Actividad 2: Informe sobre privacidad

07/10/2014

Brais López Yáñez

ÍNDICE

OBJETIVOS DE LA PRÁCTICA

Los objetivos de esta práctica consistirán en una explicación detallada de:

- Cookies
- Web bugs
- Política de privacidad de google.
- Guía para la configuración óptima de un ordenador, desde el punto de vista de la privacidad.

Se intentará explicar los puntos anteriormente mencionados, para que una persona sin conocimientos informáticos técnicos los pueda entender y aprender sin dificultades.

INTRODUCCIÓN

En este 2014, y cada vez más en la actualidad estamos conectados por el gran invento revolucionario del siglo XX, internet,. Cada vez más los dispositivos cotidianos tienen acceso a la red: ordenadores personales, televisiones, móviles.

La conectividad global va a más, pero trae importantes desafíos que las sociedad del siglo XXI tiene que afrontar: ataques informáticos, privacidad personal, etc. ¿Cómo podemos resolver estos enigmas, ante un mundo cada vez más conectado?

COOKIES

¿QUÉ SON LAS COOKIES?

Las cookies son un mecanismo para facilitar la navegación de los usuarios en un entorno cambiante, estas forman parte del protocolo *http*. Su funcionalidad es guardar los datos y preferencias de la navegación de un usuario en el lado del navegador. Quedando almacenadas en el ordenador empleado para explorar internet.

VENTAJAS

La mayoría de las personas visitamos una gran cantidad de páginas webs. Esto trae consigo numerosos problemas y quebraderos de cabeza para el usuario. Seleccionar una determinada sección, un idioma, introducir un usuario con su respectiva contraseña, etc. Un ejemplo sería que una persona visite la misma página sucesivamente y necesite hacer una serie de pasos para conseguir la información que desee. Esto ha propulsado el nacimiento de las cookies.

DESVENTAJAS

Pero a parte de sus ventajas, también presenta grandes inconvenientes (como todo). A raíz del nacimiento de las cookies, y la adaptación de todos los navegadores hasta el momento (Netscape fue el primero en utilizarlas), muchas organizaciones y personas han querido sacarle el máximo provecho. Las empresas almacenan información de los propios usuarios para mejorar la experiencia con sus clientes y en muchas ocasiones para vender su información a

terceras empresas. Esto puede ser uno de los elementos por los que una persona se muestre receloso al uso de cookies.

Si esto fuera un problema, el verdadero dilema viene cuando no se tiene absoluto control de la sesión del ordenador/móvil/tablet con el que navegamos. ¿Por qué? Porque si almacenamos información de un usuario ,con su contraseña, de una página, estas se guardarán en las cookies (quedarán en el navegador). Puede darse el caso de que otra persona, no deseada, acceda a esa misma página y disponga de nuestros datos, guardados previamente con nuestra autorización. Esta persona no deseada, podrá cometer actos indeseados y que puedan traer graves consecuencias para nuestra vida.

EJEMPLO DE COOKIE

Google Analytics

Un ejemplo muy común de la mayoría de las páginas webs sería**, las cookies de terceros de Google Analytics,** estas cookies sirven para registrar la actividad de un determinado usuario. Su navegación, su procedencia, así como el tiempo que está en esa determinada página. Este tipo de cookies, no influyen en el usuario. Además se localizan en toda la website, es muy colocarlo en las cabeceras de las páginas, entre las etiquetas *<head></head>* de html.

Aquí, las cookies utilizadas por **GoogleAnalytics**:

Nombre de cookie	Duración	Descripción
_ga	2 años	Se usa para distinguir a los usuarios.

Nombre de cookie	Duración predeterminada	Descripción
__utma	Dos años a partir de la configuración o actualización	Se usa para distinguir usuarios y sesiones. La cookie se crea cuando se ejecuta la biblioteca JavaScript y no hay ninguna cookie __utma. La cookie se actualiza cada vez que se envían datos a Google Analytics.
__utmb	30 minutos a partir de la configuración o actualización	Se usa para determinar nuevas sesiones o visitas. La cookie se crea cuando se ejecuta la biblioteca JavaScript y no hay ninguna cookie __utmb. La cookie se actualiza cada vez que se envían datos a Google Analytics.
__utmc	Fin de la sesión del	No se usa en ga.js. Se configura para interactuar con

