DOCUMENTACION DEL PROYECTO **ACCESS DGETI**

Introducción

Este proyecto aborda la problemática del actual sistema de control de acceso en el DGETI, caracterizado por la inseguridad y los altos costos asociados con las credenciales físicas. La solución propuesta es un sistema innovador basado en credenciales digitales, ofreciendo una alternativa segura y eficiente que reduce significativamente los gastos. Este sistema permite registrar con precisión las entradas y salidas de los estudiantes, limitando el uso de cada credencial digital a dos accesos diarios para prevenir el uso compartido y mejorar la seguridad del plantel. A diferencia del sistema actual, el proyecto elimina el riesgo de extravío de credenciales físicas que contienen información personal sensible, además de reducir los costos de impresión y distribución. El desarrollo se basa en una arquitectura robusta que integra tecnologías web como JavaScript, PHP, JSON, AJAX, HTML, CSS y MySQL, garantizando un sistema confiable y escalable para las necesidades del DGETI.

Planteamiento del problema

Planteamiento del Problema: Inseguridad y Costos en el Control de Acceso del DGETI

El sistema actual de control de acceso en el DGETI, basado en credenciales físicas, presenta diversas deficiencias que comprometen la seguridad del plantel y generan costos innecesarios para los estudiantes. Estas deficiencias se manifiestan en varios aspectos críticos:

1. Vulnerabilidad a Accesos No Autorizados: La facilidad con la que se extravían o son robadas las credenciales físicas representa una seria amenaza a la seguridad. Estas credenciales, que contienen información personal sensible como CURP y número de control, pueden ser utilizadas por personas ajenas al plantel, facilitando el acceso no autorizado a las instalaciones y poniendo en riesgo la integridad de la comunidad estudiantil. Además, la posibilidad de que un alumno extravíe su credencial y luego la recupere, o incluso la reporte como perdida para obtener una nueva, permite un acceso duplicado y facilita la entrada o salida no autorizada de otros estudiantes utilizando la misma credencial. La modificación de la información para dar de baja una credencial y solicitar una nueva es un proceso engorroso y poco eficiente.

2. Uso Compartido de Credenciales: La práctica común del uso compartido de credenciales entre estudiantes vulnera aún más la seguridad del plantel. La falta de control individual sobre el acceso permite que múltiples alumnos utilicen la misma credencial para entrar o salir, dificultando el seguimiento y la identificación de los estudiantes presentes en el plantel en un momento dado. Esta situación dificulta la notificación a tutores en caso de ausencias o salidas no autorizadas.

3. Costos Económicos para los Estudiantes: La frecuente pérdida o daño de las credenciales físicas representa un gasto significativo para los alumnos, quienes deben pagar por su reposición. Este costo, que puede superar los 100 pesos, representa una carga económica adicional para los estudiantes y sus familias, recursos que podrían destinarse a materiales escolares o necesidades más urgentes. El costo acumulado por la reposición de credenciales perdidas representa un gasto considerable para la comunidad estudiantil en su conjunto.

4. Ineficiencia en la Gestión de Credenciales: El proceso de reposición de credenciales perdidas o dañadas es ineficiente y engorroso. La solicitud, emisión y entrega de nuevas credenciales implican tiempo y recursos administrativos, generando una carga adicional para el personal del plantel. La falta de un sistema de seguimiento eficiente dificulta el control del inventario de credenciales y la detección de posibles irregularidades.

En resumen, el sistema actual de control de acceso presenta una serie de vulnerabilidades que comprometen la seguridad del plantel, generan costos innecesarios para los estudiantes y dificultan la gestión eficiente de los accesos. Estas deficiencias justifican la necesidad de implementar un sistema de control de acceso más seguro, eficiente y económico, como el que se propone en este proyecto.

Justificación

Justificación: Un Sistema de Control de Acceso Digital para el DGETI

Este proyecto justifica su implementación por la imperiosa necesidad de mejorar la seguridad y eficiencia del control de acceso en los planteles del DGETI, abordando las deficiencias del sistema actual basado en credenciales físicas. La problemática actual se centra en la vulnerabilidad a accesos no autorizados, el uso indebido de credenciales y los costos económicos que esto genera para los estudiantes. El sistema propuesto ofrece una solución integral a estos problemas, proporcionando un entorno más seguro y eficiente para toda la comunidad educativa.

