

Actividad 2: Informe sobre privacidad

Seguridad Informática

Orquidea Seijas

Escola Técnica Superior de Enxeñería

CONTENIDO

1.	Resumen de la sesión.....	2
a.	Pruebas realizadas con ficheros de ejemplo.....	2
i.	Prueba con el archivo prueba_poner_quitar.html	2
ii.	Prueba realizada con el archivo contador.html	3
iii.	Pruebas realizadas con el archivo cookies_usuario.html	3
iv.	Pruebas realizadas con el archivo mostrar_mensaje_inicio.html	5
	Ejemplos de cookies reales	5
b.	Ejemplos de web bugs reales.....	6
i.	Web bug de la página principal de La Vanguardia:.....	6
ii.	Web bug de la página principal del usuario en Tumblr.	7
c.	Opinión personal sobre cómo afectan las cookies y los web bugs la privacidad en la red.....	7
d.	Política de privacidad de Google.....	7
i.	Tipos de cookies utilizadas por Google	8
ii.	Opinión de Google sobre el “derecho al olvido”	8
2.	Guía para la configuración óptima de un equipo, desde el punto de vista de la privacidad.....	9
a.	Características del equipo y usuario seleccionados.....	9
b.	Configuración inicial.....	10
c.	Configuración de la aplicación para Google Chrome.....	13
d.	Configuración del navegador secundario: Opera Mini	15
	Referencias.....	16

1. RESUMEN DE LA SESIÓN

a. PRUEBAS REALIZADAS CON FICHEROS DE EJEMPLO

Al abrir cada uno de los archivos de ejemplo, se pudo comprobar que en *Google Chrome* no estaba funcionando de la forma apropiada. Por esta razón, se decidió utilizar *Mozilla Firefox* como siguiente navegador para realizar las pruebas. En este, aparentemente, el comportamiento era el deseado.

i. Prueba con el archivo *prueba_poner_quitar.html*

El primer archivo que se abrió fue *prueba_poner_quitar.html*. Al principio, aparecía el dialogo de la *Ilustración 1*, que es la primera *cookie* de la web. Esta *cookie* se activa al abrir la web a través del método *Set_Cookie*. Al presionar aceptar, salta el siguiente diálogo, *Ilustración 2*, que, tal y como se pudo comprobar en el código proporcionado, se borra la *cookie* con *Delete_Cookie*, dando lugar a que, cuando se llama a *Get_Cookie* se produzca el caso de ninguna *cookie* almacenada y, por lo tanto, aparezca el mensaje que aparece en el *pop-up* en lugar de “Funciona”.

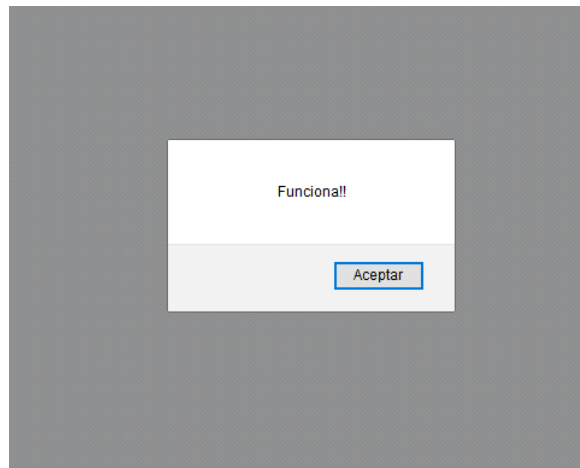


Ilustración 1 Primer diálogo emergente de prueba_poner_quitar.html

Finalmente, al hacer *click* en aceptar, se accede, finalmente, a la web a la que se pretendía acceder en un principio.

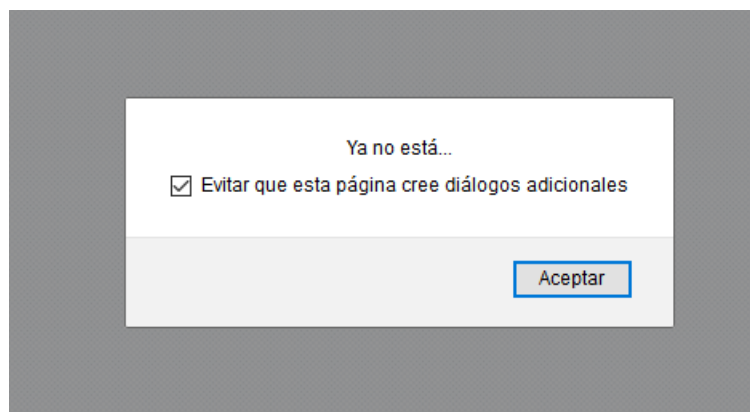


Ilustración 2 Segundo diálogo emergente.

ii. Prueba realizada con el archivo *contador.html*

En este caso, se realizó una prueba con el archivo *contador.html*. La función principal de esta *cookie* es contar cuantas veces se accede a una página desde una misma IP y un mismo navegador. Esta *cookie* es especialmente útil para los administradores de una web, ya que pueden controlar cuántas veces accede una persona a la web, que puede ayudar a ofrecer una experiencia más personalizada o a mejorar las estadísticas de uso de la web.

El diálogo flotante cambia según se va visitando la web. En primer lugar, el mensaje es: "Welcome to my page", como se puede ver en la Ilustración 3. Este mensaje va cambiando la segunda, la tercera y hasta la décima vez que se visita. A partir de esa vez, el mensaje es siempre el mismo, tal y como se puede ver en la Ilustración 4. Esto se programa a través de un *script* en *JavaScript* que accede al contenido de la *cookie* y enseña un mensaje diferente en función del mismo.

