Implementación de políticas de seguridad para el fortalecimiento del módulo de acceso a la plataforma de evaluación de proyectos integradores (SEPI)

Implementation of security policies to strengthen the access module to the integration project evaluation platform (SEPI)

Gustavo Adolfo Zúñiga Bechara[1]
David Alberto García Arango[2]
Frey de Jesús Castro Ramírez[3]

DOI: https://doi.org/10.26495/icti.v9i2.2275

RESUMEN

El presente artículo tiene como finalidad determinar una política de seguridad para el fortalecimiento del módulo login de la plataforma Sistema de Evaluación de Proyectos Integradores (SEPI), el cual está basado en implementar seguridad informática en el sistema de información para la evaluación de los proyectos correspondientes a la Facultad de Ingeniería de Sistemas e Ingeniería Industrial dentro de la Corporación Universitaria Americana (CUA). El SEPI se desarrolló en su totalidad y fue implementado en la universidad, no obstante, se plantea como etapa posterior el mejoramiento de la seguridad para evitar ataques en el login de los usuarios, ya que, si no están protegidos los campos de usuario, fácilmente alguien puede manipular esa información. Así esta información que es de carácter reservado se encuentre expuesta a casos de suplantación, accesos no autorizados, entre otros. El desarrollo del trabajo se inspira en los modelos de ingeniería y prototipos de diseño basados en prácticas institucionalizadas en la industria del software para el desarrollo de sistema de software las cuales implica fase de Análisis, Diseño, Desarrollo, Pruebas o Verificación e Implementación o Entrega.

PALABRAS CLAVE: seguridad informática, ataques cibernéticos, sistemas informáticos, políticas de seguridad, datos personales.

[1] *Corporación Universitaria Americana, Medellín, Colombia, zunigagustavo3174@coruniamericana.edu.co*
[2] *Corporación Universitaria Americana, Medellín, Colombia, dagarcia@coruniamericana.edu.co*
[3] *Corporación Universitaria Americana, Medellín, Colombia, fcastro@coruniamericana.edu.co*

ABSTRACT

The purpose of this article is to determine a security policy to strengthen the login module of the Integrator Project Evaluation System (SEPI) platform, which is based on implementing computer security in the information system for the evaluation of the corresponding projects. to the Faculty of Systems Engineering and Industrial Engineering within the American University Corporation (CUA). The SEPI was developed in its entirety and was implemented in the university, however, the improvement of security is proposed as a later stage to avoid attacks on the login of users, since, if the user fields are not protected, it is easily someone can manipulate that information. Thus, this information, which is of a reserved nature, is exposed to cases of impersonation, unauthorized access, among others. The development of the work is inspired by engineering models and design prototypes based on institutionalized practices in the software industry for the development of software systems which involve the Analysis, Design, Development, Testing or Verification and Implementation or Delivery phase.

KEYWORDS: computer security, cyber attacks, computer systems, security policies, personal data.

1. INTRODUCCIÓN

La seguridad informática en el uso de plataforma digitales en las instituciones de educación superior en Colombia es un tema central para las dependencias encargadas de administrar los sistemas de información de los usuarios, donde se cuentan con datos personales de gran valía, creándose una responsabilidad incluso legal para las universidades en su proceso de modernización, donde hoy en día se demanda el uso de las tecnologías de la información y la comunicación TIC, para mantener una interacción en tiempo real con la comunidad académica y sociedad en general. De esta manera, la Corporación Universitaria Americana en su rol misional tiene como finalidad garantizar el cuidado de la información personal de todos los estudiantes matriculados e interesados que hayan diligenciado algún formulario en la plataforma institucional de la universidad en aras de reflejar confianza, seguridad y transparencia en el desarrollo de los diferentes procesos administrativos, todo ello teniendo en cuenta que existen riesgos de dichos datos personales propiciados por ataques cibernéticos con la finalidad de afectar al estudiantado. Es por ello que surgió la necesidad de implementar seguridad en la plataforma de proyectos integradores debido a la vulnerabilidad de ataques informáticos, lleva a buscar una solución que permita proteger los datos de los estudiantes, ya que cuenta con poca seguridad de información reservada, como la contraseña, datos que no deben ser expuestos a ataques informáticos, ya que cualquier persona con conocimiento puede extraer informaciones. De modo que se plantean políticas de seguridad para proteger y aumentar los datos de los estudiantes y profesores.

