**Problemas de confidencialidad de los datos en plataforma de pagos de la Universidad Privada del Estado de México.**

***MAESTRO/A:*** RODRÍGUEZ MATÍNEZ YAZMÍN.

***ALUMNO:*** BACA GOMEZ RENE.

***MATERIA:*** AUDITORÍA EN SISTEMAS

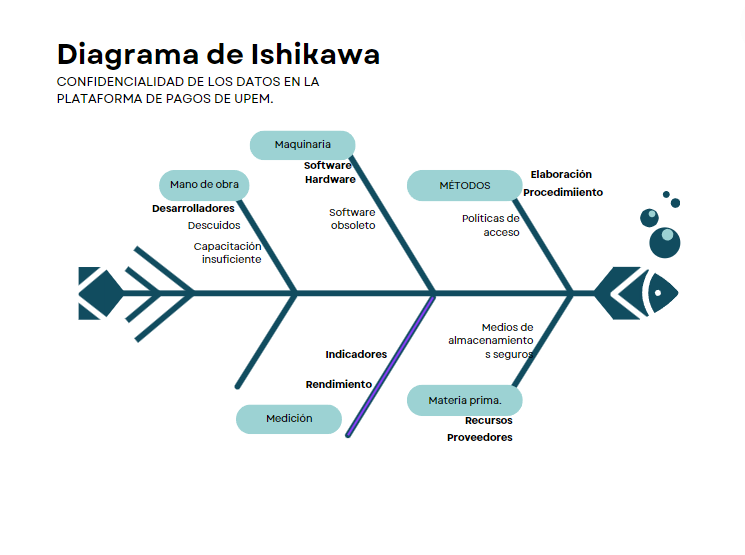


24/AGOSTO/2024

**Objetivo.**

Realizar una auditoría de la plataforma de pagos de la Universidad Privada del Estado de México del Plantel Tecámac para identificar las vulnerabilidades de seguridad relacionadas con el uso de contraseñas compartidas, evaluando su impacto en la protección de los datos personales y académicos de los estudiantes.

**Alcance.**

El alcance de este trabajo se centra en la evaluación de los problemas de seguridad, confidencialidad y usabilidad de la plataforma de pagos de la Universidad Privada del Estado de México Plantel Tecámac desde la perspectiva del usuario. A través de una auditoría, se identificarán las vulnerabilidades que permiten que, con solo conocer la matrícula de un estudiante, se pueda acceder a su información personal y académica debido al uso de una contraseña genérica. Además, se evaluarán los errores que comprometen la confidencialidad de los datos y la falta de adaptabilidad de la página en dispositivos móviles, ya que esta no se ajusta correctamente al contenido de la pantalla, lo que afecta la experiencia del usuario. 

|  |  |  |
| --- | --- | --- |
| Logotipo, nombre de la empresa  Descripción generada automáticamente | **LISTA DE VERIFICACIÓN** | **VERSIÓN:** |
| **CÓDIGO:** |
| **FECHA: 24 de Agosto del 2024** |

|  |  |
| --- | --- |
| Fecha: 24-Agosto-2024 | Auditoría: |
| Hora: 15:00 horas | Auditado: Universidad Privada del Estado de México |
| Ciudad: México | Auditor: Rene Baca Gómez. |

|  |  |  |  |
| --- | --- | --- | --- |
| REQUISITO A VERIFICAR | ESTADO DE CUMPLIMIENTO | | OBSERVACIONES Y/O COMENTARIOS |
| SI | NO |  |
| Contraseñas únicas. |  |  | Todos los usuarios poseen la misma contraseña, lo cual representa un riesgo de seguridad. |
| Responsividad y adaptabilidad para dispositivos celulares. |  |  | La barra de navegación no se ajusta al contenido total de la pantalla en un dispositivo móvil, lo cual afecta a la visibilidad de la página. |
| Tiempo de respuesta y optimización. |  |  | Superó con éxito la prueba de rendimiento de la herramienta “Page Speed Insights” de Google. |

**INFORME FINAL.**

**Análisis de Resultados.**

**Seguridad y Confidencialidad.** La auditoría reveló que la plataforma utiliza una contraseña genérica para todos los estudiantes, lo que representa un riesgo crítico de seguridad. Esta práctica permite que cualquier persona con acceso a la matrícula de un estudiante pueda visualizar sus datos personales y calificaciones, comprometiendo la confidencialidad de la información. Como señala Ruiz (2018), “el uso de contraseñas genéricas en sistemas digitales incrementa considerablemente el riesgo de acceso no autorizado, afectando la privacidad y seguridad de los usuarios.”

**Adaptabilidad en Dispositivos Móviles.** La auditoría identificó que la plataforma no se adapta correctamente a las pantallas de dispositivos móviles. Los elementos de la página se desajustan, lo que dificulta la navegación y afecta la accesibilidad de las funcionalidades de la plataforma, empeorando la experiencia del usuario. Como menciona García (2019), “un diseño web adaptativo es esencial para garantizar que los usuarios puedan acceder al contenido de manera óptima desde cualquier dispositivo, mejorando su experiencia y satisfacción.”

**Conclusiones.**

La auditoría confirma la existencia de graves vulnerabilidades en la plataforma de pagos de UPEM. La falta de seguridad en los mecanismos de autenticación pone en riesgo la confidencialidad de los datos de los estudiantes. Asimismo, la inadecuada adaptabilidad en dispositivos móviles limita el acceso eficiente y seguro a la plataforma, afectando tanto la usabilidad como la experiencia del usuario.

**Recomendaciones.**

1. Implementar contraseñas personalizadas para cada usuario, con políticas de cambio obligatorio y refuerzo mediante autenticación de dos factores.
2. Optimizar la plataforma para dispositivos móviles, asegurando una adecuada adaptación a las pantallas de diferentes tamaños y resoluciones.
3. Establecer un monitoreo constante de las prácticas de seguridad y realizar pruebas periódicas para identificar y corregir nuevas vulnerabilidades.

Referencias.

García, L. (2019). Importancia del diseño web adaptativo. Universidad Mexicana. Recuperado de <https://unimex.edu.mx/Investigacion/DocInvestigacion/Importancia_del_diseno_web_adaptativo.pdf>

Ruiz, M. (2018). Riesgos de seguridad en el uso de contraseñas genéricas en plataformas digitales. Universidad Autónoma del Estado de Hidalgo. Recuperado de <https://www.uaeh.edu.mx/scige/boletin/tlahuelilpan/n6/e5.html>