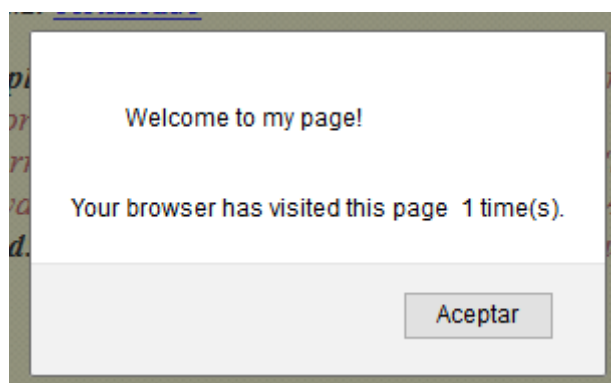


Ilustración 3 Primera visita en *contador.html*

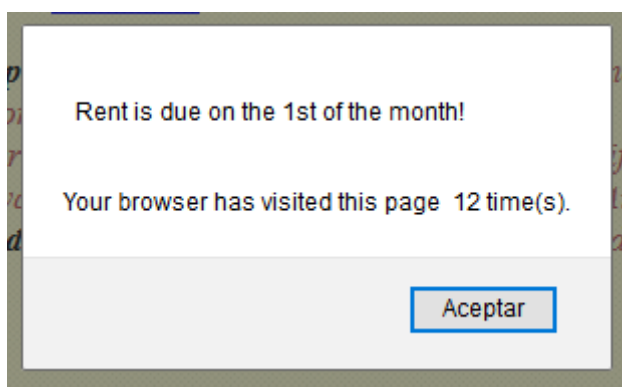
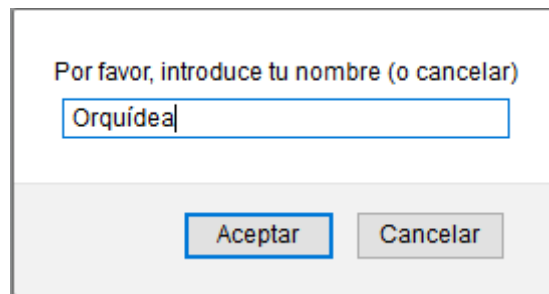


Ilustración 4 décima segunda visita en *contador.html*

iii. Pruebas realizadas con el archivo *cookies_usuario.html*

La siguiente prueba que se realizó fue con *cookies_usuario.html*. En este caso, el primer diálogo flotante que apareció fue el de la Ilustración 5, en el que se solicitaba introducir un nombre o cancelar. Esto sucede porque la *cookie* se ejecuta por primera vez y, por lo tanto, es necesario proporcionarle valores. Al introducir el nombre, la Librería de Cervantes se actualizaba y personalizaba,

como se puede ver en la Ilustración 6. En caso de no introducirlo, saltaba el diálogo de la Ilustración 7 y, finalmente, se podía acceder a la página web, como se puede ver en la Ilustración 8.



Por favor, introduce tu nombre (o cancelar)

Orquídea

Aceptar Cancelar

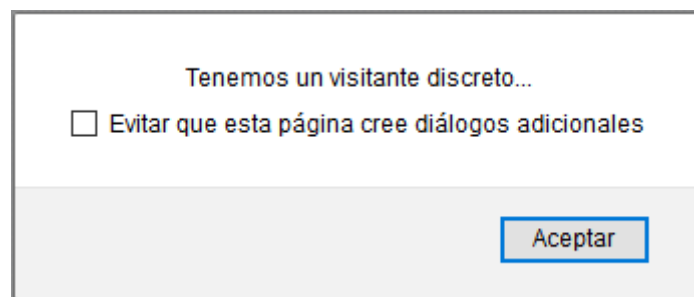
Ilustración 5 Primer diálogo de cookies_usuario.html

¡Hola, Orquídea! Bienvenido a la Librería Cervantes

Con motivo de la reciente celebración del IV Centenario del Quijote, la obra más ilustre de la literatura española, se ha elaborado un importante catálogo de publicaciones relacionadas con esta obra, además de numerosos regalos.

Le animamos a visitarnos cuanto antes en nuestro sitio web www.cervantes.com

Ilustración 6 Página personalizada



Tenemos un visitante discreto...

☐ Evitar que esta página cree diálogos adicionales

Aceptar

Ilustración 7 Diálogo que aparece si se hace click en "cancelar"

¡Hola, visitante! Bienvenido a la Librería Cervantes

Con motivo de la reciente celebración del IV Centenario del Quijote, la obra más ilustre de la literatura española, se ha elaborado un importante catálogo de publicaciones relacionadas con esta obra, además de numerosos regalos.

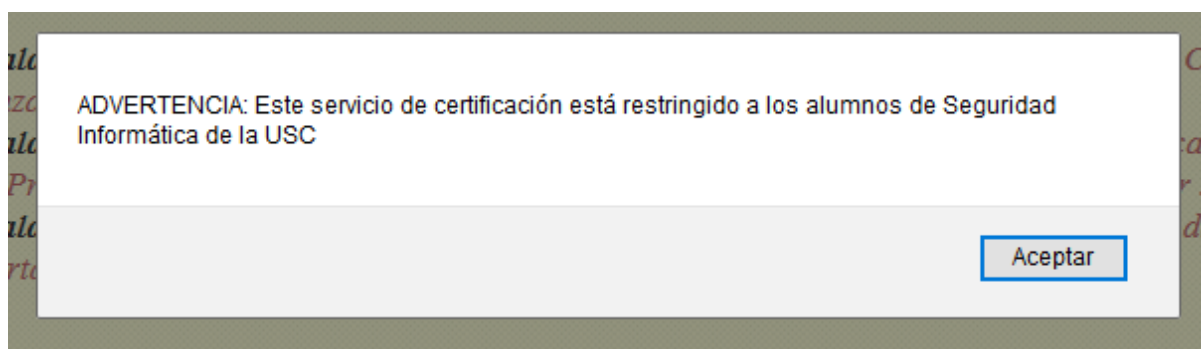
Le animamos a visitarnos cuanto antes en nuestro sitio web www.cervantes.com