De acuerdo con lo anterior, el Sistema de Evaluación de Proyectos Integradores (SEPI), data del año 2014, desarrollado para la facultad de ingeniería de la Corporación Universitaria Americana para los programas de Ingeniería de Sistemas e Ingeniería Industrial, la cual se entiende como una estrategia para realizar seguimiento al aprendizaje basado en proyectos en el que se evidencie el mejoramiento de las habilidades de los estudiantes y el aporte científico que generan sus iniciativas de investigación a la comunidad académica, todo ello como mecanismo para el fortalecimiento institucional con la finalidad de justificar la acreditación de alta calidad otorgada por el Ministerio de Educación Nacional (Ortiz & Garcia, 2021).

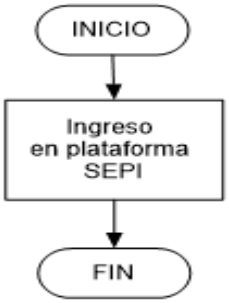
Vale decir que de acuerdo con estas iniciativas generadas en años anteriores se contribuyó como se manifestó anteriormente a la Acreditación de alta calidad al programa de ingeniería de sistemas de la Corporación Universitaria Americana mediante Resolución No. 023023 del 30 de noviembre de 2021,

ya que, se pudo demostrar la participación de (26) proyectos de extensión a través de prácticas estudiantiles, pasantías, procesos de investigación y proyectos de emprendimiento, así como la creación de (2) grupos de investigación ante Miniciencias clasificados en categoría A1 y A, respectivamente. Es de anotar que la implementación del SEPI, permitió el direccionamiento estratégico de las investigaciones y el fortalecimiento académico en los estudiantes del programa que de manera autocompositiva pueden desarrollar proyectos de gran aporte a la comunidad estudiantil. Sin embargo, cabe mencionar que en la plataforma SEPI, en el módulo del Login se evidenció una debilidad de seguridad informática que facilita el riesgo de ataques informáticos con la intención de obtener bases de datos de los estudiantes que hayan interactuado en la misma. Posiblemente hay muchos aspectos adicionales que analizar en cuanto a seguridad, pero de acuerdo con la complejidad y la importancia de iniciar asegurar los datos, se planteó como posibles soluciones para mejorar el SEPI un modelo de seguridad informática. De esta manera se precisa que este trabajo tiene como finalidad implementar un modelo de seguridad informática en el sistema de información para la evaluación de los proyectos integradores correspondientes a la facultad de ingeniería de sistemas e Ingeniería industrial de la Corporación Universitaria Americana (CUA) que permita fortalecer el módulo login en la plataforma.

2. MATERIALES Y MÉTODOS

Luego de reconocer las vulnerabilidades de la plataforma SEPI y haber definido los elementos teóricos descritos, los procedimientos con los cuales se llevan a cabo las fases de un proyecto de software que son análisis, diseño, desarrollo, pruebas o verificación e Implementación o Entrega (Drake, 2008). La Plataforma de Proyectos Integradores por ser una aplicación web que permite ofrecer soluciones a estudiantes y profesores actualmente se representa cada procedimiento mediante un diagrama de flujo, que esquematiza las tareas del usuario y la máquina de una manera sencilla, así.

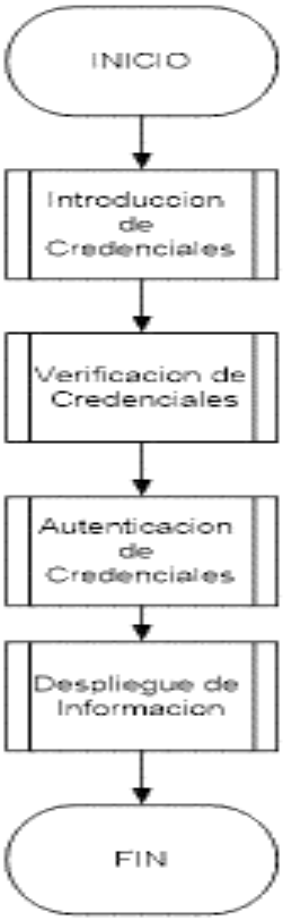
Figura 2. SEQ Figura * ARABIC 2- Modeneral del Proceso - plataforma



Fuente: Elaboración propia

La figura 2, representa un proceso cualquiera donde hay un inicio (primer óvalo, sistema bloque funcional), fin (segundo óvalo) el inicio es simplemente un punto el programa, dice toda la información está lista para comenzar, el inicio no contiene información dentro de sí. El sistema contiene otros bloques conectados de forma lógica, realiza operaciones lógicas como “and, or”, sentencias condicionales bicondicionales o anidadas. El fin indica la terminación de todas las tareas independientemente de los flujos dentro del sistema.

