Álvaro Morón González

Tecnología AJAX

Viene de las siglas “Asynchronous JavaScript and XML” (JavaScript y XML asíncrono), es una tecnología diseñada para que las páginas web puedan actualizarse sin necesidad de que tengan que estar recargándose todo el rato, es decir, las solicitudes y las respuestas entre el navegador y el servidor ocurren en segundo plano. El navegador puede enviar una solicitud al servidor y mientras espera la respuesta puede ir realizando otras tareas sin detenerse. AJAX incluye Javascript para poder realizar las solicitudes y manipular el contenido en el navegador, el objeto XMLHttpRequest para comunicarse con el servidor, HTML y CSS para mostrar los datos y darles estilo y por último JSON para mostrar la información de un manera que sea fácil de entender.

El principal beneficio de AJAX es una experiencia de usuario mas agradable ya que se reduce el tiempo de carga.

AJAX se utiliza en muchos sitios web como redes sociales por ejemplo, para actualizar comentarios en tiempo real, y en correo electrónico, para comprobar si han llegado nuevos correos sin recargar la página.

Al utilizar AJAX, lo primero que se hace es enviar una solicitud a un servidor usando Javascript y el objeto XMLHttpRequest (que es el encargado de crear, enviar las solicitudes y manejar las respuestas), el servidor procesa los datos y los envía en formato JSON o XML(también puede ser CSV o texto plano), luego el navegador recibe la respuesta del servidor y Javascript muestra esos datos sin necesidad de recargar la página.

CORS

Significa “Cross-Origin Resource Sharing” (Intercambio de recursos de origen cruzado), y es un mecanismo que “decide” si permite o restringe las solicitudes entre sitios web para aumentar la seguridad de los usuarios y de los servidores.

Un servidor establece unas reglas mediante encabezados HTTP, que indican quien tiene acceso a los datos de ese servidor, luego los sitios web que desean obtener datos de ese servidor tienen que cumplir esas reglas, y después el navegador verifica que se están cumpliendo las reglas CORS para dejar que se obtengan los datos de ese servidor.

Esto es una medida de seguridad que se implementó en los navegadores, para permitir que unos sitios web puedan acceder a los recursos de otros pero de manera segura ya que antes de CORS, las restricciones de los navegadores como la política del “mismo origen”, impedía que los sitios web realizaran solicitudes a otros sitios web, esto prevenía ataque maliciosos, pero limitaba la funcionalidad de las aplicaciones web.

Algunos de los encabezados mas comunes son:

“Access-Control-Allow-Origin”, que especifica que dominios están autorizados a acceder a los recursos o “Access-Control-Allow-Methods”, que define que métodos como GET, POST, PUT etc, son permitidos en las solicitudes.