni información local ni *cookies*. A continuación al intentar acceder al sitio "Facebook", este muestra, como en ocasiones anteriores, la política que aplica respecto de las *cookies*. Al intentar introducir las credenciales del usuario, el sitio muestra el mensaje: "Se requieren *cookies*. Las *cookies* no están habilitadas en tu navegador. Habilítalas en las preferencias del navegador para continuar". Por tanto, la opción de bloquear *cookies* y otros datos de sitios *web* siempre no es válida si el usuario quiere acceder al sitio "Facebook".

Esta configuración del navegador, al no almacenar *cookies* ni información de los sitios *web*, implica que no existirá información guardada por el navegador entre sesiones.

5.2.11 Navegador Safari – Sitio *web* "Amazon"

En este apartado 5.2.11 se describen los resultados obtenidos al modificar la configuración del navegador en relación al grado de bloqueo que el navegador realizará a las *cookies* y otros datos de sitios *web* al visitar el sitio "Amazon".

5.2.11.1 Nunca bloquear *cookies* y otros datos de sitios *web*

El navegador, al abrirse, almacena numerosas *cookies* de terceros. Al acceder al sitio "Amazon" es posible visualizar los productos que ofrecen, pero requiere la autenticación del usuario para poder obtener los servicios ofrecidos por el sitio *web*.

A través de la opción de "Inspeccionar el elemento" se pueden examinar las *cookies* que utiliza "Amazon" en una determinada página del sitio. Al acceder a las ofertas de productos, se detecta el uso de *cookies* de terceros por el sitio "Amazon", cuya finalidad es la recopilación de información del usuario. Un ejemplo de *cookie* asociada a páginas de este sitio que ha sido detectada es "Serving-sys.com".

A medida que el usuario navega a través del sitio "Amazon" se actualizan las *cookies* que son almacenadas por el navegador y sus valores.

Al cerrar la sesión de navegación y volver a iniciar otra, se detecta que todas las *cookies* persistentes han sido almacenadas por el navegador y están disponibles para la nueva sesión. De esta forma, al acceder de nuevo al sitio "Amazon" no es necesario que el usuario introduzca de nuevo sus credenciales.

Esta opción de configuración, al igual que los casos expuestos anteriormente 5.2.9.1 y 5.2.10.1, no es la más adecuada de cara a asegurar la privacidad de los usuarios que visitan sitios *web*.

5.2.11.2 Bloquear *cookies* y otros datos de sitios *web* de publicidad y terceros

El navegador, en este caso, almacena *cookies* de sesión y persistentes únicamente de los sitios visitados, y por tanto se confirma que el navegador bloquea *cookies* y otros datos de sitios *web* de publicidad y terceros.

El funcionamiento del navegador en esta ocasión es el mismo que en los casos descritos en los apartados 5.2.9.2 y 5.2.10.2.

5.2.11.3 Siempre bloquear *cookies* y otros datos de sitios *web*

Al igual como ocurría al visitar el sitio "Facebook", "Amazon" requiere el uso de *cookies* para poder proporcionar sus servicios al usuario. Es por ello que muestra el mensaje: "Habilita las *cookies* para continuar. Sobre las *cookies* y cómo habilitarlas". En el caso de que el usuario introduzca su dirección de email o su contraseña, el mensaje que aparece es: "Habilita las *cookies* para continuar. Para continuar comprando en "Amazon.es", habilita las *cookies* en tu navegador. Una vez habilitadas las *cookies* en tu navegador, haz clic en el botón de abajo para volver a la página anterior".

5.2.12 Navegación Privada Safari

El usuario tiene la opción de realizar una Navegación privada, la cual podrá ser activada en el navegador Safari clicando sobre el Menú de Safari en la opción Navegación privada. El navegador mostrará el siguiente mensaje: "¿Desea activar la Navegación privada? Safari puede mantener su historial de navegación en privado. Si activa la Navegación privada, Safari no recordará ni las páginas que visita, ni su historial de búsqueda ni la información de Auto-relleno". Al clicar sobre Aceptar el usuario entra en el modo Navegación privada. Para salir de la Navegación privada el usuario deberá simplemente entrar en el menú de Safari y clicar sobre " ✓Navegación privada".

