

# Diseño y Programación Web

Tema 5

**JavaScript (Cookies)**

Enrique Moguel  
[enrique@unex.es](mailto:enrique@unex.es)

# Índice

- **¿Qué es una Cookie?**
- **¿Para qué sirve?, ¿para qué se usa?**
- **Ideas equivocadas.**
- **Consultar las Cookies.**
- **Uso legal.**
- **Inconvenientes de las Cookies.**
- **Casos de uso.**
- **Crear, leer y eliminar una Cookie.**

# ¿Qué es una Cookie?

Una **cookie** (o **galleta informática**) es una pequeña información enviada por un sitio web y almacenada en el navegador del usuario, de manera que el sitio web puede consultar la actividad previa del usuario.

Sus principales funciones son:

- **Llevar el control de usuarios:** cuando un usuario introduce su nombre de usuario y contraseña, se almacena una cookie para que no tenga que estar introduciéndolas para cada página del servidor. Sin embargo, una cookie no identifica a una persona, sino a una combinación de computador-navegador-usuario.
- **Conseguir información sobre los hábitos de navegación del usuario,** e intentos de spyware (programas espía), por parte de agencias de publicidad y otros. Esto puede causar problemas de privacidad y es una de las razones por la que las cookies tienen sus detractores.

# ¿Para qué sirve?, ¿para qué se usa?

Las cookies son utilizadas habitualmente por los servidores de aplicaciones para **diferenciar usuarios** y para actuar de diferente forma dependiendo de éstos.

Inicialmente, las cookies se inventaron para ser utilizadas en una **cesta de la compra virtual**, que actúa como dispositivo virtual en el que el usuario va "colocando" los elementos que desea adquirir, de forma que los usuarios puedan navegar por el sitio donde se muestran los objetos a la venta y añadirlos y eliminarlos de la cesta de la compra en cualquier momento. Las cookies permiten que el contenido de la cesta de la compra dependa de las acciones del usuario.



# ¿Para qué sirve?, ¿para qué se usa?

Un uso de las cookies es identificarse en un sitio web. Los usuarios normalmente se identifican introduciendo sus credenciales en una página de validación; las cookies permiten al servidor saber que el usuario ya está validado, y por lo tanto se le puede permitir acceder a servicios o realizar operaciones que están restringidas a usuarios no identificados.

**Otros sitios web** utilizan las cookies para personalizar su aspecto según las preferencias del usuario. Por ejemplo, el motor de búsqueda de Google permite a los usuarios (incluso a los no registrados) decidir cuántos resultados de búsqueda quieren ver en cada página.

Las Cookies se utilizan también para realizar seguimientos de usuarios a lo largo de un sitio web. El seguimiento en un mismo sitio normalmente se hace con la intención de mantener **estadísticas de uso**, mientras que el seguimiento entre sitios normalmente se orienta a la **creación de perfiles de usuarios anónimos** por parte de las compañías de publicidad, que luego se usarán para orientar campañas publicitarias (decidir qué tipo de publicidad utilizar) basadas en perfiles de usuarios.

# Ideas equivocadas

Desde su introducción en Internet han circulado ideas equivocadas acerca de las cookies:

- Las cookies son similares a **gusanos** y **virus** en que pueden borrar datos 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 **solo se utilizan con fines publicitarios**.



# Ideas equivocadas

En realidad, las cookies son solo datos, no código, luego no pueden borrar ni leer información del ordenador de los usuarios. Sin embargo, las cookies permiten detectar las páginas visitadas por un usuario en un sitio determinado o conjunto de sitios. Esta información puede ser recopilada en un perfil de usuario. Estos perfiles son habitualmente anónimos, es decir, no contienen información personal del usuario (nombre, dirección, etc). De hecho, no pueden contenerla a menos que el propio usuario la haya comunicado a alguno de los sitios visitados. Pero aunque anónimos, estos perfiles han sido objeto de algunas preocupaciones relativas a la privacidad.

Según diferentes estudios, **un gran porcentaje de los usuarios de Internet no saben cómo borrar las cookies.**

# Consultar las Cookies

```
javascript:alert("Cookies: "+document.cookie)
```

Herramientas de desarrollador

Preferencias del navegador





# Uso legal

Las cookies tienen implicaciones importantes en la **privacidad** y el **anonimato** de los usuarios de la web. Aunque las cookies solo se envían al servidor que las definió o a otro en el mismo dominio, una página web puede contener imágenes y otros componentes almacenados en servidores de otros dominios.