Ilustración 8 Página web sin personalizar

Una vez se le proporcione información a la cookie por primera vez, mientras siga existiendo, no volverá a preguntarle al usuario por su nombre para la personalización de la Librería Cervantes.

iv. Pruebas realizadas con el archivo *mostrar_mensaje_inicio.html*

A continuación, se procedió a abrir el archivo *mostrar_mensaje_inicio.html* en el navegador. Este archivo cuenta con una *cookie* que enseña un *pop-up* la primera vez que se entra en la página web (Ilustración 9) y que no vuelve a lanzarlo mientras no se borre.



EJEMPLOS DE COOKIES REALES

A continuación, se proporcionarán dos ejemplos diferentes de *cookies* reales que se pudieron encontrar en el navegador principal, *Google Chrome*, del estudiante.

Origen	Nombre	Domino
https://cv.usc.es/	MoodleSession	cv.usc.es

Esta *cookie* almacena las credenciales del usuario del campus virtual de la Universidad de Santiago de Compostela de forma local. Se realiza esta acción para poder permitirle al usuario mantener la sesión iniciada sin tener que volver a escribir las credenciales cada vez que cambie de zona dentro del campus virtual o incluso si cierra la pestaña asociada al mismo. El nombre de la *cookie* hace referencia a la plataforma del campus virtual, *Moodle*, y a su función, asociada con el tipo de *cookie* que es.

Esta *cookie* caduca una vez se cierre el navegador, puesto que se considera que ya no es necesario mantenerla activa. Una vez el usuario cierra el navegador, se infiere que ya ha realizado todo lo que necesitaba en ese momento y por lo tanto no es necesario mantenerla activa. De hecho, puede ser perjudicial para el usuario si se mantiene la sesión una vez se cerró implícitamente a través del cierre del navegador.

Origen	Nombre	Dominio
https://es.wikibooks.org/	WMF-Last-Access	es.wikibooks.org

Esta *cookie* almacena datos de forma local para saber cuándo fue la última vez que se accedió al sitio y para contar cuantas veces se accede a un sitio en un período determinado. Pueden darse dos posibilidades para esta *cookie*: que no exista aún o que esté inicializada, con el valor de la fecha de último acceso.

Si se da el primer caso, la *cookie* sin inicializar, se inicializa una que incluya la fecha y una fecha de expiración. Debido a que este tipo *cookie* suele ser analizada mensualmente, con que sea mayor que un mes la fecha de expiración, servirá.

Para el segundo caso, se creará una nueva *cookie*, con la fecha de expiración mayor que un mes, y el valor anterior de la *cookie* se incluirá a través de una modificación en la cabecera, que suele ser *X-Analytics*. Estas *cookies* pueden ser utilizadas para leer accesos que se produzcan una única vez, ya que solo se modifica la cabecera si se accede más de una vez durante el tiempo que esté activa la *cookie*. Sin embargo, este método únicamente tiene en cuenta usuarios que aceptan *cookies*, por lo que siempre será una cuantía que representa menos de los usuarios que accedieron realmente a la web (usuarios que no aceptan *cookies* no serán contabilizados al no poder inicializarla).

b. EJEMPLOS DE WEB BUGS REALES

Un *web bug*, tal y como se estudió en clase de teoría, es una etiqueta electrónica que ayuda a las páginas web y a los anunciantes a rastrear dónde se encuentran los usuarios de las mismas. Son similares a las *cookies*, pero los *web bugs* son prácticamente indetectables ya que la única forma de detectarlos es accediendo al código html asociado a la web. Este elemento de la web se caracteriza por ser una imagen (u otro tipo de elemento) de 1x1 píxel. Donde debería indicarse la dirección de la imagen, se indica un enlace a una web, que suele ser de publicidad o de recogida de datos.

Cabe la posibilidad de que un *web bug* y una *cookie*, se comuniquen. Si un usuario visita una página web que utilice *cookies* y *web bugs* de una empresa A, el *web bug* podrá acceder al identificador de la *cookie*, que enseña el comportamiento previo de ese usuario en ese navegador. Una vez obtenga esos datos, podrá volver al servidor de la empresa A y se podrán almacenar estos datos asociados a una *cookie* y, por tanto, a una localización. Esto para el usuario medio es un problema, ya que por regla general no sabrá lo que está sucediendo con sus datos.

Puesto que para los ejemplos de *cookies* reales se seleccionaron dos ejemplos, también se han seleccionado dos ejemplos de *web bugs*, para estudiar su uso y funcionamiento.

i. Web bug de la página principal de La Vanguardia:

```
<iframe src="https://la-vanguardia-prod-by.accengage.net/pushweb/assets/m_main.html?" width="1" height="1" name="acc_proxy" style="border: none;"></iframe>
```

En este caso, se ha seleccionado un *web bug* de La Vanguardia, que utiliza el elemento *HTML iframe* para su realización. Este *web bug* está relacionado con la empresa *Accengage*, solución de *Google* para crear notificaciones *push*. Las notificaciones *push* pertenecen a la llamada tecnología *push*, que principalmente se utiliza para enviar notificaciones desde el servidor al cliente sin que sea necesario que esté pidiendo explícitamente cada notificación.