Durante la Navegación privada, el navegador almacena *cookies* de sesión y persistentes tanto de los sitios visitados por el usuario como de sitios terceros. Al cerrar la sesión, la Navegación privada finaliza y el navegador elimina todo tipo de *cookies* e información almacenada durante la sesión privada.

Al volver a abrir el navegador se confirma que las *cookies* almacenadas durante la sesión privada han sido eliminadas. El modo de navegación activo es la navegación normal y las *cookies* almacenadas son las que el navegador tenía almacenadas antes de iniciar la Navegación privada.

Este modo de navegación permite que no exista rastro de la navegación de un usuario, de forma que no se puedan relacionar sesiones de navegación para crear un perfil del usuario. Sin embargo, cada vez que se cierra una sesión, el usuario deberá autenticarse frente a los sitios a los que desee acceder y requieran la autenticación para ofrecer sus servicios.

6. CONFIGURACIÓN RECOMENDADA DE LOS NAVEGADORES

6.1 Configuración Recomendada del Navegador Google Chrome

Tras el análisis realizado al utilizar el navegador de Google Chrome visitando diferentes sitios *web* se recomienda al usuario la siguiente configuración:

1- Permitir JavaScript. Durante las pruebas se ha podido verificar que algunos sitios, como por ejemplo "Facebook" o "El País", requieren que esté habilitado JavaScript. En el caso de que no esté habilitado JavaScript, no se visualizarán las imágenes y no se podrá acceder a vídeos asociados a la información a la que se accede.
2- En general, es conveniente No permitir que se guarden datos de los sitios para salvaguardar la privacidad de los usuarios, a no ser que el usuario vaya a visitar sitios *web* como "Facebook" los cuales requieren que se habiliten las *cookies*. Por tanto, la mejor opción de configuración sería, en este caso, "Conservar datos locales hasta que salgas del navegador".
3- Bloquear los datos de sitios y las *cookies* de terceros. El navegador en este caso no permitirá que se almacenen *cookies* de terceros, lo cual implica un mayor grado de privacidad para el usuario.
4- Respecto de la opción del navegador de Ubicación, seleccionar "Preguntar cuando un sitio intente realizar un seguimiento de tu ubicación física (recomendado)" ya que a pesar de que los sitios *web* visitados no han proporcionado ninguna mejora relativa a la navegación, y no ha sido necesario que el sitio *web* conociera nuestra ubicación para poder ofrecernos sus servicios, algunos sitios requieren conocer la ubicación de los usuarios para ofrecer sus servicios. Sin embargo, el sitio, al preguntar, le permite al usuario decidir a que sitios *web* autoriza a realizar un seguimiento de su ubicación física, lo cual implica un mayor control sobre la información que este proporciona a determinados sitios *web*.

El navegador ha sido configurado con las opciones de configuración detalladas anteriormente y se ha procedido a ver el resultado de la navegación al visitar los tres sitios *web* que se han utilizado para realizar el análisis. El resultado ha sido el que se describe a continuación.

Al visitar el sitio "El País" el navegador va guardando *cookies* de este. Al acceder a la publicidad de Samsung que se mostraba en la página de "El País" aparecieron 15 *cookies* de Samsung y adicionalmente 2 *cookies* de terceros de serving-sys.com, a pesar de haber seleccionado bloquear los datos de sitios y las *cookies* de terceros. Este hecho ya ocurrió anteriormente tal y como se describió en el apartado 5.2.2.4, en el cual al acceder a un anuncio de la compañía Sixt que "Facebook" publicitaba implicó que el navegador almacenara la *cookie* refinedads.com. Debido a que seleccionar "Bloquear los datos de sitios y las *cookies* de terceros" no garantiza que no se almacenen *cookies* de terceros, mediante las cuales los sitios pueden rastrear la navegación que los usuarios realizan, se recomienda no acceder a los anuncios que se muestran a través de los sitios *web*.

