INSTRUMENTO DE EVALUACIÓN DE SISTEMAS TRAYECTO III

TITULO:						
AUTORES:						
CATEGORÍA: Requerimiento de validación		P	Si	Med	No	Observaciones
1	Los requerimientos han sido recolectados, analizados e implementados correctamente.	1				
2	El diseño del sistema debe ser sencillo, básico y robusto.	1				
CATEGORÍA: UI		P	Si	Med	No	Observaciones
3	El estilo visual de la web es homogéneo.	1				
4	El performance de la web es óptimo. Maniente un performance report de Lighthouse mayor a 90 y el tiempo de carga del LCP no mayor a 7 segundos.	1				
5	La web es adaptable a los diferentes dispositivos que la utilizan sin afectar la legibilidad, navegación ni interacción del contenido.	2				
6	La web cumple con los estándares de la W3C.	1				
7	El sistema proporciona mensajes de ayuda al usuario.	2				
CATEGORÍA: Eficiencia y funcionalidad		P	Si	Med	No	Observaciones
8	El tiempo de respuesta del servidor es óptimo.	2				
9	La configuración del hardware es adecuada para soportar las cargas de trabajo del sistema.	1				
10	La aplicación es mantenible, escalable, observable y testeable.	2				
CATEGORÍA: Usabilidad		P	Si	Med	No	Observaciones
11	La interfaz web permite una fácil comprensión de sus funciones al usuario.	1				
12	El sistema facilita las operaciones, tomando en cuenta las capacidades y limitaciones motoras, cognitivas y perceptuales del usuario.	1				
13	Se han implementado mecanismos de validación para proteger los datos y prevenir errores de entrada.	2				
14	Mantiene el flujo de navegación a través de la aplicación.	1				
CATEGORÍA: Seguridad		P	Si	Med	No	Observaciones
15	La autenticación se realiza a través de varias capas de seguridad, lo que dificulta significativamente el acceso no autorizado a las cuentas.	1				
16	El sistema ayuda a proteger y resguardar la integridad de los datos.	2				
17	Bloquear al usuario a los tres (3) intentos de ingreso de forma errónea.	2				

18	El bloqueo y desbloqueo de usuarios puede ser accionado únicamente por un operador con el privilegio necesario.	1				
19	El operador (administrador) con el privilegio necesario debe ingresar un método de autenticación para accionar la eliminación de un usuario.	2				
20	La autorización de acceso a funcionalidades están determinadas por RBAC, ReBAC, ABAC, MAC, o algún método de asignación de privilegios, roles, relaciones o reglas de acceso.	2				
21	Deniega los accesos a funcionalidades no autorizadas.	1				
22	Las contraseñas están hasheadas, mediante un algoritmo SHA-256, SHA-3 o de aún mayor complejidad mientras sea de una sola vía.	2				
23	La contraseña debe tener como mínimo 16 caracteres, sin máximo de almacenamiento.	2				
24	El sistema cuenta con un mecanismo de recuperación de contraseña.	1				
25	La información confidencial no se almacena en lugares accesibles para terceros.	2				
26	El sistema tiene una bitácora de acciones o transacciones realizadas por un usuario.	2				
27	El servidor está protegido contra ataques no accionados por sus usuarios usando CSRF tokens, CORS, TLS, httponly Cookies, Secure Cookies, etc.	1				
	Total	40				

Arcaya, Argüello, Pachano y Ramones (2024) PSI-2024

LEYENDA: P: Ponderación Si: Cumple con el ítem planteado, por lo tanto, tiene la máxima ponderación. Med: Cumple medianamente con el ítem planteado, por lo tanto, tiene la mitad de la ponderación. No: No cumple con el ítem planteado, por lo tanto, no tiene la ponderación correspondiente.

VALORACIÓN PARA SU IMPLEMENTACIÓN:

Categoría	Escala	Observaciones
Aprobado	35 – 40	
Con correcciones	29 – 34	
Reprobado	0 – 28	

DATOS DEL VALIDADOR			
NOMBRE Y APELLIDO		**CEDULA**	
FIRMA		**FECHA**	

Nota La aplicación de este instrumento solo será posible si:

1.- Se evidencia los requerimientos para el diseño del mismo avalados por la comunidad atendida.

2.- Se entrega dos ejemplares del instrumento al validador.