Así pues, este *web bug*, por lo que se pudo estudiar a partir de la página web principal de *Accengage*, sirve principalmente para configurar el servicio de mensajes o notificaciones automáticas al usuario.

ii. Web bug de la página principal del usuario en Tumblr.

```
<iframe height="1" width="1" frameborder="0" style="position:absolute;top:0;left:0;visibility:hidden:pointer-events:none;" tabindex="-1" allowtransparency="true" src="https://cookietex.ngd.yahoo.com/v2/cexposer/SIG=11lum9jej/*https%3A//www.tumblr.com/yahoo_cookie_receiver.html"></iframe>
```

Para el segundo caso, se ha seleccionado un *web bug* de la red social *Tumblr*, que se basa en *blogging*. Puesto que *Tumblr* es propiedad de *Yahoo*, el *web bug* redirige la información a los servidores de *Yahoo*, para realizar las acciones que sean necesarias con los datos obtenidos. Tal y como se puede ver en el código adjuntado, no se desea de ninguna forma que el usuario medio sea consciente de la existencia del *web bug* y por lo tanto se hace todo lo posible por mantenerlo oculto con `visibility:hidden` y `allowtransparency="true"`.

C. OPINIÓN PERSONAL SOBRE CÓMO AFECTAN LAS COOKIES Y LOS WEB BUGS LA PRIVACIDAD EN LA RED

Tal y como se pudo ver a partir de los ejemplos vistos en clase y los ejemplos reales estudiados en el informe tanto de *web bugs* como de *cookies*, estos elementos están por todo Internet y muchas veces ni siquiera sabemos que están ahí a menos que los busquemos específicamente. La mayoría de los usuarios están acostumbrados a aceptar las *cookies* sin siquiera saber que las pueden rechazar y es por ello por lo que las empresas de publicidad, entre ellas Google Analytics, obtienen más información de la que podrían obtener si fuéramos más responsables con nuestros datos.

Las *cookies* y los *web bugs* son herramientas utilizadas por empresas para su beneficio, pero no tiene por qué ser malo para los usuarios siempre y cuando sean conscientes de que están siendo monitorizados en mayor o menor medida. Es necesario crear una conciencia colectiva sobre privacidad en Internet y cómo no es necesario aceptar directamente todo lo que nos proponen. Es posible acceder a un servicio y que siga siendo funcional, aceptando las *cookies* propias y no las de terceros, por ejemplo. También es necesario intentar saber qué datos nuestros tienen las empresas y cómo los gestionan, aunque esto puede ser más complicado debido a la existencia de los *web bugs*. Así pues, se puede concluir que la privacidad se puede recuperar, o al menos empezar a hacerlo, siendo conscientes de lo que estamos compartiendo.

d. POLÍTICA DE PRIVACIDAD DE GOOGLE

En este apartado se recogerá un breve resumen de la política de privacidad de *Google*, los diferentes tipos de *cookies* empleadas por *Google* y la postura de *Google* respecto al “derecho al olvido” por parte de un usuario.

La política de privacidad de *Google* principalmente expone qué datos recoge, para qué lo hace, cómo los utiliza y qué opciones ofrece para acceder a esos datos y actualizarlos, entre otros. Esta solo se aplica a servicios suministrados por *Google* y sus filiales. La política se podrá modificar en cualquier momento.

En primer lugar, se habla de cómo se recogen los datos: puede ser información que proporciona el usuario explícitamente cuando se le pide o puede ser información obtenida a partir del uso de los servicios de *Google*. En este caso, se pueden incluir en los datos recogidos por la empresa

la información del dispositivo, los datos de registro, datos sobre la ubicación física del usuario, números exclusivos de aplicación, almacenamiento local y *cookies* o tecnologías similares.

A continuación, se explica cómo se utilizan los datos recogidos. En la política de privacidad, se listan una serie de acciones tales como: para proporcionarlos, mantenerlos, mejorarlos, para proteger a *Google* y a sus usuarios; y para ofrecer contenido personalizado relevante para el usuario. El tratamiento de estos datos se realiza en los servidores de *Google*.

En el siguiente apartado de la Política de privacidad se habla de cómo se puede informar al usuario sobre los datos que recoge *Google* con el fin de poder tomar decisiones apropiadas sobre su privacidad.

A continuación, se habla de cómo compartir y eliminar contenido. También se habla de que se pueden actualizar o eliminar los datos que tiene *Google* sobre un usuario concreto pero que cabe la posibilidad de que se rechace esta petición bajo el criterio de la empresa.

En el siguiente apartado se comenta qué datos se comparten y con quién. *Google* comparte información personal con empresas o particulares ajenos siempre y cuando: el usuario haya dado consentimiento explícito, si la cuenta es gestionada por un administrador de dominio, si el procesamiento de los datos lo lleva una empresa externa a *Google* o por motivos legales. La información de carácter no personal se puede compartir de forma pública.