Al acceder a "Facebook", el navegador almacena 12 *cookies* de este sitio. Adicionalmente, a medida que el usuario navega por el sitio y accede a publicaciones de otros sitios, estos almacenan *cookies* en el ordenador. Un ejemplo son las *cookies* que el navegador almacena al haber accedido a una información mostrada en "Facebook" del diario Última Hora.

El sitio "Amazon" almacena sus *cookies* a través del navegador una vez que el usuario accede a él. Al autenticarse y navegar, no se detecta que el navegador almacene ninguna *cookie* adicional.

Una vez finalizada la navegación por los tres sitios *web*, se ha cerrado el navegador y se ha vuelto a abrir, detectando que el navegador ha eliminado todas las *cookies* de la sesión anterior, con lo cual las *cookies* almacenadas por los sitios no podrán obtener información de los hábitos de navegación de los usuarios entre sesiones.

Una opción adicional de configuración respecto de la privacidad que nos permite el navegador es al elegir la opción de configuración de contenido seleccionar “Administrar excepciones”, pero esta opción para un usuario que visita diferentes tipos de sitios *web* no es muy útil ya que debería indicar que es lo que desea hacer con ciertos dominios. Las opciones que proporciona al introducirle un dominio son: permitir, borrar al salir o bloquear. Además los usuarios suelen desconocer desde qué dominios son enviadas las *cookies* de terceros de rastreo, ya que estas son las que afectan mayormente a la privacidad del usuario y las que deberían ser bloqueadas.

6.2 Configuración Recomendada del Navegador Mozilla Firefox

Tras el análisis realizado al utilizar el navegador de Mozilla Firefox visitando diferentes sitios *web* se recomienda al usuario la siguiente configuración:

1- Aceptar *Cookies*. Numerosos sitios *web* requieren que el navegador esté configurado para aceptar *cookies* para poder proporcionar sus servicios. Durante las pruebas realizadas, los sitios “Facebook” y “Amazon” requirieron que las *cookies* estuvieran habilitadas. Por tanto, lo más conveniente es habilitar las *cookies* seleccionando otras opciones adicionales de forma que la privacidad del usuario se vea lo menos comprometida.
2- El hecho de configurar el navegador de forma que permita el almacenamiento de *cookies* de terceros no proporciona ningún servicio adicional que mejore la navegación del usuario. Sin embargo, el hecho de permitir que estos sitios almacenen *cookies* puede comprometer la privacidad de los usuarios por lo que el navegador se debería configurar de forma que No permita aceptar *cookies* de terceros. Así, las *cookies* almacenadas por los sitios no podrán obtener información de los hábitos de navegación de los usuarios entre sesiones de navegación.

La siguiente opción que permite configurar el navegador Firefox es el tiempo que el navegador debe mantener las *cookies* almacenadas. Las opciones que permite el navegador son: Mantener hasta que caduquen, Mantener hasta que cierre Firefox y Preguntar siempre si el usuario quiere almacenar *cookies* de ese sitio *web*. Para ver cuál es la opción más conveniente, habrá que analizar si el navegador será utilizado por un usuario únicamente o por varios usuarios, siendo las recomendaciones las expuestas a continuación:

3- Si el navegador sólo va a ser utilizado por un único usuario, la opción más conveniente de configuración es Preguntar siempre si el usuario quiere almacenar *cookies* de ese sitio *web,* ya que en este caso el usuario será siempre preguntado en relación a las *cookies* que los sitios desean almacenar y él tendrá un control total sobre las *cookies* que permite o no. Además, entrando en la opción de Excepciones podrá ver en cualquier momento el estado de cada sitio y podrá modificar el estado si lo desea. Utilizando esta opción permitirá al usuario el nivel de privacidad que desee en relación con cada sitio.
4- Si por el contrario, el navegador va a ser utilizado por varios usuarios, la opción más conveniente de configuración es Mantener hasta que cierre Firefox. De esta forma se proporciona un mayor grado de privacidad a los usuarios, ya que la información almacenada durante la sesión de un usuario es eliminada una vez que este cierre el navegador.