3.- Los sistemas deberán ser evaluados por tres profesionales en la área de desarrollo de software y la revisión establece si el producto es óptimo para la comunidad

LEYENDA DEL INSTRUMENTO DE EVALUACIÓN DE SISTEMAS TRAYECTO III

CATEGORÍA: Requerimiento de validación		***Leyenda***
1	Los requerimientos han sido recolectados, analizados e implementados correctamente.	Los requisitos del sistema han sido obtenidos, analizados e implementados siguiendo una metodología rigurosa de ingeniería de software, garantizando la calidad y trazabilidad del producto final.
2	El diseño del sistema debe ser sencillo, básico y robusto	El sistema presenta una arquitectura sencilla y bien estructurada, lo que facilita su comprensión, mantenimiento y escalabilidad.
CATEGORÍA: UI		***Leyenda***
3	El estilo visual de la web es homogéneo.	La identidad visual de la web se expresa de manera coherente a través de todos los elementos gráficos, tipográficos y cromáticos, reforzando la marca
4	El performance de la web es óptimo. Maniente un performance report de Lighthouse mayor a 90 y el tiempo de carga del LCP no mayor a 7 segundos	La web ofrece una experiencia de usuario excepcional gracias a su alto rendimiento, garantizando una carga rápida de los contenidos y una interacción fluida.
5	La web es adaptable a los diferentes dispositivos que la utilizan sin afectar la legibilidad, navegación ni interacción del contenido.	La web ofrece una experiencia de usuario óptima en todos los dispositivos, adaptándose de manera fluida a diferentes tamaños de pantalla y resoluciones, sin comprometer la legibilidad ni la funcionalidad.
6	La web cumple con los estándares de la W3C.	El código de la web ha sido validado siguiendo las pautas de la World Wide Web Consortium (https://www.w3.org/), lo que asegura la calidad y accesibilidad del contenido.
7	El sistema proporciona mensajes de ayuda al usuario.	El sistema proporciona mensajes de ayuda a través de Tooltip, Tutorial, mensaje de error, Dialog, Modal, Toast u otro elemento. Los mensajes son claros, concisos y contextualizados, mejorando la usabilidad y reduciendo la curva de aprendizaje, lo que se traduce en una experiencia de usuario más satisfactoria.
CATEGORÍA: Eficiencia y funcionalidad		***Leyenda***
8	El tiempo de respuesta del servidor es óptimo.	El sistema ha sido configurado para minimizar la latencia del servidor, como el uso de caché HTTP, réplicas de lectura, memcache y otros; asegurando una entrega rápida de los datos.
9	La configuración del hardware es adecuada para soportar las cargas de trabajo del sistema.	El hardware actual soporta los requerimientos del sistema, evitando cuellos de botella y asegurando una experiencia de usuario fluida.
10	La aplicación es mantenible,	La aplicación utiliza patrones de diseño que promueven la reutilización de código y la

	escalable, observable y testeable.	extensibilidad. Sigue lo principios de testeabilidad, lo que facilita la detección y corrección de errores. La aplicación cuenta con mecanismos de monitoreo y logging que permiten identificar y resolver problemas de manera eficiente. El código de la aplicación es limpio, bien estructurado y documentado, facilitando su mantenimiento y permitiendo futuras expansiones.
CATEGORÍA: Usabilidad		***Leyenda***
11	La interfaz web permite una fácil comprensión de sus funciones al usuario.	La interfaz web presenta un diseño claro, intuitivo y coherente, lo que permite a los usuarios comprender rápidamente sus funcionalidades y realizar sus tareas de manera eficiente, sin necesidad de una capacitación especializada.
12	El sistema facilita las operaciones, tomando en cuenta las capacidades y limitaciones motoras, cognitivas y perceptuales del usuario.	La web ha sido diseñada siguiendo las Web Content Accessibility Guidelines (https://www.w3.org/WAI/standards-guidelines/wcag/), garantizando una experiencia inclusiva para todos los usuarios.
13	Se han implementado mecanismos de validación para proteger los datos y prevenir errores de entrada.	La aplicación valida los datos de los formularios tanto en el lado del cliente (JavaScript) como en el lado del servidor (API), utilizando expresiones regulares, validaciones de tipo y longitud, y sanitización de entrada que proporciona una experiencia de usuario fluida y protege la aplicación de ataques maliciosos.
14	Mantiene el flujo de navegación a través de la aplicación.	Se ha implementado una jerarquía de información clara y consistente para facilitar la orientación del usuario.
CATEGORÍA: Seguridad		***Leyenda***
15	La autenticación se realiza a través de varias capas de seguridad, lo que dificulta significativamente el acceso no autorizado a las cuentas.	El inicio de sesión requiere del uso de otro elemento que valide la autenticidad del usuario. Ejemplo: 2FA, OAuth 2.0, paswordless, OTP, llave RSA, llave ECDSA, llave GPG, etc.
16	El sistema ayuda a proteger y resguardar la integridad de los datos.	El sistema garantiza la confidencialidad, integridad y disponibilidad de los datos, protegiéndolos de accesos no autorizados, alteraciones y pérdidas, como el uso de réplicas o copias de seguridad.
17	Bloquear al usuario a los tres (3) intentos de ingreso de forma errónea.	Se ha implementado un mecanismo de bloqueo de cuenta para prevenir ataques de fuerza bruta y proteger la seguridad de las cuentas de usuario. El usuario bloqueado no puede leer ninguna información ni accionar ninguna operación.
18	El bloqueo y desbloqueo de usuarios puede ser accionado	Para garantizar la seguridad de los datos, el bloqueo y desbloqueo de usuarios está restringido a personal