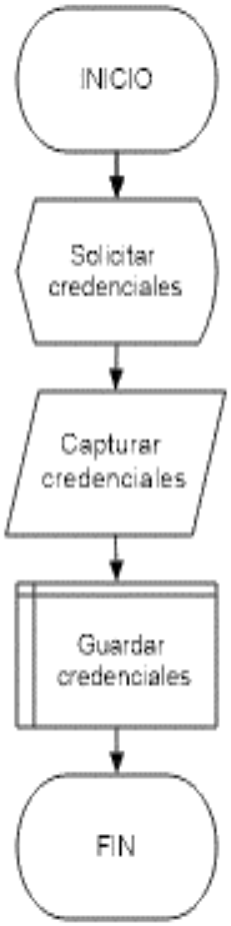
Figura 3. Subproceso Proyecto SEPI



Fuente: elaboración propia

En la Figura 3, se evidencian cuatro subprocesos, configurados en series. Estos se realizan por el usuario y la máquina, es decir el usuario es el actor quien lee y escribe digitando cada carácter y la máquina registra estos caracteres. En este subproceso la máquina compara los caracteres escritos por el usuario con el set de caracteres almacenados en su memoria. En la autenticación de credenciales la máquina envía información a otra máquina para que compare cadena de caracteres. El despliegue de información entrega información en forma de matrices, impresa en pantalla.

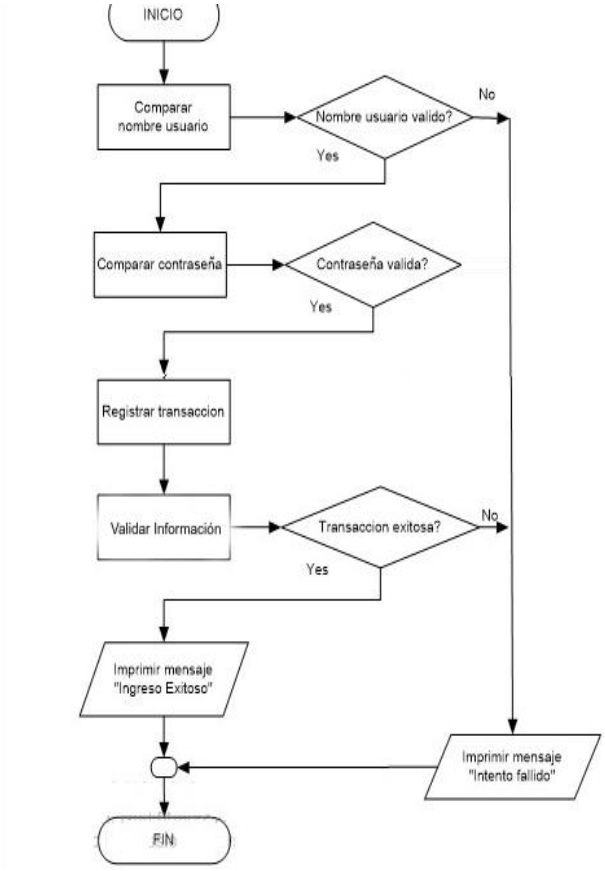
Figura 4. Procedimiento Introducción de Credenciales



Fuente: elaboración propia

Este subproceso tiene tres bloques que se resumen en solicitar, capturar y almacenar. Aquí se intercambian tareas entre el usuario y la máquina, el usuario ordena a la máquina a través de comandos y la máquina solicita información al usuario. Como muestran las figuras 5 y 6.

Figura 5. SEQ Figura * ARABIC 5 - Interacción Usuario y Sistema SEPI



Este subproceso tiene como tarea comparar si los datos ingresados en la caja de texto usuario y contraseña coinciden con datos almacenados en la base de datos, si los caracteres ingresados no son válidos el sistema imprime un mensaje indicando "intento fallido", si los datos ingresados son válidos en los campos usuario y contraseña la transacción es exitosa e imprime un mensaje de ingreso exitoso.

Figura 6. Autenticación de credenciales

Fuente: elaboración propia

El subproceso Autenticación de Credenciales tiene esencialmente tres (3) tareas. La tarea "Buscar DDBB" consiste en consultas de información general acerca del usuario (ejemplo, nombre de usuario - username -, computador - host -, localización); la tarea "Solicitar Código Nuevo" consiste en un requerimiento (petición), dirigido hacia el servidor; la tarea "Guardar Código Nuevo" consiste en el almacenamiento de caracteres en memoria, ya sean discos locales, remotos, internos, externos, entre otros.

