INSTITUTO TÉCNICO RICALDONE
ESPECIALIDAD DESARROLLO DE SOFTWARE
TERCER AÑO DE BACHILLERATO
BTVDS 3.8: PROYECTO INNOVADOR DE DESARROLLO DE SOFTWARE
FASE DE EJECUCIÓN: FUNDAMENTOS DE SEGURIDAD WEB
DOCENTE: DANIEL CARRANZA
daniel_carranza@ricaldone.edu.sv

INSTRUMENTO DE HETEROEVALUACIÓN

(ESCALA ESTIMATIVA**)**

OBJETIVO:
Valorar las medidas de seguridad implementadas para la aplicación web de la TIENDA EN LÍNEA de acuerdo con los riesgos más comunes según OWASP Top 10 – 2017 y tomando en cuenta los criterios establecidos.

CONSIDERACIONES:

- La tarea ha sido asignada en la semana del 30 de agosto al 03 de septiembre y será revisada del 13 al 17 de septiembre según el horario proporcionado.
- La actividad vale 40% de la fase del módulo y se calificará siempre y cuando el proyecto se encuentre unificado y funcionando de forma local, de lo contrario la nota será 1.0
- La tarea debe ser desarrollada bajo la misma lógica de programación del proyecto (arquitectura de software multicapa mediante PHP y JavaScript, sin frameworks), de lo contrario la nota será 1.0
- Durante la calificación se tomará en cuenta el dominio en los criterios que se estimen convenientes y no está permitido realizar correcciones mientras se desarrolla la evaluación.
- Considerar la experiencia de usuario en los criterios que tienen que ver con la interacción y aplicar las buenas prácticas de desarrollo que fueron compartidas en la fase de preparación del módulo 1.
- Para realizar la calificación se asigna el puntaje correspondiente a cada criterio de acuerdo con la siguiente escala de valoración: **1 = Deficiente, 2 = Regular, 3 = Bueno, 4 = Muy bueno** y **5 = Excelente**
- La SUMATORIA se calcula sumando los puntajes obtenidos en cada criterio. La NOTA se obtiene mediante el siguiente procedimiento: **SUMATORIA / 30**

#	CRITERIOS	PUNTAJE
	DESARROLLO	
1	**Ocultar contraseña.** Todos los campos de los formularios designados para contraseñas no muestran textualmente el valor mientras se digita y no se visualiza a nivel de la vista.	
2	**Cifrar contraseña.** Se ha utilizado un algoritmo criptográfico tipo hash fuerte de sentido único para convertir la contraseña de los usuarios que es guardada en la base de datos.	
3	**Cambiar contraseña.** Los usuarios pueden actualizar la contraseña en cualquier momento después de iniciar sesión y se comprueba que su nuevo valor sea diferente al actual.	
4	**Restaurar contraseña.** Se ofrece a los usuarios un mecanismo confiable para restablecer o cambiar la contraseña si ha sido olvidada cuando se quiere iniciar sesión.	
5	**Validar contraseña.** Se comprueba que la contraseña contenga como mínimo ocho caracteres entre alfanuméricos y especiales (al menos uno de cada uno) y que sea diferente al nombre de usuario.	
6	**Confirmar contraseña.** Al momento de ingresar una nueva contraseña, se solicita al usuario corroborar este dato para evitar el ingreso de un valor erróneo.	
7	**Obligar cambio de contraseña.** Se pide a los usuarios cambiar la contraseña cada 90 días después de registrar, actualizar o restaurar; de lo contrario no se permite iniciar sesión.	
8	**Desactivar autocompletado.** En los formularios se evita el almacenamiento en cache de datos sensibles ingresados por los usuarios como alias, correo, DUI, teléfono, etc.	
9	**Bloquear vista de directorios (error 403).** No se permite a los usuarios ver el contenido de las carpetas, mostrando a cambio una página web de error personalizada.	

10	**Bloquear direcciones erróneas (error 404).** Se muestra a los usuarios una página web de error personalizada al acceder a una URL inexistente dentro del dominio.	
11	**Prevenir Cross Site Scripting (XSS).** Se validan todos los datos de entrada para evitar que los usuarios ingresen cadenas de texto maliciosas como código JavaScript o HTML.	
12	**Preparar sentencias.** Se utilizan consultas parametrizadas al realizar cualquier operación en la base de datos para evitar inyecciones SQL.	
13	**Comprobar humano.** El sitio público cuenta con reCAPTCHA o algún mecanismo similar para validar que el usuario sea una persona al momento de registrarse.	
14	**Registrar primer usuario.** El sitio privado permite crear una cuenta de usuario inicial si y solo si, no existe una al momento de ingresar al dashboard por primera vez.	
15	**Manejar excepciones de la base de datos.** Al existir un problema en la base de datos se muestra un mensaje de error personalizado para evitar dar información del servidor.	
16	**Controlar intentos fallidos de autenticación.** Se bloquea la cuenta del usuario durante 24 horas o de forma indefinida al ingresar como máximo tres veces una contraseña errónea.	
17	**Incluir segundo factor de autenticación.** Se valida el acceso mediante una doble comprobación de usuario después de ingresar alias y contraseña, ya sea de forma opcional u obligatoria.	
18	**Registrar historial de sesiones.** Se registran las diferentes autenticaciones que han realizado los usuarios, mostrando diversos datos de referencia como fecha/hora, sistema operativo, etc.	
19	**Validar autenticación de usuarios.** Se verifica que los usuarios hayan iniciado sesión al acceder a las diferentes partes que lo ameritan, permitiendo cerrarla en cualquier momento.	
20	**Permitir sesiones diferentes.** Es posible iniciar sesión en el sitio público y en el sitio privado de forma simultánea e independiente en una misma ventana del navegador.	
21	**Cerrar sesión por inactividad.** Se cierra la sesión del usuario después de 5 minutos sin realizar alguna acción, para evitar que otros usuarios utilicen o usurpen la cuenta.	
22	**Implementar seguridad extra.** Se ha propuesto una medida de seguridad web adicional y significativa en base al documento de OWASP proporcionado.	
GENERALIDADES		
23	**Documentación.** Se han utilizado comentarios detallados para describir las diferentes secciones del código, con el objetivo de facilitar su comprensión.	
24	**Estándares de programación.** Se ha empleado un estilo de código predefinido para la escritura de la programación con PHP (API, modelos y reportes) y JavaScript (controladores).	
25	**Experiencia de usuario.** Las vistas cuentan con un diseño atractivo, responsivo y uniforme; siendo fácil de comprender, navegar y utilizar.	
26	**Ortografía y redacción.** El contenido estático de las vistas cumple con las reglas de escritura del idioma español y posee coherencia textual.	
27	**Control del proyecto.** Se ha utilizado un sistema de control de versiones para gestionar el proyecto y todos los integrantes del equipo han realizado aportaciones significativas (commits).	
CONDUCTA		
28	**Asistencia a clases.** Los integrantes del equipo participan en todas las jornadas sincrónicas en Microsoft Teams correspondientes a la tarea y acatan la normativa institucional de conducta.	
29	**Puntualidad y exposición.** Los miembros del proyecto se presentan a la hora y fecha solicitada según el horario de evaluación y cumplen con las reglas proporcionadas.	
30	**Consultas.** Los integrantes del equipo respetan el horario proporcionado para solventar dudas, esto es por medio de Microsoft Teams de lunes a viernes entre 07:00 y 16:00	
	SUMATORIA	
	NOTA	