	navegador	urchin.js. Anteriormente, esta cookie actuaba junto con la cookie __utmb para determinar si el usuario estaba en una nueva sesión o visita.
__utmz	Seis meses a partir de la configuración o actualización	Almacena la fuente de tráfico o la campaña que explica cómo ha llegado el usuario al sitio. La cookie se crea cuando se ejecuta la biblioteca JavaScript y se actualiza cada vez que se envían datos a Google Analytics.
__utmv	Dos años a partir de la configuración o actualización	Se usa para almacenar datos de variables personalizadas de visitante. Esta cookie se crea cuando un programador usa el método _setCustomVar con una variable personalizada de visitante. También se usaba para el método _setVar obsoleto. La cookie se actualiza cada vez que se envían datos a Google Analytics.

****Un sitio que emplea analytics es: http://mentalidadfitness.com/.*

WEB BUGS

¿QUÉ SON LOS WEB BUGS?

Un web bug, o también llamado baliza web (en inglés web beacon), es una diminuta imagen imperceptible para el ojo humano o normalmente invisible (1pixel, generalmente), que se puede encontrar en una página web o en un mensaje de correo electrónico. Esta imagen es cargada desde una fuente externa a esa web, generalmente.

Un web bug, es muy dificil de localizar y de distinguir de otras imágenes que se cargan en una página. La razón es fácil, un 99% de páginas utilizan links y referenccias a otras páginas, importando contenido de estos sitios externos. Por esto, localizar un web bug es una tarea tediosa.

¿QUÉ FUNCIÓN TIENEN LOS WEB BUGS?

En un principio, los web bug son un medio importante en el análisis web. Suelen ser utilizados por terceros para controlar la actividad de los clientes en una página web. También se utilizan en correos electrónicos para determinar si el usuario leyó ese correo y la fecha en la que se produjo su lectura. Su fin sería el de monitorear al usuario y para labores de marketing.

El web bug es una herramienta que acompañada con otras es muy efectivo a la hora de determinar:

- Países de origen.

- Secciones más visitadas.
- Tiempo de permanencia en cada sección.
- Información del sistema operativo.
- Tipo de ordenador.
- Tipo de navegador.
- Palabras utilizadas en la búsqueda.

Todo esto puede ser aprovechado para fines que ayuden al usuario o todo lo contrario.

De las maneras negativas de utilizar los web bugs los destacados son ataques al usuario (conociendo de antemano las vulnerabilidades de programas), uso de estos para confirmación de correos electrónicos (una vez se aseguran de que esa dirección existe, se usa para envío de de emails fraudulentos), etc.

Además otro aspecto negativo destacado, es la monitorización total de nuestra actividad en internet a través del uso de cookies y web bugs. Dando lugar a una ausencia de privacidad, que la mayoría de las personas desconocen.

Ejemplo de Web Bug

Con unos conocimientos previos sobre web bugs, se puede reconocer uno, con trabajo y mucha paciencia. Para conseguirlo, lo que hay que hacer es rastrear el código html de las páginas. Concretamente la etiqueta <img>, y buscar imágenes de 1 pixel.

Si, todo eso concuerda, estaremos probablemente con toda seguridad ante un web bug. La última confirmación sería, acceder al dominio de la imagen, para ver de qué web se trata.

El ejemplo escogido es de un periódico muy común en Galicia, La voz de galicia.

Web bug: La voz de galicia

Encontrada justo antes del cierre del cuerpo: </body>. Del código html.

```
<noscript>
  <img src="http://logc279.xiti.com/hit.xiti?s=524867&s2=&p=&di=&an=&ac=" alt="" height="1" width="1" />
</noscript>
```

El dominio principal: http://xiti.com/, ofrece determinados productos sobre estadísticas y medición de páginas web. Confirmamos entonces de que se trata de un web bug.

POLÍTICAS DE PRIVACIDAD DE GOOGLE

DATOS RECOGIDOS POR GOOGLE

Para determinar información básica, como el idioma que hablas, hasta datos más complejos, como los anuncios que te resultarán más útiles o las personas que más te interesan online.