Mozilla Firefox no proporciona la opción al usuario de decidir cómo se debe comportar el navegador cuando los sitios web deseen obtener información de la ubicación física del usuario. Esta opción sí que está disponible cuando el usuario utiliza el navegador Google Chrome.

El navegador ha sido configurado con las opciones de configuración detalladas anteriormente y se ha procedido a ver el resultado de la navegación al visitar los tres sitios *web* que se han utilizado para realizar el análisis. El resultado se describe a continuación.

Navegador utilizado por un único usuario

El usuario al intentar acceder al sitio de "El País" recibe un mensaje solicitando si permite que este sitio pueda almacenar *cookies*. Al aceptar que pueda almacenar *cookies*, este almacenará las *cookies* que necesite para proporcionar servicios al usuario. Adicionalmente, en la ventana de Excepciones-*Cookies* se observa que el navegador ha registrado que el estado para el sitio de "El País" es Permitir.

A continuación, se ha intentado acceder al sitio "Facebook" y el usuario ha recibido el correspondiente mensaje por el cual el usuario al aceptar, permitirá que el navegador almacene *cookies* de este sitio. Igual como ocurría al acceder al sitio "El País", en la ventana de Excepciones-*Cookies* se observa que el estado del sitio "Facebook" es Permitir.

Por último, se ha accedido al sitio "Amazon" tras aceptar que el navegador pueda almacenar *cookies* y, una vez más, la ventana de Excepciones-*Cookies* muestra que el estado del sitio "Amazon" es Permitir.

Una vez finalizada la navegación por los tres sitios *web*, se ha cerrado el navegador y se ha vuelto a abrir, detectando que este ha eliminado todas las *cookies* de sesión de la sesión anterior, pero sigue almacenando las *cookies* persistentes de los cuatro sitios para los que el usuario ha permitido que el navegador almacene *cookies*. Respecto de la ventana que muestra las Excepciones-*Cookies*, se observa que el navegador indica que el estado de los cuatro sitios es Permitir. Al acceder a los sitios de "Facebook" y "Amazon" no es necesario que el usuario vuelva a autenticarse, ya que el navegador a través de *cookies* de estos sitios proporciona la información requerida para autenticarse, con lo cual en este caso al ser un único usuario el que utilizará el navegador permite a este usuario no tener que introducir de nuevo las credenciales para acceder a esos sitios.

Navegador utilizado por un varios usuarios

En este caso la opción de configuración del navegador Firefox elegida para el tiempo que el navegador debe mantener las *cookies* almacenadas es Mantener hasta que cierre Firefox. Con esta selección el navegador no solicitará cada vez que un usuario desee acceder a los servicios de un sitio si desea que el navegador almacene *cookies* del sitio. Por lo tanto, la ventana Excepciones-*Cookies* no registrará ningún estado para ningún sitio *web*. Este hecho implicará que el navegador no guardará ninguna credencial de un usuario una vez que el usuario haya cerrado el navegador. A pesar de que este hecho pueda provocar que un usuario deba introducir sus credenciales cada vez que cierre una sesión del navegador, garantizará que las credenciales de un usuario no puedan ser usadas por el siguiente usuario si la sesión de navegación se ha cerrado, con lo cual, se garantiza la privacidad de los usuarios entre sesiones.

Las *cookies* que almacenará el navegador con las opciones de configuración seleccionadas serán *cookies* de sesión, las cuales serán eliminadas una vez que el usuario cierre la sesión de navegación. La primera *cookie* de sesión almacenada corresponde al sitio "Google", a continuación el resto de sitios visitados "El País", "Facebook" y "Amazon" irán almacenando *cookies* de sesión a medida que el usuario navegue por estos sitios.

