SENA	Servicio Nacional de Aprendizaje - SENA Regional Risaralda **INSTRUMENTO DE EVALUACIÓN**	Formato no controlado Página 1 de 7

INFORMACIÓN GENERAL
FECHA DE APLICACIÓN: 26/Abril/2025
PROGRAMA DE FORMACIÓN: Tgo. Análisis y Desarrollo de Software
FICHA: 2692988 TGO ADSO
CENTRO: Diseño e Innovación Tecnológica Industrial
COMPETENCIA: 1. Desarrollar la solución de software de acuerdo con el diseño y metodologías de desarrollo 2. Implementar la solución de software de acuerdo con los requisitos de operación y modelos de referencia
RESULTADO DE APRENDIZAJE: **1 - RAE 04:** Codificar el software de acuerdo con el diseño establecido. **1 - RAE 05:** Realizar pruebas al software para verificar su funcionalidad. **2 – RAE 01:** Planear actividades de implantación del software de acuerdo con las condiciones del sistema. **2 – RAE 02:** Desplegar el software de acuerdo con la arquitectura y las políticas establecidas. **2 – RAE 03:** Documentar el proceso de implantación de software siguiendo estándares de calidad. **2 – RAE 04:** Implantar el software de acuerdo con los niveles de servicio establecidos con el cliente.
TIPO DE EVIDENCIA: Producto
EVIDENCIA: Diseño y Desarrollo de Blog de Información Deportiva
NOMBRE DEL APRENDICES: BRAHIAN CARDONA PIEDRAHITA
NOMBRE DE LOS INSTRUCTORES: • Jhoan Sebastián Duque Vera • Yuly Paulin Saenz Agudelo • Jhon Faber Cortes Osorio • Oscar Garcia Soto → Coordinador Académico

Ítem	*VARIABLES / INDICADORES*	*CUMPLE*	
		SI	*NO*
Funcionalidad del Sistema (50%)			
1	Permite ingreso y cierre de sesión para cada tipo de usuario (admin, creator, user)	X	
2	Funciona la gestión de usuarios (crear/modificar/eliminar) por el admin	X	
3	Funciona la gestión de publicaciones (crear/editar/eliminar) por el creador de contenido		X
4	El usuario puede visualizar, buscar, comentar y compartir publicaciones	X	
5	Funciona la categorización de publicaciones por temas	X	
6	Comentarios pueden ser aprobados/eliminados por el admin	X	
7	Sistema cierra sesión por inactividad de 10 minutos		X
8	Blog es responsivo (móvil y escritorio)	X	
9	Mensajes informativos tras acciones (crear publicación, error de login, etc.)	X	
10	Validación de formularios y consistencia visual	X	
11	Modelo de base de datos normalizado (sin redundancia)		X
12	Relaciones entre tablas coherentes con requerimientos		X
Documentación (30%)			
13	Código fuente correctamente estructurado y comentado		X
14	Manual de usuario incluido y comprensible	X	
15	Manual técnico detallado (arquitectura, tecnologías, estructura)	X	
16	Manual de instalación (paso a paso para montar el sistema)	X	

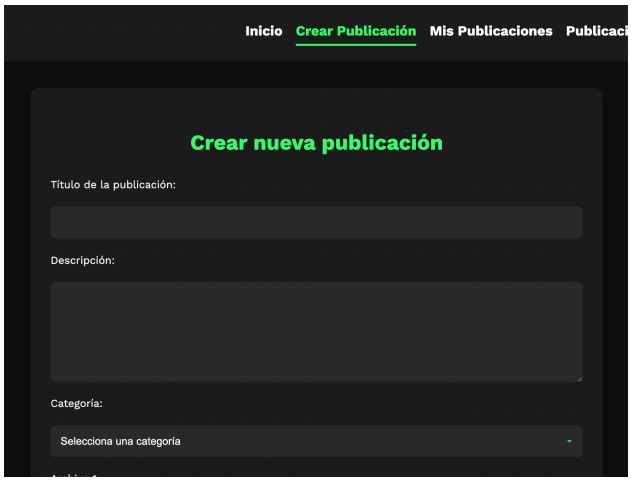
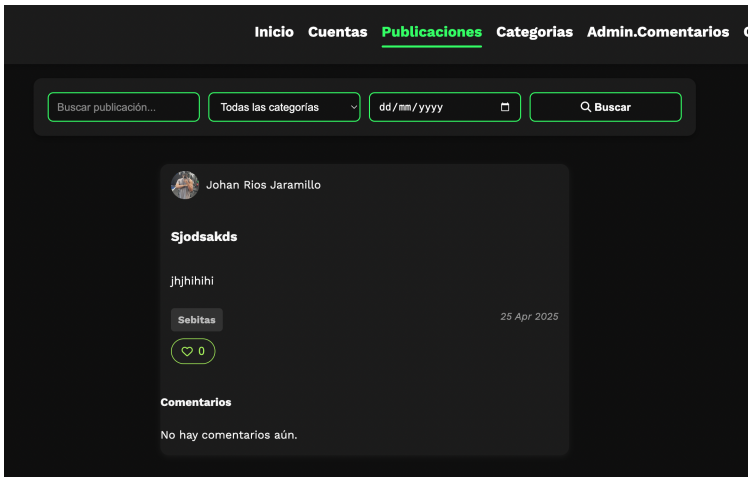
17	Informe de pruebas (funcionalidades y resultados esperados)	X	
Despliegue en la Nube (20%)			
18	Sistema desplegado correctamente en el hosting cPanel	X	
19	HTTPS implementado correctamente	X	
20	Datos de usuarios encriptados en base de datos	X	
21	Proyecto alojado en repositorio Git (con README)	X	
22	Archivo README claro y completo (instalación, uso, descripción)	X	
ACTITUDES Y VALORES			
23	Porta los elementos institucionales (uniforme, carné) de manera correcta, de acuerdo a lo establecido en el reglamento del aprendiz.	X	
24	Desarrolla las actividades propuestas de forma disciplinada	X	
25	Presenta trabajos con honestidad	X	