La recogida de datos se lleva a cabo de dos formas:

- **Información que proporcionas a Google.** Al registrarte en Google accedes a dar información relevante como: información personal (nombre, email, teléfono, tarjeta de crédito) .
- **Información que obtienen del uso que haces de sus servicios.** Cuando interactúas con un servicio de Google, este almacena la información que desea. Ejemplos: publicidad de google, navegador Chrome, etc. Cada vez que usas la tecnología de Google, la compañía americana almacenará todos los datos posibles, provenientes de:
    - **Información del dispositivo utilizado**
    - **Datos de registro**
    - **Datos sobre tu ubicación física**
    - **Números exclusivos de aplicación**
    - **Almacenamiento local (por ejemplo del navegador Chrome)**
    - **Cookies e identificadores anónimos**

UTILIZACIÓN DE LOS DATOS RECOGIDOS

Google utiliza la información recompilada del usuario para mejorar sus productos, para desarrollar otros nuevos y para proteger a Google y a sus usuarios. Además para dar una calidad acorde a lo que desea el usuario. El ejemplo serían las búsquedas personalizadas de Google y los anuncios que muestra en las diferentes páginas que utilizan sus servicios.

Un aspecto importante, es que la información obtenida se guarda en diferentes servidores que la compañía americana tiene por todo el planeta.

QUÉ DATOS PERSONALES COMPARTE POR GOOGLE

No comparten información personal con empresas, organizaciones ni particulares que no tengan relación con Google, a menos que se dé alguna de las siguientes circunstancias:

- **Consentimiento**
- **Administradores de dominio (si tu cuenta es gestionada)**

- **Tratamiento externo (empresas colaboradores con Google)**
- **Motivos legales**

CUÁNDO SE APLICA ESTA POLÍTICA DE PRIVACIDAD

La política de privacidad de Google se aplica a todos los servicios ofrecidos por Google Inc. y sus filiales, incluyendo los servicios ofrecidos en otros sitios web (como, por ejemplo, nuestros servicios publicitarios).

TIPOS DE COOKIES QUE UTILIZA GOOGLE

Utilizamos diferentes tipos de cookies para el funcionamiento de los productos relacionados con anuncios y de los sitios web de Google.

- Preferencias
- Seguridad
- Procesos
- Publicidad
- Estado de la sesión
- Google analytics

CÓMO UTILIZA GOOGLE LAS COOKIES

Google utiliza cookies con diversos fines, entre los que se incluyen recordar tus preferencias de SafeSearch, aumentar la relevancia de los anuncios que ves, contar el número de visitas que recibimos para acceder a una página, ayudarte a registrarte en sus servicios y proteger tus datos.

GUÍA PARA LA CONFIGURACIÓN ÓPTIMA DE UN ORDENADOR, DESDE EL PUNTO DE VISTA DE LA PRIVACIDAD:

EQUIPO EMPLEADO Y USUARIOS

EQUIPO EMPLEADO

El ordenador utilizado para esta práctica es un ordenador portátil en constante utilización. Tiene instalado los sitemas operativos Windows 7 Home Premium y una versión de linux, ubuntu. En esta actividad, nos centraremos en el análisis desde el sistema operativo Windows 7.

Utilización

El ordenador portátil se emplea con fines académicos, laborales y para entretenimiento personal. El equipo, se conecta a diferentes redes de acceso a internet. Como pueden ser la conexión de la universidad, sitios públicos y diferentes redes privadas.

USUARIOS

El equipo en cuestión es empleado por solo una persona con conocimientos informáticos elevados, técnico superior en desarrollo de aplicaciones informáticas y actualmente cursando ingeniería informática.

ANÁLISIS INICIAL

En un primer momento, vamos a hacer un pequeño resumen de la utilización y la configuración del ordenador.

El equipo tiene instaladas tanto para la versión Linux como Windows cuentas con password para el acceso al ordenador. Dichas contraseñas son bastante seguras, ya que son caracteres generados aleatoriamente, no tienen ninguna relación con el usuario del portatil.

Una vez arracamos la sesión en Windows, podemos comprobar un ordenador con varias aplicaciones, una de estas es el antivirus Avast! Pro Antivirus, en su última versión. Sirve de defensa y de analizador de archivos de dudosa procedencia. También protege contra el malware y spyware. Además el firewall de windows está totalmente activado.

A la hora de proceder a instalar aplicaciones no se piden ninguna credencial de acceso, es totalmente vulnerable a instalar cualquier programa, si ya estamos logueados en la cuenta de usuario. La razón de esto, es que el usuario del equipo tiene los permisos de administrador. Esto puede ser un problema si el usuario del equipo no está presente. Aún así, cada vez que se ausenta el usuario, bloquea la sesión.