Beneficios en Seguridad: El sistema de credenciales digitales, con su limitación de dos accesos diarios por estudiante, elimina la posibilidad del uso compartido de credenciaqles y reduce significativamente el riesgo de accesos no autorizados. La eliminación de las credenciales físicas minimiza el riesgo de extravío o robo, protegiendo la información personal de los estudiantes y la seguridad del plantel. El registro preciso de entradas y salidas permite un mejor control y monitoreo de la presencia estudiantil, facilitando la notificación a tutores en caso de ausencias o salidas no autorizadas. La implementación de este sistema contribuye a la creación de un ambiente de aprendizaje más seguro y confiable. Estudios realizados en planteles similares (como el caso del CETis 17, donde se han registrado al menos tres incidentes de ingresos no autorizados) demuestran la necesidad de un sistema de control de acceso más robusto. La falta de credenciales en un número significativo de alumnos (estimado en 900 alumnos de nuevo ingreso solo en el turno matutino, lo que implica potencialmente más de 2700 alumnos sin registro diario) evidencia la necesidad de una solución que asegure un mejor control de acceso.

Beneficios Económicos: El sistema digital elimina los costos asociados con la impresión, distribución y reposición de las credenciales físicas, generando un ahorro significativo para los estudiantes y la institución. El uso de dispositivos móviles y una cuenta institucional reduce la necesidad de invertir en infraestructura adicional, como lectores de credenciales físicas. La gestión centralizada de las credenciales digitales simplifica los procesos administrativos y reduce la carga de trabajo del personal del plantel. La reducción de costos en la administración de credenciales permite una mejor asignación de recursos a otras áreas prioritarias de la institución. Además, la colaboración con un proveedor de servicios para la administración del servidor reduce la necesidad de inversión en infraestructura tecnológica por parte del plantel.

Beneficios Educativos y Sociales: Este proyecto promueve la innovación tecnológica en el ámbito educativo, fomentando el uso de herramientas digitales para mejorar la seguridad y la eficiencia. La implementación del sistema ofrece una valiosa oportunidad para adquirir experiencia y conocimientos en el campo de la ciberseguridad y el desarrollo de servicios web. El proyecto beneficia a múltiples actores: estudiantes, docentes, personal administrativo, padres de familia y la institución en su conjunto. La investigación y la implementación de este sistema contribuyen a la creación de un entorno educativo más seguro y eficiente, generando un impacto positivo en la comunidad educativa y la sociedad en general. La recopilación de datos sobre incidentes de seguridad permitirá una mejor comprensión de la problemática y la implementación de medidas preventivas más efectivas.

En resumen, la justificación de este proyecto reside en su capacidad para abordar de manera integral los problemas de seguridad y costos asociados al sistema actual de control de acceso en el DGETI, ofreciendo una solución innovadora, eficiente y económica que beneficia a toda la comunidad educativa. La inversión en este proyecto representa una contribución significativa a la seguridad, la eficiencia y el desarrollo tecnológico de las instituciones educativas.

Objetivos

Objetivos: Sistema de Control de Acceso Digital DGETI

Objetivo General:

Implementar un sistema de control de acceso basado en credenciales digitales seguro, eficiente y amigable para el usuario en los planteles del DGETI. Este sistema debe mejorar la seguridad del plantel, reducir los costos asociados con la gestión de credenciales y optimizar la experiencia de los estudiantes y el personal. La implementación exitosa del sistema debe contribuir a la creación de un entorno educativo más seguro, eficiente y confiable.

Objetivos Específicos:

1. Mejorar la Seguridad del Plantel: Reducir significativamente los accesos no autorizados al plantel mediante la implementación de un sistema de credenciales digitales con medidas de seguridad robustas. Se espera alcanzar una reducción del 90% en el uso múltiple de credenciales y una disminución del 80% en la pérdida o robo de credenciales físicas dentro de los primeros tres meses de la implementación del sistema. Este objetivo se logrará mediante la limitación de accesos por credencial, el registro preciso de entradas y salidas y la eliminación de las credenciales físicas. Se implementarán medidas de seguridad adicionales para prevenir accesos no autorizados, como la autenticación multifactorial y el monitoreo continuo del sistema.

2. Reducir Costos de Gestión de Credenciales: Minimizar los costos asociados con la emisión, distribución y reposición de las credenciales físicas. Se espera un ahorro del 70% en estos costos dentro del primer año de implementación del sistema. Este ahorro se logrará mediante la eliminación de los gastos de impresión, distribución y reposición de credenciales físicas, así como la simplificación de los procesos administrativos. Se buscará optimizar la gestión de recursos y la asignación de presupuesto para maximizar el impacto del ahorro.

3. Optimizar la Eficiencia Administrativa: Automatizar el proceso de control de acceso para mejorar la eficiencia administrativa del plantel. Se espera un aumento del 60% en la eficiencia administrativa dentro de las primeras pruebas del sistema. Este objetivo se logrará mediante la implementación de un sistema automatizado que registre las entradas y salidas de los estudiantes, genere reportes de acceso y facilite la gestión de las credenciales digitales. Se buscará simplificar los procesos administrativos, reducir el tiempo de trabajo dedicado a la gestión de credenciales y mejorar la precisión de los datos.