Figura 7. Despliegue de la información

Fuente: elaboración propia

Aquí se tienen dos (2) tareas básicas, la tarea "mostrar ventanas" consiste en la impresión de marcos (frames) que contienen formatos, menús, botones, y demás; la tarea "mostrar información de usuario" consiste en la impresión de datos, textos, figuras, y otros. Una vez la plataforma complete estos bloques de sistema habrá seguridad en la información.

Con esta información procedimental se establece que la plataforma SEPI, de propiedad de la Corporación Universitaria Americana (CUA), al momento de su puesta en marcha refleja una debilidad de seguridad informática establecida por falta de credenciales, desde esta perspectiva esta investigación demanda un estudio descriptivo y exploratorio que permita dar respuesta a las necesidades de la plataforma a partir de la aplicación de políticas de seguridad que a continuación se presentarán.

3. RESULTADOS

En este apartado se presentarán los resultados obtenidos a partir de los aspectos metodológicos y procedimentales establecidos, los cuales constarán de la descripción conceptual y técnica de los objetivos específicos expresados en la parte inicial de esta investigación.

Descripción del Problema de Seguridad de la Plataforma SEPI

De acuerdo con lo evidenciado en la plataforma "Sistema de Evaluación de Proyectos Integradores" (SEPI), de propiedad de la Corporación Universitaria Americana (CUA), se ha estimado que en el login de la misma no cuenta con credenciales de autenticación que permita respaldar la identificación de los usuarios, implicando que cualquier persona que acceda a los datos personales de estudiantes matriculados puedan sacar provecho de información valiosa de estos.

En este sentido se puede visualizar que al ingresar a la página principal de esta plataforma se solicita una credencial (usuario), la cual se puede construir con letras y números y por otro lado una contraseña que no exige caracteres especiales y se crea a partir de (6) caracteres de la preferencia del titular de la cuenta. Pero antes, se debe crear una cuenta de usuario, la cual corresponde a llenar un formulario con

datos personales, como celular, correo electrónico, nombres, apellidos, programa académico, nivel, entre otros.

Una vez surtida estas diligencias, el sistema brinda la activación de la cuenta sin que se allegue un correo electrónico o un mensaje de texto con código de autenticación que permita corroborar el dominio de la información por parte del estudiante y no de un tercero que conoce dicha información personal.

Atributos de Seguridad a Nivel de Cliente

En los lenguajes de programación existen atributos de los cuales se usaron para proteger el módulo de ataques ya que permiten implementar seguridad del lado de cliente y servidor

Atributo Required: Asegura que los campos o cajas de texto no estén vacíos a la hora de enviar datos y obligando a los usuarios que completen los campos. (Ver Tabla 1)

Tabla 1. Atributo Required

Atributo Required
Required placeholder="Usuario Admin"onkeyup="form1.field2. value=home. usr.value"/> </td>

Fuente: Elaboración Propia

Atributo Pattern: Atributo que nos permite decirle a nuestro input que caracteres o tipos de datos debe aceptar y tiene una compatibilidad con un sinnúmero de aplicaciones y navegadores web" (Barrena, 2015). De acuerdo con la información de la figura *8* , se muestra la verificación de los navegadores compatibles, donde cada color representa el grado de compatibilidad viendo así el color verde como el color que aprueba su usabilidad total y el color rojo incompatibilidad, lo que puede indicar que el atributo es compatible con más del 90% de los navegadores en la actualidad, las cifras que se muestran a continuación detallan las versiones del navegador mencionado, solo muestra el navegador opera mini en color rojo que no es compatible (ver Tabla 2)

Tabla 2. Atributo Pattern

Atributo Pattern
<td>‹input type="text"name="usr" class="CajasTxt" pattern="[A-Za-20-9_-1{10}"

Fuente: Elaboración Propia

Funciones de Seguridad a Nivel de Servidor

Se optó por una solución con funciones dentro del lenguaje de programación que satisface los requisitos de la seguridad que se requerían, así hacer que las consultas fueran mucho más seguras para cumplir el objetivo, se elige la función Real Scape String que escapa caracteres especiales en una cadena para su uso en una sentencia SQL.

Así que, para comprobar el funcionamiento de esta función, se desactivaron los atributos que protegen el módulo a nivel de usuario y se comprueba insertando código SQL, como se observa en la Figura 8.