OBSERVACIONES

Funcionalidad del Sistema (50%)

Punto 3. Funciona la gestión de publicaciones (crear/editar/eliminar) por el admin.

Revisando el admin no tiene la función de *crear/modificar/eliminar* publicaciones, recuerde que el usuario administrador siempre lleva todos los permisos debido a que es el rol más importante dentro del aplicativo.

Usuario - Creador de Contenido	Usuario – Admin
	

Punto 7. Sistema cierra sesión por inactividad de 10 minutos

Esta a 5 minutos.

```
52  function resetInactivityTimer() {
53      clearTimeout(timeout);
54      timeout = setTimeout(() => {
55          window.location.href = 'logout.php';
56      }, 5 * 60 * 1000);
57  }
58
59  document.addEventListener('mousemove', resetInactivityTimer);
60  document.addEventListener('keydown', resetInactivityTimer);
61  document.addEventListener('scroll', resetInactivityTimer);
62  document.addEventListener('click', resetInactivityTimer);
```

Adicionalmente no tiene una función global para controlar la inactividad es decir que tiene que ir página por página cambiando esta función. Esto es una muy mala práctica de programación

Punto 11. Modelo de base de datos normalizado (sin redundancia)

Duplicación de categoría: además de la tabla categorias, publicaciones tiene la columna categoria (varchar) que repite ese dato. Debería referenciar id_categoria como FK.

Tablas de estado inconsistentes: existen estado, estado_publicacion, estado_categorias, estado_comentarios... y la columna publicaciones.estado no referencia ninguna de ellas.

Punto 12. Relaciones entre tablas coherentes con requerimientos

Faltan claves primarias: Ninguna tabla define explícitamente PRIMARY KEY, Relaciones con FK para comentarios→publicaciones, comentarios→cuentas, compartidos→publicaciones, compartidos→cuentas, likes→publicaciones, likes→cuentas, cuentas→roles, categorías→estado_categorias, comentarios→estado_comentarios.

Faltan:

FK de publicaciones.categoria hacia categorias.id_categoria.

FK de publicaciones.estado hacia estado_publicacion.id_estado (o estado.id_estado).

Uso de la tabla estado genérica no conectado a ninguna tabla.

Documentación (30%)

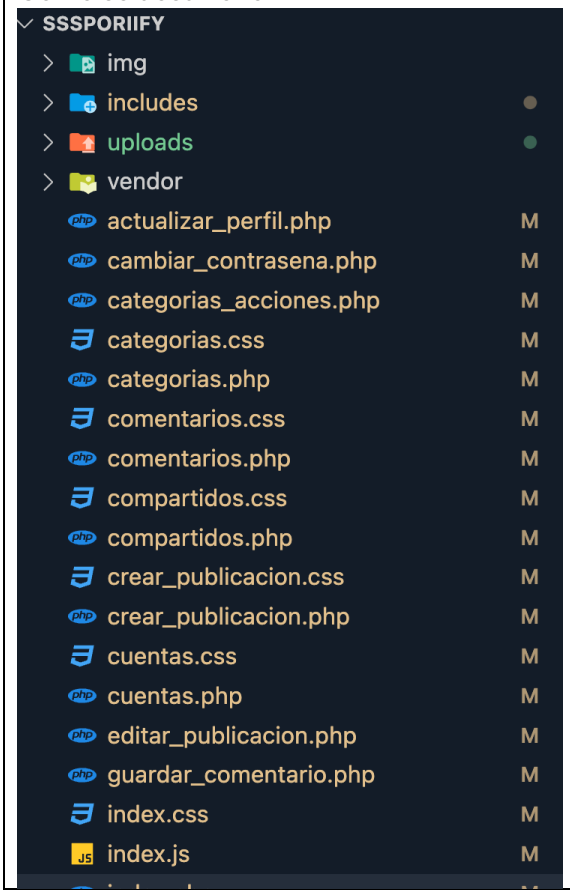
Punto 13. Código fuente correctamente estructurado y comentado

El código no tiene ningún patron de diseño de software, Todo esta desorganizado y no hay un buen control de los archivos, porque se evidencia que hay funciones en cada uno de los archivos que deberían ser globales.