Al finalizar la sesión, el usuario debe cerrar el navegador para garantizar que sus credenciales no son utilizadas por el siguiente usuario. Una vez cerrada la sesión se puede comprobar que el navegador no tiene ninguna *cookie* almacenada, y por tanto, si el usuario desea acceder a un sitio que requiera credenciales deberá introducirlas de nuevo.

Firefox permite eliminar las *cookies* almacenadas al clicar sobre el botón "Eliminar todas las *cookies*" sin tener que eliminar las reglas que el usuario ha ido determinando a medida que ha ido navegando y ha contestado las preguntas del navegador. En el caso de que el usuario quiera eliminar las reglas deberá clicar sobre el botón "Eliminar todos los sitios" de la pantalla Excepciones-*Cookies*.

6.3 Configuración Recomendada del Navegador Safari

Las opciones ofrecidas por el navegador Safari son menos si las comparamos con las opciones que proporcionan los dos navegadores analizados anteriormente Google Chrome y Firefox.

Tal y como hemos observado, numerosos sitios *web* requieren el uso de *cookies* para poder prestar sus servicios a los usuarios, con lo cual se debería habilitar el uso de *cookies* en el navegador y no seleccionar la opción de bloquear siempre *cookies* y otros datos de sitios *web*.

El navegador Safari, en relación al tratamiento que debe hacer de las *cookies*, permite seleccionar entre dos opciones más. La primera es nunca bloquear *cookies* y otros datos de sitios *web* y la segunda es bloquear solo las de publicidad y terceros. La opción más recomendable para el usuario, de cara a su privacidad, es permitir el uso de *cookies* pero bloqueando las *cookies* y otros datos de sitios *web* de publicidad y terceros.

El navegador Safari, tal como ocurría con el navegador Google Chrome, sí que permite limitar el acceso, a sitios *web,* al servicio de localización. Las tres opciones que ofrece son: Preguntar una vez al día para cada sitio *web*, Preguntar una sola vez para cada sitio *web* y Denegar sin avisar. Debido a que algunos sitios *web* requieren conocer la ubicación del usuario para ofrecer sus servicios, se ha descartado la opción de Denegar sin avisar. Las otras dos opciones permiten la localización del usuario y se recomienda Preguntar una vez al día para cada sitio *web*, ya que esta opción permite al usuario recordar más fácilmente qué sitios *web* requieren conocer su ubicación notificándole una vez al día.

A partir de esta configuración se han visitado los tres sitios *web* utilizados para realizar el análisis del funcionamiento de los navegadores y se ha detectado que no ha habido problemas de acceso a los mismos, y que una vez que el usuario se ha autenticado frente a un sitio, no es necesario que se vuelva a autenticar incluso si el navegador ha sido cerrado y se ha vuelto a abrir.

Seleccionando esta configuración, el navegador sólo ha almacenado *cookies* de aquellos sitios a los que el usuario ha deseado acceder, a pesar de que muchas de las páginas visitadas de los sitios contenían numerosas *cookies* de terceros.

Al realizar las mismas visitas, pero configurando el navegador de forma que nunca bloquee *cookies* ni información de lo sitios *web*, el número de *cookies* almacenadas pasa de 6 a 39. Por tanto, en este caso se han registrado 33 *cookies* no necesarias para proporcionar los servicios al usuario. Así se confirma que, de cara a la privacidad del usuario, es deseable configurar el navegador de forma que bloquee *cookies* e información de sitios anunciantes y terceros.

7. CONCLUSIONES

La utilización de *cookies* es una práctica extendida en la mayoría de los sitios *web*. Sin la utilización de ellas no hubiera sido posible proporcionar los innumerables servicios que están disponibles para los usuarios de Internet a través de los sitios *web*, servicios que actualmente son indispensables en muchos casos y que sería imposible su implementación sin Internet, o servicios que pueden prestarse de una forma más rápida y cómoda para el usuario.