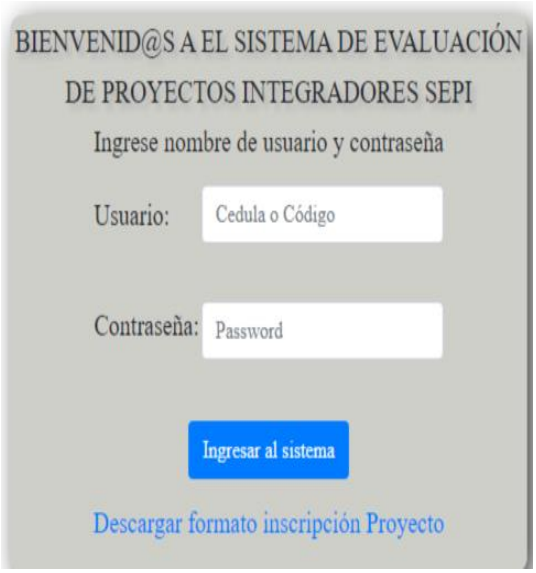
Figura 8. Insertando código SQL a nivel de servidor

Fuente: elaboración propia

Una vez implementados los códigos Required y Oat para evitar ataques de inyección SQL y cifrar la base de datos evitando ataques de inyección SQL, se considera realizar ataques, así de esta manera comprobar la eficacia de la plataforma.

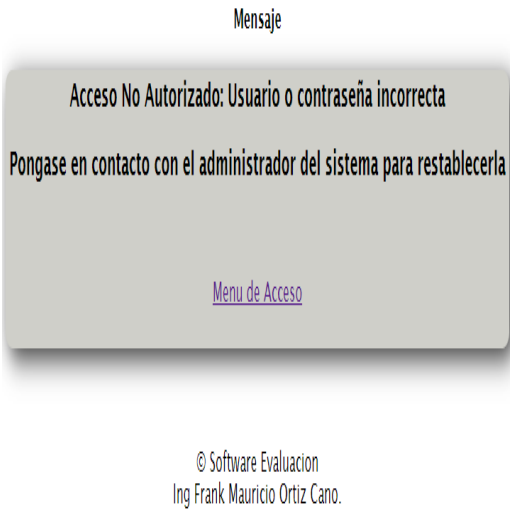
Primero se inicia simulando un servidor a nivel local y poder hacer pruebas en un ambiente controlado, localhost/RESPALDO/ para poder simular los ataques que permite la plataforma SEPI. se inicia el sitio web desde el enlace antes indicado, se realiza la primera prueba dejando vacías las cajas de texto, luego se presiona el botón de ingresar al sistema y podemos ver que a nivel de cliente la plataforma no tiene ninguna protección enviando datos vacíos a la base de datos (ver Figura 9)

Figura 9. Captura módulo login



Fuente: elaboración propia

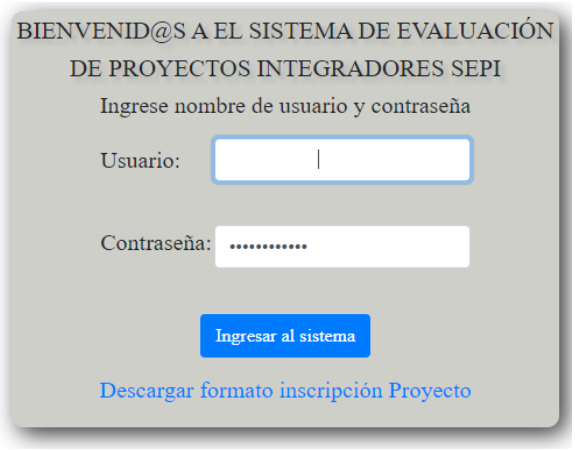
Figura 10. Comprobando el envío de datos vacíos



Fuente: elaboración propia

Seguido de la primera prueba se intenta ingresar datos vacíos con la barra espaciadora donde de igual forma permite escribir datos que son usados en los ataques más comunes en la inyección SQL

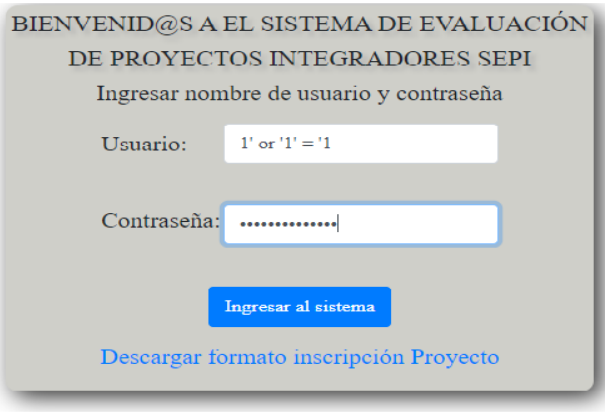
Figura 11. Ingreso de datos sin atributos



Fuente: elaboración propia

Se inicia con algo sencillo, uno de los ataques básicos y más usados por los atacantes, la línea de código 1' or '1' = '1 donde seguido de esto al presionar el botón de ingresar se puede ver que logra penetrar y mostrar datos importantes de la base de datos, por ejemplo, se puede ver el tipo de base de datos que se está usando y la conexión.