Finalmente, en relación con la seguridad del usuario, *Google* intenta evitar cualquier modificación, divulgación, acceso o destrucción no autorizada de los datos. También intenta verificar el cumplimiento de su política de privacidad constantemente con marcos de autorregulación.

i. Tipos de *cookies* utilizadas por *Google*

Google utiliza varios tipos de *cookies* para el correcto funcionamiento de los productos relacionados con los anuncios y los sitios web. En primer lugar, utiliza *cookies* de preferencias, para que las webs que los usuarios visitan cambien en función de los mismos. También utiliza *cookies* de seguridad, con el fin de poder autenticar a los usuarios de forma segura. Para permitir correctamente el funcionamiento de algunos sitios web, se utilizan las *cookies* de procesos. Las *cookies* de publicidad se utilizan para que la publicidad sea más personalizada y, por lo tanto, más efectiva para los usuarios. Las *cookies* de estado de la sesión permiten recopilar información sobre la forma en la que los usuarios interactúan con una web. Finalmente, las *cookies* de *Google Analytics* se utiliza para recopilar información sin identificar personalmente a los visitantes de *Google*.

ii. Opinión de *Google* sobre el “derecho al olvido”

En general, parece que el fallo del Tribunal de Justicia Europeo puso en una posición complicada a *Google*, ya que, aunque parece una tarea trivial, decidir si alguien tiene derecho al olvido o no, no es fácil. Es una tarea ardua y delicada: si es información sobre la que hay un interés público, o puede haberlo, debería seguir en la red, pero decidir si esta información entra en esa categoría es algo subjetivo. Además, tienen que destinar personal especializado a realizar esta tarea, con el impacto monetario que implica el volumen de peticiones que tienen.

En este momento, parece que están intentando hallar una solución que acate la ley, más allá de revisar caso por caso personalmente.

2. GUÍA PARA LA CONFIGURACIÓN ÓPTIMA DE UN EQUIPO, DESDE EL PUNTO DE VISTA DE LA PRIVACIDAD

a. CARACTERÍSTICAS DEL EQUIPO Y USUARIO SELECCIONADOS

Para esta tarea se ha seleccionado un dispositivo móvil, ya que no se suele utilizar el navegador como aplicación de acceso principal a Internet. El dispositivo seleccionado es un *IPad 4*, con iOS 10.3.3. El navegador principal es *Google Chrome* y el navegador secundario es *Opera Mini*. Se realizarán cambios en la configuración de seguridad actual.

La usuaria principal de esta *tablet* es la estudiante que realiza la práctica. Sin embargo, no es un dispositivo que utilice habitualmente y por lo tanto no se han realizado cambios en las opciones de seguridad que están por defecto en el *IPad*. A este *IPad* se accede a través de un pin de cuatro dígitos. En contadas ocasiones, el dispositivo es utilizado por miembros de su familia y para esos casos tiene el navegador *Opera Mini*, que se utiliza con el fin de no mezclar sus datos con los datos temporales de la familia.

Para realizar correctamente una configuración de un equipo, hay que revisar la configuración inicial y analizarla. Es posible que haya ajustes por defecto que le sirvan a un usuario concreto. Por ejemplo, en este caso, la comodidad de poder tener todo sincronizado con diferentes dispositivos prevalecería sobre la inseguridad de tenerlo todo sincronizado. Sin embargo, dar permisos relacionados con aspectos de privacidad a aplicaciones que no lo necesitan explícitamente, es algo que se considerará inseguro y que las ventajas que ofrecen no compensan.

A continuación, se mostrarán una serie de pasos que se siguieron y que se deberían seguir para realizar la configuración apropiada para este caso concreto.

b. CONFIGURACIÓN INICIAL

En primer lugar, se decidió acceder al menú de configuración del *iPad* con el fin de configurarlo apropiadamente:

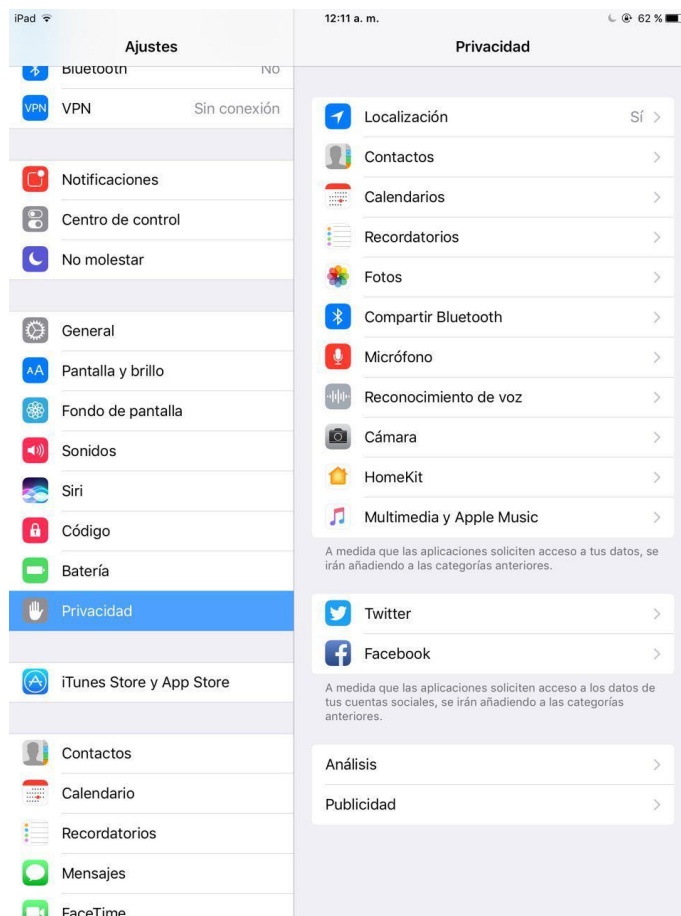


Ilustración 9 Privacidad

En primer lugar, se accedió al apartado de privacidad, que se puede ver en la Ilustración 9. Se accedió por orden a los distintos elementos, así que, en primer lugar, se accedió a Localización. Las aplicaciones que comparten la localización informaron de ello en el momento de instalación, por lo que se dejaron los ajustes tal y como estaban (se puede ver en la Ilustración 10). Sin embargo, al acceder a “Compartir mi ubicación”, se pudo comprobar que estaba activado. Ese servicio se utiliza para que los contactos autorizados puedan conocerla localización del dispositivo en todo momento. Como no es un dispositivo de uso diario, no es necesario activar esta opción.

