Introducción Plugin Handbook

<https://developer.wordpress.org/plugins/wordpress-org/detailed-plugin-guidelines/>

Las directrices detalladas para plugins en WordPress.org proporcionan reglas y recomendaciones para los desarrolladores que desean publicar sus plugins en el repositorio oficial de WordPress.

**Seguridad y Cumplimiento de Normas**:

* Los plugins deben cumplir con todas las leyes aplicables, incluidas las relacionadas con privacidad y derechos de autor.
* La seguridad es primordial. Los desarrolladores deben seguir las mejores prácticas para evitar vulnerabilidades.

**Contenido Aceptable**:

* No se permite contenido ilegal, ofensivo o dañino.
* Los plugins deben ser apropiados para una audiencia global, lo que incluye la prohibición de contenido que fomente el odio o la violencia.

**Uso de la API y Funcionalidad**:

* Los plugins deben usar las API de WordPress adecuadamente y no interferir con las funcionalidades centrales de WordPress o con otros plugins.
* Deben estar bien codificados y no incluir código innecesario o malicioso.

**Datos de Usuario y Privacidad**:

* Los plugins deben manejar los datos de los usuarios de manera responsable, cumpliendo con las leyes de protección de datos como el GDPR.
* La recopilación de datos debe estar claramente indicada y justificada, y se debe pedir consentimiento a los usuarios cuando sea necesario.

**Publicidad y Promoción**:

* No se permite publicidad o autopromoción agresiva dentro de los plugins.
* Los plugins gratuitos no deben incluir características bloqueadas por un muro de pago sin una versión completa y funcional disponible sin costo.

**Actualizaciones y Mantenimiento**:

* Los desarrolladores deben mantener sus plugins actualizados y ofrecer soporte a los usuarios.
* Es importante que los plugins sean compatibles con las versiones más recientes de WordPress.

**Comportamiento Profesional**:

* Se espera que los desarrolladores actúen de manera profesional y respetuosa dentro de la comunidad.
* Los conflictos y disputas deben manejarse con respeto y buscar resoluciones pacíficas.

Estas directrices están diseñadas para asegurar que los plugins en el repositorio de WordPress.org sean seguros, funcionales y respeten los derechos de los usuarios. Siguiendo estas reglas, los desarrolladores pueden contribuir positivamente al ecosistema de WordPress.

Contribuir Plugin Handbook

Cuando escribas o reescribas las secciones del Plugin Handbook, piensa en lo que te hubiera gustado saber cuando comenzaste a desarrollar plugins. Imagina que estás guiando a un desarrollador nuevo a través del proceso, ayudándote a evitar errores comunes y a adoptar las mejores prácticas desde el principio.

Aprovecha la oportunidad para llenar los vacíos de la documentación oficial con detalles que consideres valiosos, y hazlo en un lenguaje claro y directo. Tu contribución puede ayudar a que la comunidad de desarrolladores en español tenga acceso a recursos más completos y útiles.

### **Ejemplo: Seguridad de Plugin**

#### **Paso 1: Introducción del Tema**

* **Original en inglés:** "Plugin security is crucial to protect your site from vulnerabilities."
* **Reescritura en español:** "La seguridad de los plugins es un aspecto fundamental para proteger tu sitio web de vulnerabilidades que puedan ser explotadas por atacantes."

**Consejo:** Al comenzar, asegúrate de explicar claramente la importancia del tema que estás abordando. Usa un lenguaje accesible para que cualquier desarrollador, sin importar su nivel de experiencia, pueda comprender la relevancia del tema.

#### **Paso 2: Explicación de una Práctica Básica**

* **Original en inglés:** "Always sanitize user inputs using functions like sanitize\_text\_field()."
* **Reescritura en español:** "Siempre debes sanitizar las entradas de usuario utilizando funciones como sanitize\_text\_field() para prevenir la inyección de código malicioso."

**Consejo:** Describe las prácticas básicas que deberían seguirse, pero no te limites a la información existente. Añade contexto adicional o ejemplos que ayuden a los usuarios a entender mejor cómo implementar estas prácticas.

#### **Paso 3: Introducción de un Método Alternativo**

* **Original en inglés:** "Using wp\_nonce\_field() helps protect against CSRF attacks."
* **Reescritura en español:** "En la documentación oficial se sugiere el uso de wp\_nonce\_field() para proteger contra ataques CSRF, pero también puedes considerar el uso de check\_admin\_referer() en funciones específicas del área de administración para una capa de seguridad adicional."

**Consejo:** Aquí es donde puedes compartir tu experiencia personal. Si descubriste un método alternativo o complementario que no está bien documentado, explícalo con detalle. Describe por qué este método es útil, en qué situaciones debería aplicarse y cómo implementarlo paso a paso.

#### **Paso 4: Ejemplo Práctico**

* **Original en inglés:** "Example: sanitize\_text\_field($\_POST['your\_field']);."

**Reescritura en español:** "Ejemplo: Si estás recibiendo datos de un formulario, puedes sanitizarlos de la siguiente manera:  
  
  
$nombre\_usuario = sanitize\_text\_field($\_POST['nombre\_usuario']);

if (!check\_admin\_referer('guardar\_usuario\_nonce', '\_wpnonce')) {

wp\_die('No tienes permisos para realizar esta acción.');

}

* Este código no solo sanitiza la entrada, sino que también verifica un nonce de seguridad antes de procesar los datos, asegurando que solo usuarios autorizados puedan enviar el formulario."

**Consejo:** Proporciona ejemplos de código que demuestren claramente cómo implementar las prácticas que estás describiendo. Asegúrate de que el código esté bien comentado y sea fácil de seguir.

#### **Paso 5: Conclusión y Buenas Prácticas Adicionales**

* **Original en inglés:** "Make sure to always validate and sanitize inputs."
* **Reescritura en español:** "Recuerda siempre validar y sanitizar las entradas de usuario. Además, considera auditar regularmente tu código para identificar posibles vulnerabilidades y mantenerlo actualizado con las últimas recomendaciones de seguridad."

**Consejo:** Finaliza la sección ofreciendo consejos adicionales o recordatorios que puedan ayudar a los desarrolladores a mantener altos estándares de seguridad en sus plugins.