Figura 12. Módulo Login con Código Inyección SQL



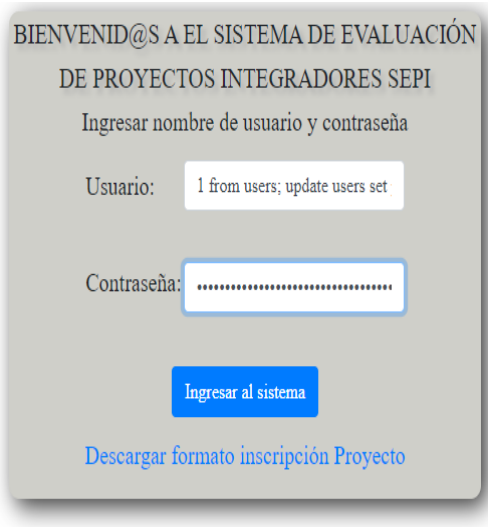
Fuente: elaboración propia

Figura 13. Muestra datos importantes de base de datos

Fuente: elaboración propia

Se persiste de igual forma atacando el sistema para descubrir datos importantes enviando una sentencia más específica y se puede ver de igual manera que muestra información de la base de datos.

Figura 14. Captura Insertando Línea de Códigos



Fuente: elaboración propia

Configuración de las Políticas de Seguridad

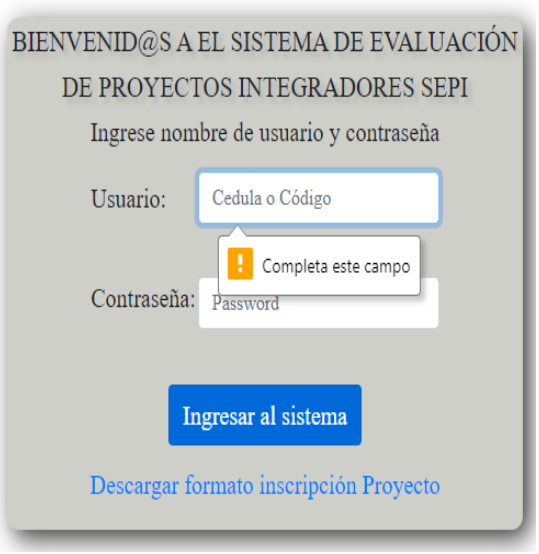
Para evitar el riesgo con procesos que pueden poner en peligro la información o posibles ataques a la Plataforma de Proyectos Integradores se establecen las siguientes políticas Generales de Seguridad de la Información.

No permitir caracteres especiales tales como comillas dobles, comillas sencillas y espacios.
No confiar en datos externos, validar la información con la base de datos.
Aceptar caracteres especiales específicos en la caja de texto de contraseñas que ayuden a fortalecer la construcción de una contraseña sólida tales como asteriscos, arrobas, puntos.

Luego de una serie de pruebas en un ambiente controlado, es decir, sin riesgos de sufrir un ciberataque a los datos personales, con la finalidad de verificar la efectividad de los atributos aplicados simulando el ingreso de datos y códigos que pueden penetrar el sistema, se obtuvo resultados exitosos gracias a la implementación de los atributos se logró evitar introducir líneas de códigos con caracteres especiales que permiten vulnerar una base de datos.

Con el atributo Required *se asegura* que los campos no estén vacíos, mostrando un mensaje que el usuario debe completar el campo.

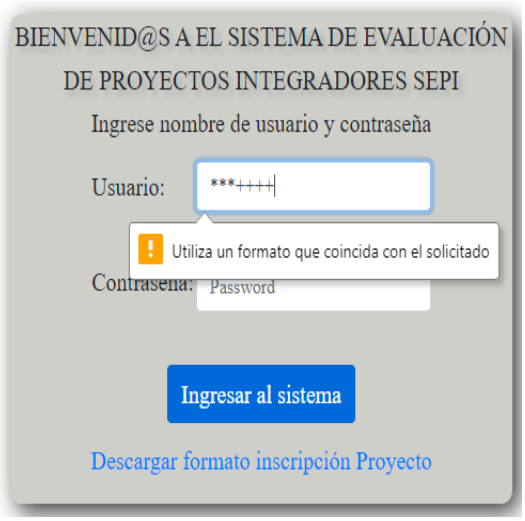
Figura 15. No permite enviar datos vacíos



Fuente: elaboración propia

En la captura al módulo se puede observar, luego de presionar el botón ingresar al sistema nos muestra un mensaje que es necesario introducir datos, así el sistema queda protegido a nivel de usuario.

