AMPLIACIÓN DEL EJERCICIO: FORMULARIO DE SUSCRIPCIÓN SEGURO Y ACCESIBLE

Vamos a añadir un **formulario de suscripción** a la página principal. Este formulario será **seguro, accesible, amigable**, y estará protegido contra amenazas comunes como XSS, inyección SQL y bots.

CARACTERÍSTICAS DEL FORMULARIO

1. **Accesibilidad**:
    - Uso de etiquetas <label> y atributos ARIA.
    - Uso correcto de atributos como required, aria-describedby, y mensajes claros de error.
2. **Seguridad**:
    - Validación en el cliente mediante atributos HTML (type, pattern, required) para prevenir datos incorrectos.
    - Protección en el servidor (sanitización y validación de datos) para evitar ataques XSS e inyecciones SQL.
3. **Protección contra Bots**:
    - Inclusión de un **campo honeypot** oculto.
    - Un **campo CAPTCHA simple** para validar que el usuario es humano.
4. **Amigable para el Usuario**:
    - Mensajes descriptivos y claros.
    - Flujo fácil y directo.

CÓDIGO HTML DEL FORMULARIO DE SUSCRIPCIÓN

FORMULARIO EN LA PÁGINA PRINCIPAL (INDEX.HTML)

Aquí agregamos el formulario dentro de una nueva sección al final del contenido principal.

```
<!DOCTYPE html>

<html lang="es">

<head>

  <meta charset="UTF-8">

  <meta name="viewport" content="width=device-width, initial-scale=1.0">

  <title>Pink Floyd: Una Leyenda del Rock</title>

</head>
```

```
<body>
  <!-- Header -->
  <header id="header">
    <h1>Pink Floyd: Una Leyenda del Rock</h1>
    <nav>
      <ul>
        <li><a href="index.html">Inicio</a></li>
        <li><a href="historia.html">Historia</a></li>
        <li><a href="albumes.html">Álbumes</a></li>
        <li><a href="integrantes.html">Integrantes</a></li>
      </ul>
    </nav>
  </header>

  <!-- Main Content -->
  <main>
    <section>
      <h2>Bienvenidos</h2>
      <p>Bienvenidos a la página dedicada a Pink Floyd, una de las bandas más influyentes de todos los tiempos.</p>
    </section>

    <!-- Formulario de Suscripción -->
    <section>
      <h2>Suscríbete a nuestras Noticias</h2>
      <form action="procesar_suscripcion.php" method="POST" aria-labelledby="suscripcion-title">
        <!-- Campo visible -->
        <div>
          <label for="email">Correo Electrónico:</label>
          <input type="email" id="email" name="email" placeholder="ejemplo@correo.com" required
              aria-describedby="email-info">
          <small id="email-info">Por favor, ingresa un correo electrónico válido.</small>
        </div>
```

```
            <!-- Campo CAPTCHA Simple -->
            <div>
              <label for="captcha">¿Cuánto es 2 + 3?</label>
              <input type="text" id="captcha" name="captcha" pattern="5" required
                  aria-describedby="captcha-info">
              <small id="captcha-info">Esta pregunta nos ayuda a confirmar que no eres un robot.</small>
            </div>

            <!-- Honeypot: Campo oculto para bots -->
            <div style="display: none;">
              <label for="extra">Si eres humano, deja este campo vacío:</label>
              <input type="text" id="extra" name="extra">
            </div>

            <!-- Botón de envío -->
            <div>
              <button type="submit">Suscribirse</button>
            </div>
          </form>
        </section>
    </main>

    <!-- Footer -->
    <footer>
      <p>&copy; 2024 Pink Floyd Fan Page</p>
    </footer>
</body>
</html>
```

EXPLICACIÓN DEL CÓDIGO

1. **Estructura Semántica**:
    - El formulario está contenido dentro de un <section> con un título <h2>.

2. **Campos del Formulario**:
    - **Correo Electrónico**:
        - Usa type="email" para validar correos.
        - Atributo required asegura que el campo no esté vacío.
    - **CAPTCHA Simple**:
        - Pregunta matemática (2 + 3) con un pattern para validar la respuesta correcta en el lado del cliente.
    - **Campo Honeypot (Protección contra bots)**:
        - Campo oculto visible solo para bots. Si se completa, se invalida el formulario.
3. **Accesibilidad**:
    - Uso de aria-describedby para asociar mensajes informativos a los campos.
    - Etiquetas <label> conectadas con for aseguran que los campos sean accesibles.
4. **Seguridad**:
    - La validación en el cliente previene errores básicos.
    - El servidor (archivo procesar_suscripcion.php) deberá validar y sanitizar los datos antes de procesarlos.

VALIDACIÓN EN EL SERVIDOR (EJEMPLO PHP)

A continuación, una implementación básica para el archivo procesar_suscripcion.php. Este código protege contra XSS y bots.

```
<?php
if ($_SERVER["REQUEST_METHOD"] === "POST") {
  // Validar Honeypot
  if (!empty($_POST['extra'])) {
    die("Error: Se detectó actividad no autorizada.");
  }

  // Captura y sanitización de datos
  $email = filter_input(INPUT_POST, 'email', FILTER_SANITIZE_EMAIL);
  $captcha = filter_input(INPUT_POST, 'captcha', FILTER_SANITIZE_NUMBER_INT);

  // Validación de los datos
  if (!filter_var($email, FILTER_VALIDATE_EMAIL)) {
    die("Error: El correo electrónico no es válido.");
```

```
    }

    if ($captcha != 5) {
        die("Error: La respuesta al CAPTCHA es incorrecta.");
    }

    // TODO: Aquí se guardaría el correo en la base de datos de manera segura.

    echo "¡Gracias por suscribirte! Pronto recibirás nuestras noticias.";
} else {
    die("Acceso no permitido.");
}
?>
```

RESUMEN DE SEGURIDAD

1. **Protección contra XSS**: Se sanitizan las entradas del usuario utilizando filter_input() y FILTER_SANITIZE_*.
2. **Protección contra Bots**:
    - Campo honeypot oculto (extra).
    - CAPTCHA simple.
3. **Validación estricta**:
    - Verificación del correo electrónico.
    - Validación del CAPTCHA.

RESULTADO FINAL

PÁGINA PRINCIPAL (INDEX.HTML):

- Contiene un formulario amigable y accesible.
- Los campos aseguran una experiencia óptima para usuarios y protegen contra bots y amenazas comunes.

SERVIDOR (PROCESAR_SUSCRIPCION.PHP):

- Verifica y sanitiza las entradas.
- Proporciona protección contra ataques como XSS y spam.