Las compañías publicitarias utilizan **cookies de terceros** para realizar un seguimiento de los usuarios a través de múltiples sitios. En concreto, una compañía publicitaria puede seguir a un usuario a través de todas las páginas donde ha colocado imágenes publicitarias o web bugs. El conocimiento de las páginas visitadas por un usuario permite a estas compañías dirigir su publicidad según las supuestas preferencias del usuario.

La posibilidad de crear un perfil de los usuarios se ha considerado como una **potencial amenaza a la privacidad**, incluso cuando el seguimiento se limita a un solo dominio, pero especialmente cuando es a través de múltiples dominios mediante el uso de cookies de terceros. Por esa razón, algunos países tienen legislación sobre cookies (por ejemplo, **España**).

# Uso legal

La directiva de la **Unión Europea** de **2002** sobre privacidad en las telecomunicaciones contiene reglas sobre el uso de cookies. En concreto, en el artículo 5, párrafo 3 establece que el almacenamiento de datos (como cookies) en el ordenador de un usuario solo puede hacerse si:

1. el usuario recibe información sobre cómo se utilizan esos datos;
2. el usuario tiene la posibilidad de rechazar esa operación.

Cualquiera puede actualmente configurar su navegador para que se deshabiliten las cookies de terceros, pero lo que pide la directiva es que sea al contrario, y que el usuario que quiera aceptar este tipo de cookies tenga que realizar una acción consciente para su activación.

# Inconvenientes de las Cookies

Además de lo relativo a la privacidad que ya se ha mencionado, hay otras razones por las que el uso de cookies ha recibido cierta oposición:

1. **Identificación inexacta:** no siempre identifican correctamente a los usuarios, y se pueden utilizar para ataques de seguridad. Si se utiliza más de un navegador en un ordenador, cada uno tiene su propio almacenamiento de cookies. Por lo tanto, las cookies no identifican a una persona, sino a una combinación de cuenta de usuario, ordenador y navegador. De esta manera, cualquiera que utilice varias cuentas, varios ordenadores, o varios navegadores, tiene también múltiples conjuntos de cookies.

# Inconvenientes de las Cookies

- 2. Robo de cookies:** durante el funcionamiento normal, las cookies se envían en los dos sentidos entre el servidor (o grupo de servidores en el mismo dominio) y el ordenador del usuario que está navegando. Dado que las cookies pueden contener información sensible (nombre de usuario, un testigo utilizado como autenticación, etc.), sus valores no deberían ser accesibles desde otros ordenadores. Sin embargo, las cookies enviadas sobre sesiones HTTP normales son visibles a todos los usuarios que pueden escuchar en la red utilizando un *sniffer* de paquetes. Estas cookies no deben contener por lo tanto información sensible. **Este problema se puede solventar mediante el uso de https, que invoca seguridad de la capa de transporte para cifrar la conexión.**

# Inconvenientes de las Cookies

3. **Falsificación de cookies:** aunque las cookies deben ser almacenadas y enviadas de vuelta al servidor sin modificar, un atacante podría modificar el valor de las cookies antes de devolverlas. Si, por ejemplo, una cookie contiene el valor total de la compra de un usuario en un sitio web, cambiando ese valor el servidor podría permitir al atacante pagar menos de lo debido por su compra. El proceso de modificar el valor de las cookies se denomina falsificación de cookies y a menudo se realiza tras un robo de cookies para hacer un ataque persistente.
4. **Cookies entre sitios (cross-site cooking):** cada sitio debe tener sus propias cookies, de forma que un sitio *malo.net* no tenga posibilidad de modificar o definir cookies de otro sitio como *bueno.net*. Las vulnerabilidades de *cross-site cooking* (Cookies entre sitios) de los navegadores permiten a sitios maliciosos romper esta regla. Esto es similar a la falsificación de cookies, pero el atacante se aprovecha de usuarios no malintencionados con navegadores vulnerables, en vez de atacar el sitio web directamente. El objetivo de estos ataques puede ser realizar una fijación de sesión (robo de sesión en un sitio web).

# Casos de uso

- **Tiendas virtuales:**

Por ejemplo: <https://afiliados.amazon.es/>

- **Agencias de viajes:**

Por ejemplo: *eDreams*

- **Publicidad personalizada.**

- **Chollometro.**

- **Etc.**



Kindle, ahora  
con luz frontal...

EUR 89,99

Comprar ahora

[Enlace](#)

# Crear, leer y eliminar Cookies

// Crear Cookie:

```
document.cookie = cookie;
```

// Consultar Cookie:

```
keyValue = document.cookie.match("(^|;) ?" + key + "=[^;]*)(;|$)");
```

// Eliminar Cookie:

```
document.cookie = key + ';;expires=Thu, 01 Jan 1970 00:00:01 GMT;';
```