Un ejemplo muy marcado es de la expiración de la sesión

```
52  function resetInactivityTimer() {
53      clearTimeout(timeout);
54      timeout = setTimeout(() => {
55          window.location.href = 'logout.php';
56      }, 5 * 60 * 1000);
57  }
58
59  document.addEventListener('mousemove', resetInactivityTimer);
60  document.addEventListener('keydown', resetInactivityTimer);
61  document.addEventListener('scroll', resetInactivityTimer);
62  document.addEventListener('click', resetInactivityTimer);
```

Como se desarrollo



Como debería estar



Tampoco esta comentado

```php
<?php
session_start();
require_once "includes/db_conection.php";

if (!isset($_SESSION['id_cuenta'])) {
    http_response_code(401);
    echo "No autorizado";
    exit();
}

$id_usuario = $_SESSION['id_cuenta'];
$id_publicacion = $_POST['id_publicacion'] ?? null;

if (!$id_publicacion) {
    echo "Falta ID de publicación";
    exit();
}

$sql = "SELECT * FROM likes WHERE id_usuario = $id_usuario AND id_publicacion = $id_publicacion";
$res = mysqli_query($conn, $sql);

if (mysqli_num_rows($res) > 0) {
    mysqli_query($conn, "DELETE FROM likes WHERE id_usuario = $id_usuario AND id_publicacion = $id_publicacion");
} else {
    mysqli_query($conn, "INSERT INTO likes (id_usuario, id_publicacion) VALUES ($id_usuario, $id_publicacion)");
}

$count_res = mysqli_query($conn, "SELECT COUNT(*) as total FROM likes WHERE id_publicacion = $id_publicacion");
$count = mysqli_fetch_assoc($count_res)['total'];

$names_res = mysqli_query($conn, "
    SELECT c.user_name
```

```php
<?php
session_start();
require_once "includes/db_conection.php";

if (isset($_SESSION['id_cuenta'])) {
    $id_cuenta = mysqli_real_escape_string($conn, $_SESSION['id_cuenta']);

    $query = "SELECT nombres, apellidos, correo, user_name, rol, foto_perfil FROM cuentas WHERE id_cuenta =
    $id_cuenta";
    $stmt = mysqli_query($conn, $query);

    if ($stmt && mysqli_num_rows($stmt) > 0) {
        $resultado = mysqli_fetch_assoc($stmt);
        $nombres = $resultado['nombres'];
        $apellidos = $resultado['apellidos'];
        $correo = $resultado['correo'];
        $user_name = $resultado['user_name'];
        $rol_usuario = $resultado['rol'];
        $foto_perfil = $resultado['foto_perfil'] ?? 'img/avatar.jpg';
    } else {
        die("Error: No se encontraron datos para el usuario. " . mysqli_error($conn));
    }
} else {
    header("Location: login.php");
    exit();
}

$popup_message = "";
$popup_type = "";
```

Observaciones Finales

- El proyecto está organizado como un conjunto de scripts PHP independientes (uno por acción/página), mezclando lógica de negocio, acceso a datos y presentación en un mismo archivo.
- No sigue ningún patrón de diseño (MVC, Capas, PSR-4), lo que dificulta la escalabilidad, el mantenimiento y la colaboración en equipo.
- La carpeta vendor indica uso de Composer (PHPMailer), pero el resto del código es completamente procedural y no aprovecha autoloaders ni namespaces.
- Las credenciales de MySQL están “hardcodeadas” en includes/db_conection.php en lugar de utilizar variables de entorno o un archivo de configuración protegido.
- Se emplea la extensión mysqli en modo mixto: unas pocas consultas usan prepared statements (mysqli_prepare / bind_param), pero muchas otras construyen cadenas SQL interpolando variables escapadas con mysqli_real_escape_string(), lo que deja puntos de posible inyección si algún caso escapa de esa sanitización.
- Aunque el registro y el cambio de contraseña utilizan password_hash(), la validación de inputs (longitudes, formatos, contenido malicioso) es dispersa y no centralizada.
- No hay protección contra CSRF (no se usan tokens en formularios), ni salida HTML escapada para prevenir XSS.
- Falta manejo de permisos a nivel de rol en muchas rutas: por ejemplo, varios scripts asumen que la sesión está iniciada, pero no validan rol/estado de usuario antes de ejecutar acciones.

- Cada sección tiene su propio CSS, sin un framework o sistema de plantillas comunes. Esto provoca inconsistencias en estilo y aumenta el esfuerzo de mantenimiento.
- No hay un sistema de “layout” ni parcialización de cabeceras/píes de página: un cambio global en la UI requiere editar múltiples archivos.
- No existen librerías internas o funciones reutilizables para operaciones comunes (por ejemplo, gestión de mensajes de usuario, redirecciones, validación).
- Se repiten fragmentos de código en distintos controladores, lo que incrementa la probabilidad de errores y desincronización de lógica.
- No hay scripts de migración o seeders para la base de datos: la importación es manual.

_____ _____

Firma de Instructor Firma del Aprendiz