A continuación, se accedió a servicios del sistema con el fin de comprobar si todos los servicios que estaban utilizando la localización realmente la requerían. Tal y como se puede ver en la Ilustración 11, estaban todos activados salvo Mejorar mapas. Sin embargo, puesto que no se desea publicidad específica por zonas ni el servicio Busca mi *iPad* ni se poseen más elementos de *Apple* (*HomeKit* es un servicio para sincronizar *AppleTV* o elementos similares con dispositivos más tradicionales como un *iPad* o un *MAC*), se decidieron desactivar esos servicios.

Por otra parte, proporcionar información sobre el uso del *iPad* a *Apple* es una práctica que se considera aceptable ya que no hay datos sensibles en el dispositivo.

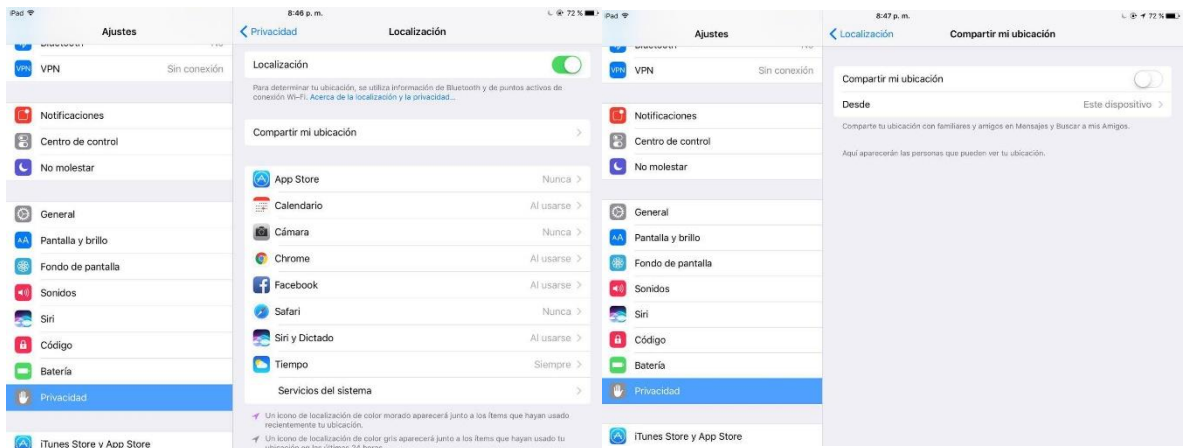


Ilustración 10 Localización y Compartir mi ubicación

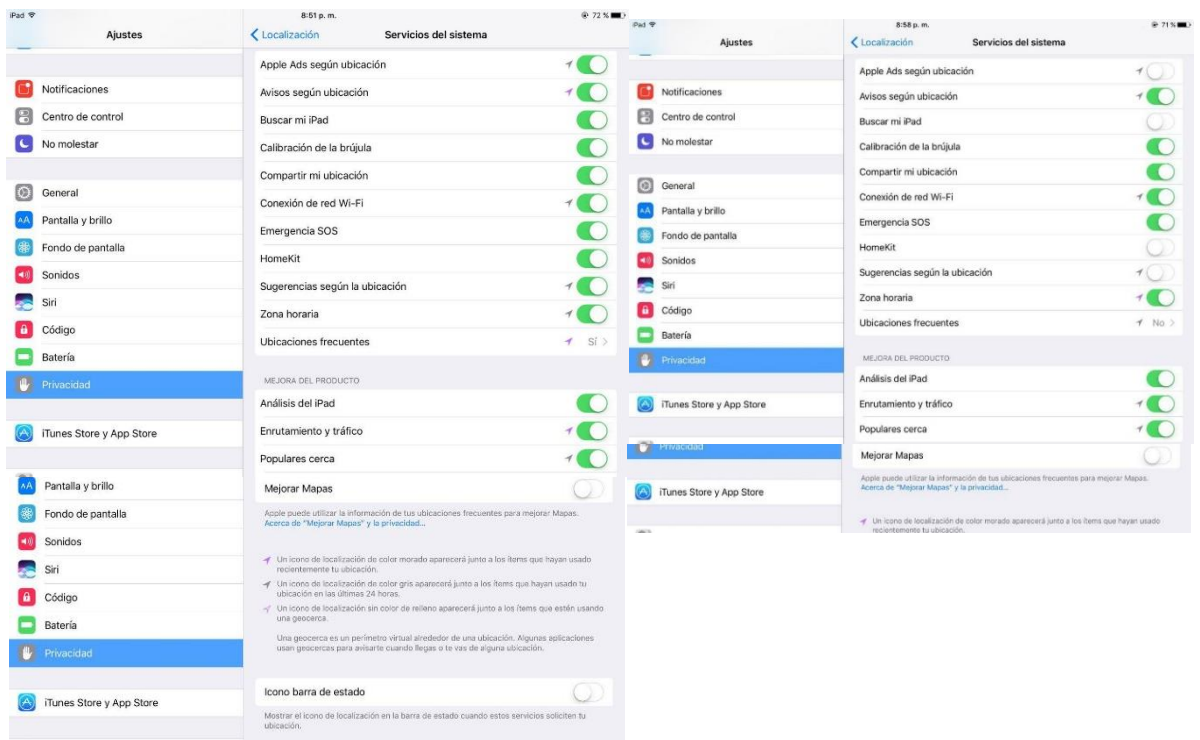


Ilustración 11 Servicios del sistema

A continuación, se accedió a Contactos. En este caso la única aplicación autorizada es la aplicación de mensajes *Telegram*, tal y como se puede ver en la Ilustración 12. Se decidió mantener este ajuste. Para los ajustes de la Cámara y de las Fotos, también, tal y como se puede ver en la Ilustración 13.