Coincidimos con Hal Berghel cuando afirma en su artículo Toxic *Cookies*: "El problema que la sociedad tiene que tratar es si debe tolerarse la recopilación de información personal sobre las personas sin el consentimiento de la persona". Una vez concienciadas las partes involucradas (legisladores, sitios *web*, usuarios, etc) y regulado adecuadamente el uso de las *cookies*, no debería implicar su utilización ningún problema, de forma que estas puedan proporcionar una serie de servicios a los usuarios sin comprometer su privacidad. Evidentemente, la regulación, para que sea efectiva, necesitará que los organismos dispongan de las herramientas y medios necesarios para hacer cumplir la normativa reguladora.

El análisis teórico del comportamiento de los navegadores en relación a la privacidad de los usuarios descrito en este trabajo, nos ayuda a entender que el problema no es el hecho de utilizar *cookies* para que los sitios *web* puedan implementar servicios. El problema radica en las prácticas que son realizadas por algunas entidades para obtener algún tipo de beneficio a través del uso de estas. Un uso inadecuado puede implicar una intrusión en la privacidad de los usuarios.

Está claro que los usuarios deberían ser conscientes de los posibles riesgos respecto de la privacidad a los que están expuestos cuando navegan a través de Internet. Algunos estudios revelan que un amplio porcentaje de los usuarios de Internet borran las *cookies* almacenadas habitualmente, probablemente porque han oído hablar de cómo la utilización de *cookies* puede afectar a su privacidad. Pero generalmente el conocimiento que tienen los usuarios de la tecnología que se aplica al usar las *cookies* es limitado y en muchos casos inexistente.

La primera recomendación para los usuarios respecto de lo mejor que se puede hacer cuando se utilizan las *cookies* es estar informado acerca de los problemas de seguridad que pueden suponer su uso y las últimas técnicas para prevenir ataques. Adicionalmente, es aconsejable que el usuario esté al día de los servicios que proporcionan las últimas versiones de los navegadores, actualizándolos para evitar vulnerabilidades de seguridad que son solucionadas con las nuevas versiones.

Independientemente del grado de conocimiento que tenga el usuario, y debido a la necesidad de convivir con las *cookies,* la opción más recomendable para el usuario es la de configurar el navegador *web* de forma que el uso de las *cookies* se adapte a los niveles de seguridad y privacidad requeridos por parte de este. Tal y como se ha comentado en este trabajo, numerosos sitios *web* hacen uso de *cookies* para proporcionar sus servicios, lo cual implica que las *cookies* sean imprescindibles para el correcto funcionamiento de la mayoría de los sitios *web*.

Antes de configurar el navegador *web*, el usuario deberá analizar **quiénes son los usuarios** que tienen acceso y harán uso del navegador instalado en el ordenador. La configuración del navegador respecto de la privacidad puede diferir si el ordenador es compartido o si por el contrario es utilizado por una única persona. Si el ordenador es utilizado por más de una persona, la opción más recomendable es evitar que la información que pueda ser almacenada durante una sesión de navegación por un usuario pueda ser utilizada por otro usuario que utilice el navegador a posteriori.

Hoy en día la mayoría de navegadores proporcionan la opción del **modo de navegación privado**, y en el caso de que el ordenador sea compartido, la opción más sencilla y más conveniente es la de utilizar este modo de navegación, ya que permite al usuario evitar que las *cookies* persistentes queden almacenadas entre sesiones. Si se selecciona esta opción de navegación, las *cookies* serán utilizadas como si fueran *cookies* de sesión.

Cada navegador ofrece a los usuarios diferentes opciones y el primer paso que se deberá realizar es **seleccionar el navegador que sea más conveniente** debido a la facilidad de uso, a las prestaciones que este le ofrece respecto de la seguridad y privacidad y a las opciones de gestión de las *cookies*. El navegador proporciona cierto control sobre las *cookies*, ya que estas serán aceptadas, rechazadas o eliminadas dependiendo de la configuración establecida por el usuario.