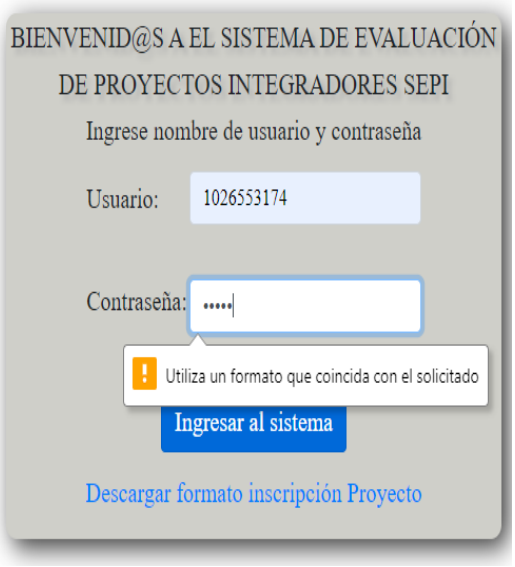
Figura 16. Protección Campo Usuario



Fuente: elaboración propia

Además del atributo anterior mencionado se protege el sistema con el atributo pattern que es el que permite decirle a nuestro input qué caracteres debe aceptar cuando un usuario malintencionado intenta introducir caracteres especiales, limitando el sistema solo a recibir los caracteres especiales indicados, tales como [-_+*], indicando con un mensaje "utiliza un formato que coincida con el solicitado". En la figura anterior se puede evidenciar que aplicó en la caja de texto del usuario y en la siguiente figura se aplica a la contraseña.

Figura 17. Protección Campo contraseña



Fuente: elaboración propia

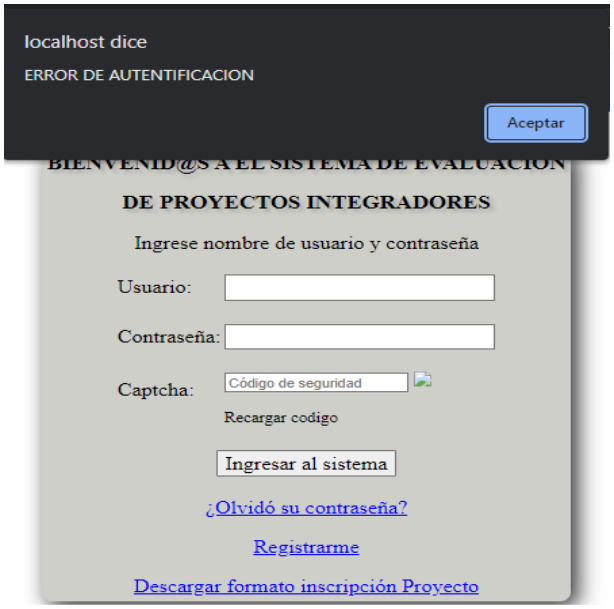
Si los datos del cliente son burlados se protege el servidor con la función ***mysq real Scape string,*** como lo muestra la siguiente imagen. Posteriormente al ingresar dando clic en el botón de ingresar al sistema se comprueba con una alerta que la protección al servidor está habilitada, desplegando una alerta como se puede ver en la siguiente imagen.

Tabla 3. Función Real Scape String

Función Real Scape String
include('conexion.php");$usuario=($_POST['usr']);$password=$_POST['pwd'];Susuario=
MySQL Real Escape String
($conexion, usuario);$password =
MySQL Real Escape String
($conexion, $password);$sqlconexion = "SELECT * FROM tblusuarioWHEREIDUsuario=$usr')ANDstrClave='$pwd"'$resultado=mysqliquery($conexion, $sq1conexion);$filas=mysqlinumrows($resultado);lom

Fuente: elaboración propia

Figura 18. Protección de autentificación.



Fuente: elaboración propia

Se intenta un inicio de sección con un usuario existente para comprobar que efectivamente a la hora de validar la información en la base de datos el ingreso es exitoso.

Figura 19. Ingreso con datos de usuario existente.

Fuente: elaboración propia

4. CONCLUSIONES

En la plataforma "Sistemas de Evaluación de Proyectos Integradores" SEPI, de la Corporación Universitaria Americana se pudo identificar debilidad en la administración y control de la información personal de docentes y estudiantes que interactúan en la misma, teniendo en cuenta que en el apartado del login no se aplicaron parámetros de autenticación en el que se pueda verificar que la persona que accede a la plataforma es el titular de la cuenta, colocando en riesgo información confidencial el cual debe ser fortalecido para prevenir vulneraciones a datos personales, dando cumplimiento a las normatividades nacionales e internacionales que protegen el habeas data.