Comprobando los diversos tipos de navegadores que tiene el equipo podemos ver que hay 3 instalados: Chrome versión 37, Firefox 30 e Internet Explorer 11. El único explorador actualizado en el equipo es el navegador Chrome, los otros tienen versiones antigüas. Verificando si todo está correcto, hemos encontrado que los navegadores no están protegidos contra las cookies. Esto es un problema que se puede solucionar navegando de forma segura o en el modo incógnito.

MODO INCÓGNITO

Si utilizamos el modo incógnito en google Chrome. No dejaremos ni rastro de lo que hemos visitado o descargado ni en el historial de exploración del navegador ni en el historial de descargas, pero si que quedarán guardados los archivos que hayamos descargado a nuestro equipo, algo lógico pero que no está de más recordarlo.

Tampoco se guardará ninguna *cookie* que se haya creado utilizando el modo incógnito, ya que si bien están disponibles durante la sesión de navegación en este modo, éstas se eliminan una vez cerradas todas las ventanas o pestañas del modo incógnito. Por el contrario, si hemos

realizado algún cambio en la configuración o en los marcadores de Google Chrome quedarán guardados, ya que esto no entra dentro de la navegación privada que ofrece el modo incógnito.

Por último, tened en cuenta que si iniciáis sesión con vuestra cuenta de Google –o algún otro servicio que registre vuestras visitas– dentro del modo incógnito, los sitios que visitéis quedarán reflejados en el historial web que almacena la cuenta Google en la nube. Así que si queréis tener una sesión de navegación completamente privada, más allá del dispositivo que estéis utilizando, y usar en ella vuestra cuenta Google, recordad borrar o deshabilitar el historial web que ésta guarda.

Para Firefox e Internet Explorer también existen modos parecidos.

- **Firefox:** Navegación privada
- **Explorer:** InPrivate

¿CÓMO SE ACCEDE AL MODO DE INCÓGNITO?