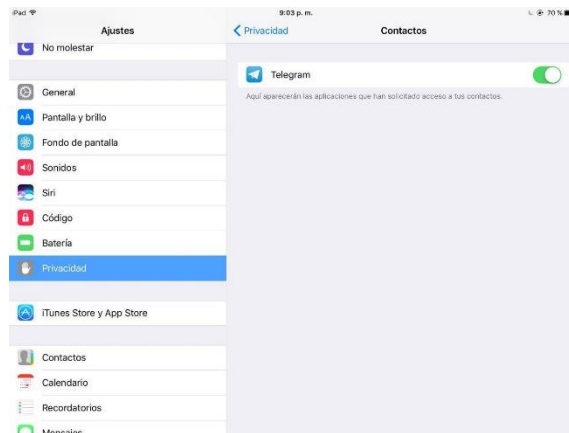


Ilustración 12 Contactos



Ilustración 13 Fotos y cámara

Para algunos de los servicios del *iPad* no había ninguna aplicación que accediera. Estos servicios son: calendarios, recordatorios, compartir *Bluetooth* y reconocimiento de voz.



Ilustración 14 Micrófono

Tal y como se puede ver en la Ilustración 14, los ajustes por defecto del Micrófono eran demasiado permisivos. Fue necesario modificarlos para que únicamente la aplicación de mensajería pudiera acceder al micrófono.

Esta fue toda la configuración realizada en general en el dispositivo. Para seguir asegurando que la configuración de seguridad fuera correcta, fue necesario actualizar la configuración de los navegadores utilizados habitualmente.

c. CONFIGURACIÓN DE LA APLICACIÓN PARA *GOOGLE CHROME*

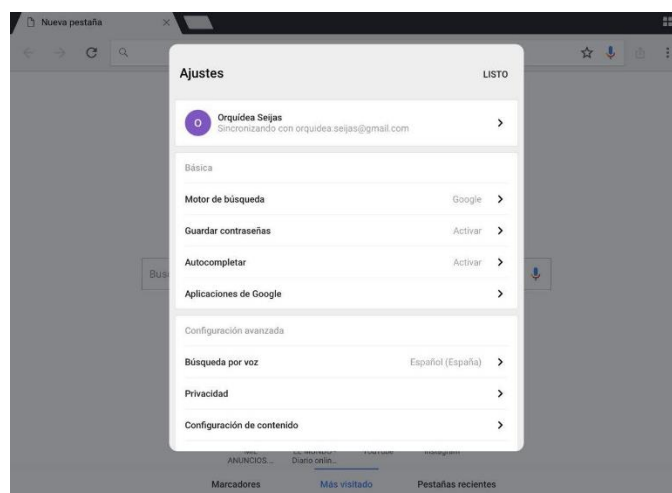


Ilustración 15 Ajustes del navegador principal

En primer lugar, se accedió al menú de ajustes para revisar las posibles opciones de personalización del navegador. Tal y como se puede ver en la Ilustración 15, el navegador está sincronizado con la cuenta principal de la autora de este informe de *Google*. Esto es así para poder tener sincronizados los dispositivos que se utilizan habitualmente tales como móvil y ordenador privados con los que no se usan habitualmente, como el *iPad*, que es utilizado como mucho un par de veces al mes, para que cuando se use no se note diferencia respecto a los demás. Es decir, se tienen sincronizados por comodidad y para una experiencia de uso satisfactoria. Están activadas las opciones de guardar contraseñas y autocompletar para facilitar el uso de la *tablet*, ya que es poco eficiente para escribir con el teclado virtual.

A continuación, se accedió al menú de privacidad, Ilustración 16. La opción *Handoff* estaba activada y se decidió desactivarla ya que no se posee ningún *AppleWatch*. A pesar de que se desea que sea cómodo y, a primera vista, podría parecer que no hace daño tenerla activada es mejor que si no se tiene el dispositivo de sincronización, no se pueda sincronizar. Se decidió dejar el resto como estaba por defecto: con la opción de mostrar sugerencias activada y con el envío de datos desactivado.

Para continuar con el análisis y configuración de la seguridad, Ilustración 17, se decidió acceder a los ajustes de sincronización para revisar si estaba todo correctamente sincronizado y para ver que no había elementos sensibles sincronizados. En primer lugar, se desactivó la opción de sincronizar todo, ya que no es necesario para este dispositivo. También se desactivó la sincronización de pestañas abiertas ya que se pueden estar realizando operaciones sensibles en alguno de los dispositivos de uso

habitual y no es necesario que se abran en el *iPad* si se accede al navegador. Por otra parte, la lista de lectura es un ajuste no relacionado con la seguridad.

Finalmente, se accedió al ajuste de autocompletar para observar qué se autocompletaba exactamente. En este caso, estaba activada la opción de “Mostrar direcciones y tarjetas de crédito de *Google Payments*”. Tal y como se comentó previamente, a través de este dispositivo no se realizan operaciones sensibles tales como compras. Es por ello por lo que no se desea ni se debe tener sincronizada esta opción y, por lo tanto, se desactivó.