Como ya se ha mencionado, **la opción de no permitir *cookies* o desactivar *cookies* no es conveniente** ya que no nos permitiría acceder a los servicios ofrecidos por muchos sitios *web*. Adicionalmente, el hecho de bloquear las *cookies* es a menudo inefectivo a la hora de conseguir un mayor grado de privacidad, en el caso de que los servidores utilicen las restricciones para conseguir rastrear las actividades de los usuarios.

Algunos navegadores, como por ejemplo Mozilla Firefox, ofrecen la opción de aprobación una a una de las *cookies*, de manera que cuando un sitio *web* quiera almacenar una *cookie* en el navegador, el usuario recibirá un mensaje preguntando al usuario si aprueba o rechaza que la *cookie* o *cookies* de un determinado sitio sean guardadas. Algunos usuarios pueden considerar molestas la cantidad de mensajes que reciben, sin embargo, otros, conscientes de los problemas que pueden acarrear el uso de las *cookies*, no consideran los mensajes una molestia y se sienten más seguros decidiendo ellos qué *cookies* se deben guardar.

Una opción adicional que mejorará la privacidad de los usuarios es la utilización de programas específicos, llamamos *cookies cleaners*, los cuales son utilizados para detectar compañías que intentan almacenar *cookies* en el dispositivo del usuario o que pueden eliminarlas del sistema.

Internet no salvaguarda el derecho a la privacidad de los usuarios que acceden a los servicios que proporcionan los sitios web. Una correcta configuración del navegador utilizado por el usuario, junto con la ayuda de nuevas normativas que regulan el uso de las tecnologías, proporcionan herramientas que mejoran la privacidad de los usuarios y dificulta que determinados sitios web puedan obtener información privada de los usuarios. Aunque tal y como se ha demostrado, a pesar de que el usuario seleccione no ser rastreable, no se garantiza que los sitios web no obtengan información desde el navegador sin su autorización. La opción de satisfacer el deseo de no rastreo de un usuario, es voluntaria para el sitio *web* y no de obligado cumplimiento por parte de este.

En cualquier caso, conviene recordar que la seguridad cien por cien no existe en general, y tampoco referida a la privacidad relacionada con las *cookies*.

BIBLIOGRAFÍA

Redes de computadoras: Un enfoque descendente –James F. Kurose & Keith W. Ros - Pearson Prentice Hall – Ed 5 – 2010

Redes de computadoras – Andrew S.Tanenbaum - Pearson Prentice Hall – Ed 4 - 2003

Transmisión de datos y redes de comunicaciones – Behrouz A. Forouzan – McGraw Hill – Ed 4 – 2006

Comunicaciones y Redes de Computadores – William Stallings - Pearson Prentice Hall – Ed 7 – 2004

Internet *Cookies*: Security Implications. Simon Perkins - 2000

HTTP *Cookies*: Standards, Privacy, and Politics – David M. Kristol – 2001

The Unofficial *Cookie* FAQ Version 2.6 – *Cookie* Central - David Whalen - 2008

Browse at Your Own Risk – Nick Nikiforakis & Günes Acar -North American - Spectrum.IEEE.Org – Agosto 2014

Toxic *Cookies* – Hal Berghel – University of Nevada (Las Vegas) – IEEE Computer Society – 2013

Protecting *Cookies* from Cross Site Script Attacks Using Dynamic *Cookies* Rewriting Technique – Rattipong Puttthacharoen, Pratheep Bunyathnoparat – Advanced Communication Technology (ICACT) – 13 -16 de Febrero de 2011

Directiva de la Unión Europea de 2002 sobre la privacidad en las telecomunicaciones (Directiva 2002/58/CE)

Wikipedia- Brian Quinton: Study: Users Don't Understand, Can't Delete *Cookies*. Disponible: http://searchinfo.com/InsightExpress_*cookie*_study/ - 18 de mayo de 2005

Wikipedia website [Online]. Disponible: https://es.wikipedia.org/wiki/Cookie_(informática) - 15 de Marzo de 2016