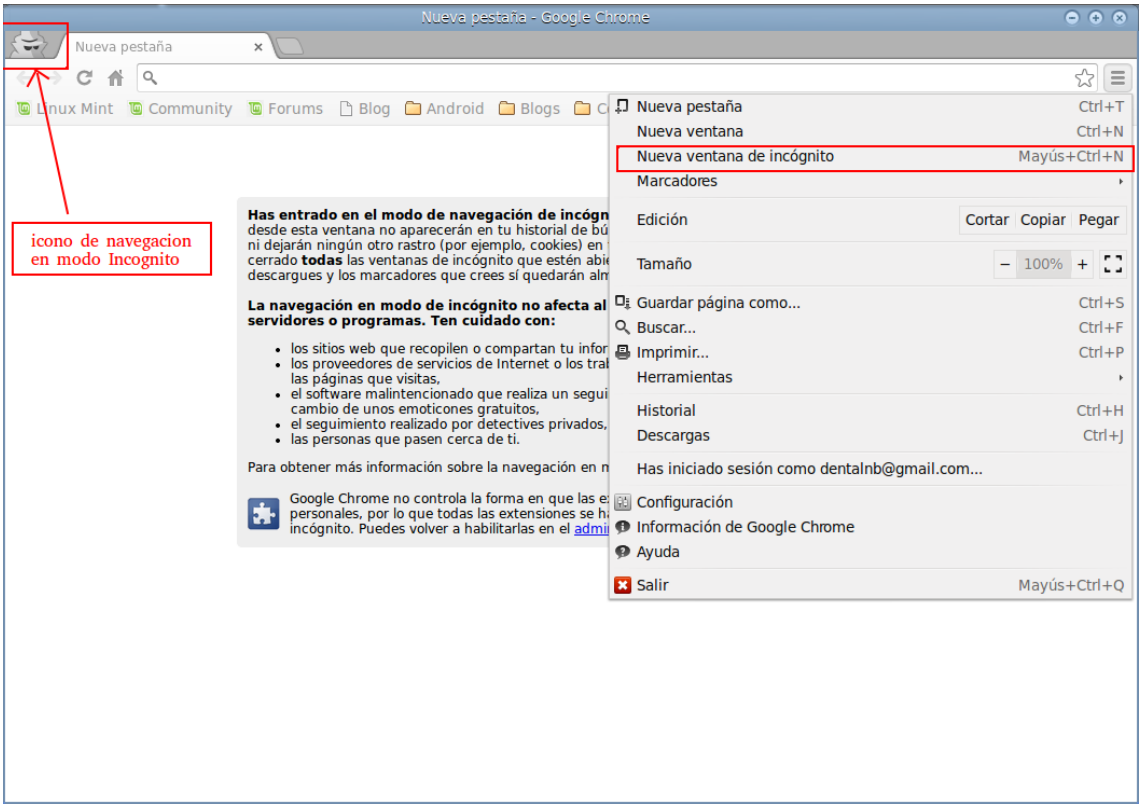


****Imagen de Google Chrome proveniente de Ubuntu (el que hizo la captura no se debió de dar cuenta de su email)*

MEJORAR LA PRIVACIDAD

El ordenador empleado está bastante bien equipado y protegido, es utilizado por una persona con conocimientos de lo que le puede pasar con sus datos si sus acciones no son las correctas.

Sin embargo, todo es mejorable. Aspectos a mejorar:

- **Privacidad en los navegadores**
- **Sesiones**

SESIONES

Un aspecto fundamental para el uso del equipo sería si está compartido o no. En este caso no estaba, aún así siempre se puede dejar a alguien por diversos motivos.

Si le dejas a alguien un equipo con una sola cuenta de usuario, no tienes otra opción que darle las credenciales y accederá a toda tu información almacenada en este. Tanto sean archivos, contraseñas almacenadas en el navegador, historial, etc.

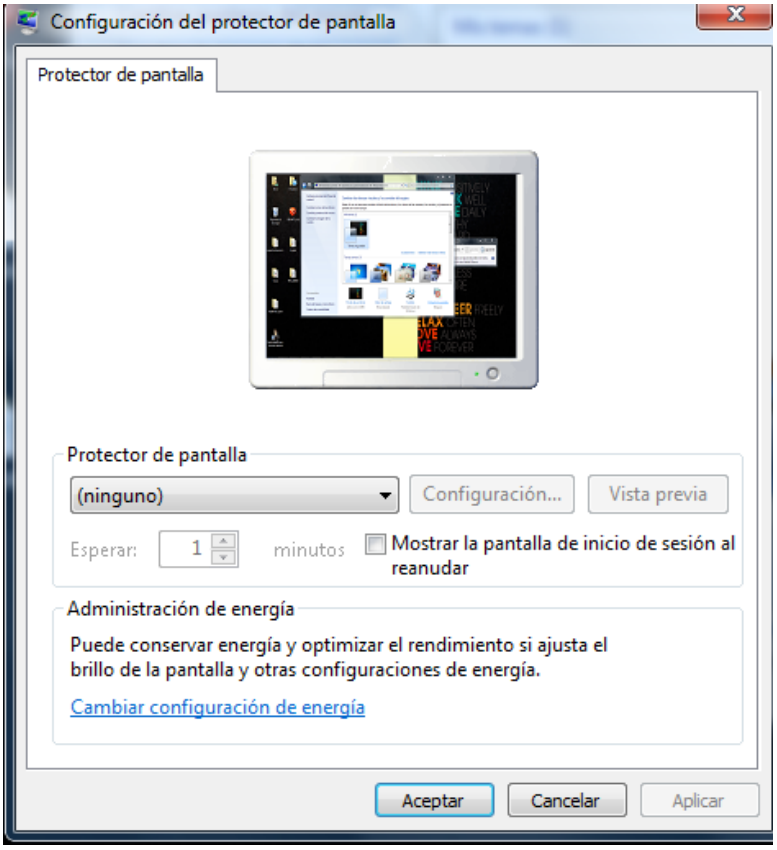
La solución para arreglar el problema si más de una persona trabaja en el equipo sería el uso de cuentas de usuario personalizadas

- Para el usuario que generalmente administra el equipo, una cuenta de administrador.
- Para un usuario espontáneo, se podría hacer una cuenta genérica con permisos limitados. Sólo lectura y ejecución.