	únicamente por un operador con el privilegio necesario.	autorizado con los permisos necesarios, como administrador de sistema, gerente, supervisor, técnico de soporte, u otro mientras esté dentro de los actores del sistema.
19	El operador (administrador) con el privilegio necesario debe ingresar un método de autenticación para accionar la eliminación de un usuario.	Aun siendo un operador autorizado, administrador de sistema, soporte técnico… Se requiere de autenticación adicional para eliminar cuentas de usuario, bien sea contraseña, 2FA, código enviado al correo, OTP, llave RSA, llave ECDSA, llave GPG, entre otros.
20	La autorización de acceso a funcionalidades están determinadas por RBAC, ReBAC, ABAC, MAC, o algún método de asignación de privilegios, roles, relaciones o reglas de acceso.	Los permisos de acceso se gestionan de forma granular, asegurando que cada usuario solo tenga acceso a la información y funciones necesarias para realizar su trabajo.
21	Deniega los accesos a funcionalidades no autorizadas.	Proporciona una respuesta clara y concisa al usuario cuando intenta realizar una acción no autorizada, como devolver un error 403 (Prohibido) para solicitudes no autorizadas.
22	Las contraseñas están hasheadas, mediante un algoritmo SHA-256, SHA-3 o de aún mayor complejidad mientras sea de una sola vía.	Utiliza algoritmos de hash de una sola vía para almacenar las contraseñas de los usuarios, garantizando la confidencialidad de sus datos. La contraseña no puede desencriptarse.
23	La contraseña debe tener como mínimo 16 caracteres, sin máximo de almacenamiento.	Las recomendaciones de la Agencia de Ciberseguridad de la Unión Europea (ENISA) describen las contraseñas de hasta 9 caracteres como “hackeables” utilizando herramientas de dominio público. Se recomienda el uso de contraseñas mayores a 14 caracteres. Ver https://www.enisa.europa.eu/topics/incident-response/glossary/authentication-methods
24	El sistema cuenta con un mecanismo de recuperación de contraseña.	En caso de olvidar su contraseña, la aplicación envía un enlace mediante correo electrónico, ruta que permite al usuario establecer su nueva contraseña, que incluye un token o código de un solo uso que lo autorice para restablecer su contraseña de forma autónoma.
25	La información confidencial no se almacena en lugares accesibles para terceros.	La información sensible (tokens, url de bases de datos, API tokens, secrets) no está almacenada en lugares vulnerables: localStorage, sessions, o el código fuente.
26	El sistema tiene una bitácora de acciones o transacciones realizadas por un usuario.	Se registra un historial inmutable de todas las acciones realizadas por los usuarios en el sistema, que incluyen fecha y hora.
27	El servidor está protegido	El servidor utiliza mecanismos para prevenir ataques

	contra ataques no accionados por sus usuarios usando CSRF tokens, CORS, TLS, httponly Cookies, Secure Cookies, etc.	y minimizar los riesgos de seguridad, siguiendo las recomendaciones de la Fundación OWASP.

Arcaya, Argüello, Pachano y Ramones (2024) PSI-2024

Los sistemas deberán ser evaluados por tres profesionales en la materia de desarrollo de software y la validación certifica si aprobó, con correcciones o reprobado.