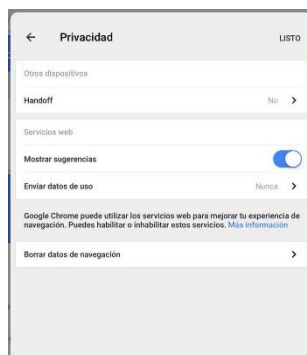


Ilustración 16 Ajustes de privacidad de Google Chrome

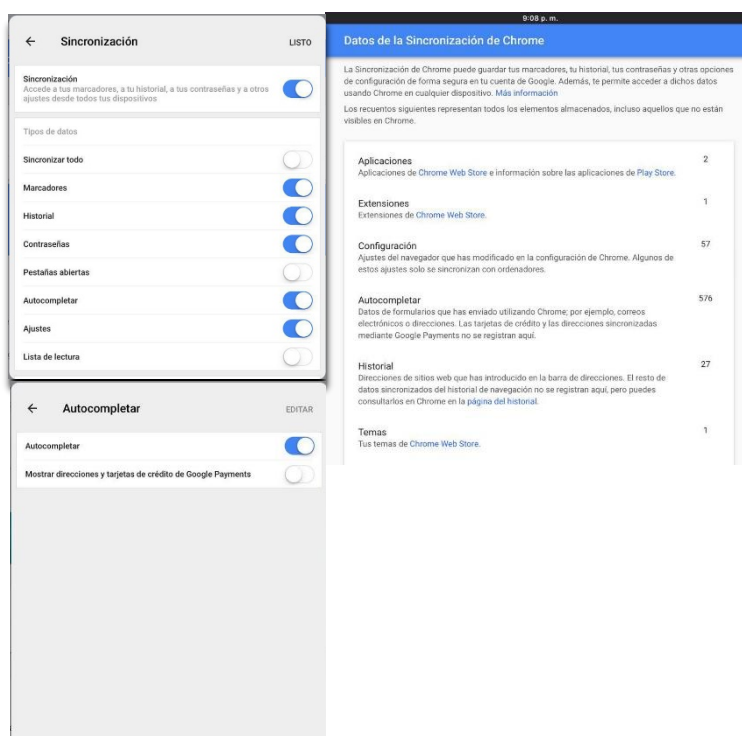


Ilustración 17 Sincronización de la cuenta principal con el navegador

d. CONFIGURACIÓN DEL NAVEGADOR SECUNDARIO: *OPERA MINI*

Para concluir la configuración de la seguridad del dispositivo actualizada, se decidió revisar las opciones del navegador secundario. En este caso, la única posibilidad de configuración encontrada relacionada con la seguridad fue la de desactivar las *cookies*. Siendo un navegador de uso esporádico y por usuarios ajenos al dispositivo, interesa guardar la menor cantidad de información posible y es por ello por lo que esta opción se desactivó.

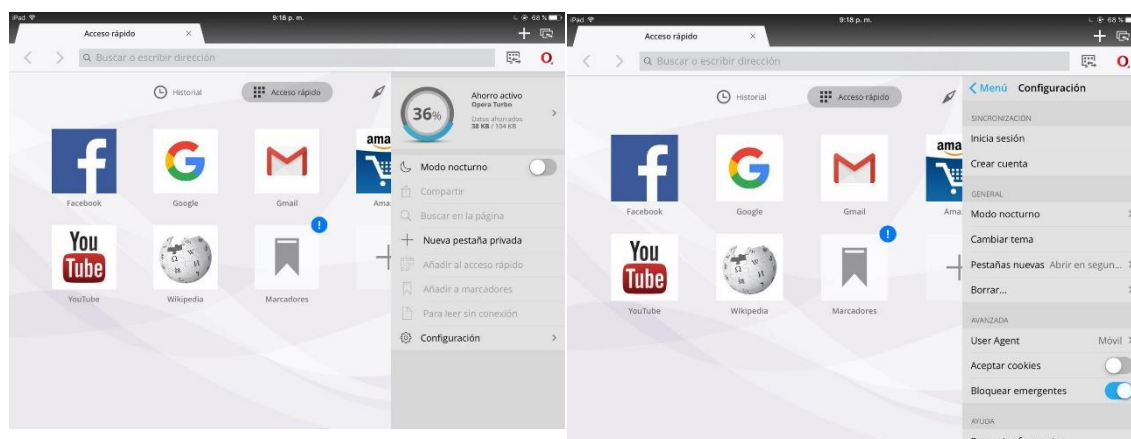


Ilustración 18 Ajustes del navegador secundario

REFERENCIAS

1. Stefanie Olsen. 2002. *Nearly undetectable tracking device raises concern*. <https://www.cnet.com/news/nearly-undetectable-tracking-device-raises-concern/> [Última visita: 28/09/2017]
2. Accengage. 2017. <http://accengage.net> [Última visita: 30/09/2017]
3. Wikitech. 2017. *Analytics/Data Lake/Traffic/Unique Devices/Last access solution*. https://wikitech.wikimedia.org/wiki/Analytics/Data_Lake/Traffic/Unique_Devices/Last_access_solution [Última visita: 29/09/2017]
4. Wikipedia. 2017. *Tecnología push*. https://es.wikipedia.org/wiki/Tecnología_push [Última visita 30/09/2017]
5. Google. 2017. *Política de privacidad*. <https://www.google.com/intl/es/policies/privacy/> [Última visita 30/09/2017]
6. Google. Preguntas frecuentes. <https://www.google.com/intl/es/policies/faq/> [Última visita 30/09/2017]