El diseño de las políticas de seguridad para el sistema login de la plataforma SEPI, se enfocó en el nivel de seguridad del cliente con la utilización de (2) atributos denominados Required que sirve para evitar que los campos de información de manera obligatoria se envían vacíos en el que se utilice información que solo el usuario puede emplear y pattern en el que se programan o incorporan los caracteres permitidos para la creación de contraseñas las cuales acepta caracteres especiales excepto comillas dobles, simples y espaciado, se estima que estas políticas de seguridad contribuyen a fortalecer la seguridad de los datos personales de la plataforma.

Finalmente, en la implementación de las políticas de seguridad en el login de SEPI y la aplicación de la función Real Scape String el cual permite emitir alertas sobre datos no permitidos que intentan penetrar la base de datos, generando un fortalecimiento sobre los posibles ataques informáticos que puedan generarse en búsqueda de apropiarse de información personal de los estudiantes y docentes.

AGRADECIMIENTOS

Agradecemos a la Corporación Universitaria Americana por el desarrollo de este proyecto en el marco del programa formativo de diplomado de seguridad informática.

REFERENCIAS

Aguilar. (2018). La ley de protección de datos en Colombia: Sus inicios y examen de sus principales postulados. Obtenido de https://repository.ucatolica.edu.co/bitstream/10983/23060/1/La%20Ley%20De%20Protecci%C3%B3n%20De%20Datos%20En%20Colombia.pdf

Aldas, C. (2017). Seguridad de la Información en las Actividades Académicas Virtuales de la Carrera de Ingeniería en sistemas informáticos y Computacionales de las FISEI de la UTA. Obtenido de https://repositorio.uta.edu.ec/bitstream/123456789/27124/1/Tesis_%20t1359si.pdf

Avenía. (2017). Fundamentos de la Seguridad Informática. Obtenido de https://core.ac.uk/download/pdf/326424171.pdf

Congreso de la República de Colombia. (5 de enero de 2009). Ley 1273. Bogotá, Colombia: Diario Oficial No. 47.223.

Congreso de la República de Colombia. (17 de Octubre de 2012). Ley 1581. Bogotá, Colombia: Diario Oficial No. 48587.

Drake. (2008). Proceso de Desarrollo de Aplicaciones Sotware. Obtenido de https://www.ctr.unican.es/asignaturas/MC_OO/Doc/OO_08_I2_Proceso.pdf

Duartae, W. (2018). Diseño de Politicas de Seguridad para la red de datos de la Institución Universitaria Tecnológica de Comfacauca - Popayan a través de análisis, gestión de riesgos y vulnerabilidades. Obtenido de https://repository.unad.edu.co/jspui/bitstream/10596/21189/1/1061712760.pdf

Hernández. (2003). Los sistemas de información: Evolucion y Desarrollo. Universidad de Zaragoza, 1-15.

National Terrorism Advisory System. (14 de septiembre de 2022). Seguridad Cibernetica. Obtenido de https://www.ready.gov/es/ataque-cibernetico

Oñate, A. (2021). Propuesta de Políticas de Seguridad de la Información para proteger los activos de información en las organizaciones. Obtenido de https://repository.unad.edu.co/bitstream/handle/10596/41984/aonatear_3ago2021.pdf?sequence=1

Ortiz, F., & Garcia, D. (Enero - Diciembre de 2021). Sistema de Evaluación de proyectos integradores (SEPI): análisis de su implementación en la corporación universitaria americanaq. (C. U. Americana, Ed.) Ingente Americana, 1(1), 67-71. doi:https://doi.org/10.21803/ingecana.1.1.414

Pereira, Z. (1 de Enero - Junio de 2011). Los diseños de método mixto en la investigación en educación: Una experiencia concreta. (U. N. Rica, Ed.) Revista Electrónica Educare, 15(1), 15-29. Recuperado el 11 de Agosto de 2022, de https://www.redalyc.org/pdf/1941/194118804003.pdf

Sampieri. (1991). Metodología de la Investigación. México: McGraw Hill Education.

Soto, & Ducuara. (2018). Protección de Datos Personales en los Servicios de Internet. Obtenido de https://repository.ucatolica.edu.co/bitstream/10983/22521/1/Protecci%C3%B3n%20de%20Datos%20en%20los%20servicios%20de%20Internet.pdf