Otra forma de riesgo para la privacidad del usuario sería una ausencia temporal dejando el ordenador con la sesión abierta. Para solventar esto configuramos el protector de pantalla:

Marcar:

- ✓ ***Mostrar la pantalla de inicio de sesión al reanudar.***



**Configuración del protector de pantalla*

PRIVACIDAD EN LOS NAVEGADORES

Como hemos explicado antes, no tendríamos que hacer ningún cambio en nuestro equipo para cubrirnos las espaldas en caso de navegar y acceder a sitios web que no queremos que nadie pueda registrar. Es fácil, usando el **modo incógnito** y **problema resuelto**.

De todas formas se puede hacer una configuración minuciosa de los navegadores, si se quiere absoluta privacidad (explicado para Google Chrome):

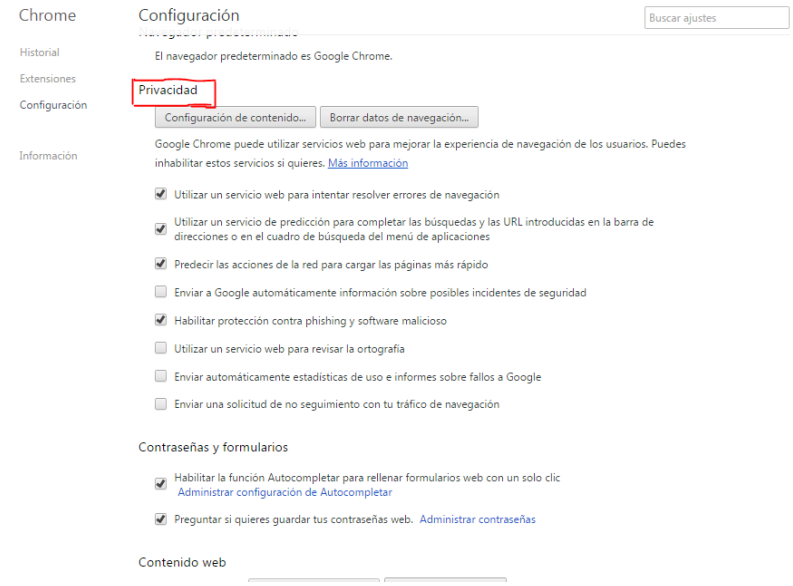
- Acceder al navegador---> configuración

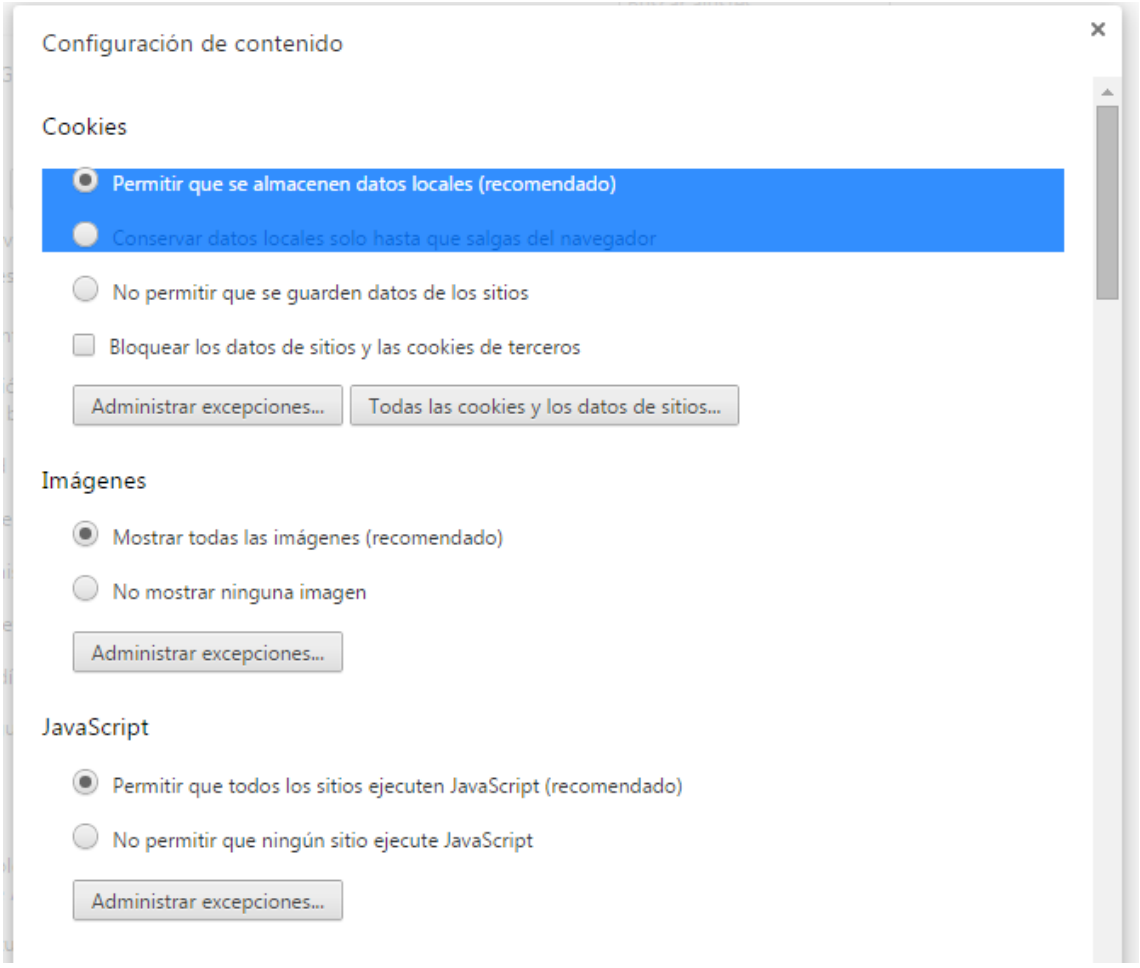
Ahí podemos acceder a:

- Nuestro historial para limpiar toda nuestra navegación y datos guardados.
- Configurar toda nuestra privacidad, permitir la inclusión de cookies, imágenes, Javascript.

Cambiando estas configuraciones podremos delimitar nuestra privacidad cuando naveguemos, y que sea más difícil de monitorizar nuestra actividad.

<u>Configuración de la privacidad:</u>





ELIMINAR O PROHIBIR LAS COOKIES EN LOS NAVEGADORES

La mayoría de navegadores actualmente permiten al usuario configurar si desean aceptar cookies y cuáles de ellas. Estos ajustes normalmente se encuentra en las 'opciones' o

'Preferencias' del menú de su navegador. Estas son las instrucciones para configurar las cookies en los principales navegadores:

- **Chrome**: Configuración -> Mostrar opciones avanzadas -> Privacidad -> Configuración de contenido. Para más información, puede consultar el soporte de Google o la Ayuda del navegador.
- **Firefox:** Herramientas -> Opciones -> Privacidad -> Historial -> Configuración Personalizada. Para más información, puede consultar el soporte de Mozilla o la Ayuda del navegador.
- **Internet Explorer:** Herramientas -> Opciones de Internet -> Privacidad -> Configuración. Para más información, puede consultar el soporte de Microsoft o la Ayuda del navegador.
- **Safari:** Preferencias -> Seguridad. Para más información, puede consultar el soporte de Apple o la Ayuda del navegador.

CONCLUSIÓN

El equipo evaluado cumple con los requisitos de seguridad con respecto a la privacidad. Aunque, con los consejos antes explicados se elevará el nivel de privacidad.

Sin embargo, aunque un ordenador esté muy bien protegido, si el usuario no es consciente de sus actos y de los peligros que entrañan unos malos hábitos (descargarse todo tipo de archivos e instalarlos, navegar por sitios web desconocidos y peligrosos, no cambiar las contraseñas, etc), dará igual que el ordenador esté totalmente equipado y protegido.

Por último, cabe mencionar que lo más importante siempre es el sentido común. ¿Darías tu datos personales a un completo desconocido en la calle? ¿Lo harías en internet?

FUENTES

Páginas webs consultadas e información obtenida de estas:

- https://developers.google.com/analytics/devguides/collection/analyticsjs/cookie-usage?hl=es
- http://www.google.es/intl/es/policies/privacy/
- https://www.google.com/intl/es_es/policies/technologies/cookies/
- http://es.wikipedia.org/wiki/Web_bug
- http://es.wikipedia.org/wiki/Cookie_(inform%C3%A1tica)
- http://bocabit.elcomercio.es/informatica/seguridad-informatica-las-cookies-maliciosas
- http://rootear.com/web/navega-sin-dejar-rastro-modo-incognito-google-chrome
- http://planetubuntu.es/post/navegacion-anonima
- http://mentalidadfitness.com/politicas-de-privacidad-y-cookies/