4. Mejorar la Experiencia del Usuario: Diseñar un sistema de credenciales digitales fácil de usar e intuitivo para los estudiantes y el personal del plantel. Se buscará obtener retroalimentación de los usuarios para asegurar la usabilidad y la satisfacción con el sistema. Se implementarán mecanismos de soporte técnico y capacitación para asegurar una adopción exitosa del nuevo sistema. Se buscará una experiencia de usuario positiva que fomente la colaboración y la aceptación del sistema por parte de la comunidad educativa.

Estos objetivos específicos, en conjunto, contribuirán al logro del objetivo general de implementar un sistema de control de acceso seguro, eficiente y económico en los planteles del DGETI, mejorando la seguridad, la eficiencia y la experiencia de todos los usuarios.

Tipo de Investigación

Tipo de Investigación: Un Enfoque Mixto

Este proyecto de investigación se caracteriza por un enfoque mixto, combinando elementos de investigación exploratoria, diagnóstica y explicativa, a la vez que se sitúa en el espectro entre la investigación básica y la aplicada (tecnológica).

1. Enfoque Cualitativo (Exploratorio y Diagnóstico):

La investigación inicia con una fase exploratoria para familiarizarse con el problema de la seguridad en el acceso al plantel del DGETI. Esta fase implica la identificación de las necesidades y problemas relacionados con el sistema actual de control de acceso, incluyendo la recolección de datos cualitativos (entrevistas, observaciones, etc.) para comprender la perspectiva de los diferentes actores involucrados (estudiantes, personal administrativo, docentes, etc.). Posteriormente, se realiza una fase diagnóstica para analizar las causas y consecuencias de los problemas identificados en la fase exploratoria. Esto implica un análisis profundo de las variables que contribuyen a la inseguridad y la ineficiencia del sistema actual, estableciendo relaciones de causa y efecto entre ellas.

2. Enfoque Cuantitativo (Explicativo):

La fase explicativa se centra en el análisis cuantitativo de los datos obtenidos para comprender las relaciones entre las variables identificadas en la fase diagnóstica. Se busca cuantificar el impacto de las diferentes variables en la seguridad del plantel y la eficiencia del control de acceso. Esto implica el uso de métodos estadísticos para analizar los datos recolectados y evaluar la efectividad de la solución propuesta (el sistema de credenciales digitales). La hipótesis planteada se somete a prueba mediante la recolección y análisis de datos cuantitativos, lo que permite evaluar la validez de las predicciones realizadas.

3. Investigación Básica y Aplicada (Tecnológica):

Este proyecto se ubica en el espectro entre la investigación básica y la aplicada. Por un lado, la investigación contribuye al conocimiento teórico sobre la seguridad en el acceso a instituciones educativas y la aplicación de la tecnología para resolver problemas complejos en este ámbito. Se exploran y analizan las diferentes variables relacionadas con la seguridad, generando conocimiento que puede ser aplicado a otros contextos. Por otro lado, el proyecto tiene un fuerte componente aplicado, ya que busca resolver un problema específico mediante el diseño, desarrollo e implementación de un prototipo funcional: el sistema de credenciales digitales. La investigación se centra en la aplicación práctica de la tecnología para mejorar la seguridad y la eficiencia del control de acceso en el plantel. Se busca demostrar la viabilidad y la efectividad de la solución propuesta en un contexto real.

En resumen, este proyecto de investigación utiliza un enfoque mixto, combinando métodos cualitativos y cuantitativos para comprender a profundidad el problema, diagnosticar sus causas y evaluar la efectividad de la solución propuesta. Se sitúa en el espectro entre la investigación básica y aplicada, contribuyendo al conocimiento teórico y ofreciendo una solución práctica a un problema real en el contexto del DGETI.

Descripción del desarrollo e implementación del prototipo

Desarrollo e Implementación del Prototipo: DGETI ACCESS

El proyecto DGETI ACCESS aborda la problemática de accesos múltiples con una misma credencial y los altos costos de reposición asociados al sistema de credenciales físicas en los planteles del DGETI. La solución propuesta es un sistema de credencial digital que mejora la seguridad, reduce costos y optimiza la experiencia del usuario.

Descripción del Prototipo:

DGETI ACCESS es un sistema de control de acceso basado en credenciales digitales que reemplaza las credenciales físicas tradicionales. El prototipo actual se compone de tres elementos principales:

1. Plataforma Web de Gestión: Una plataforma web desarrollada con PHP, MySQL, AJAX, JSON, HTML, CSS y JavaScript para la administración de las credenciales digitales de los estudiantes. Esta plataforma permite la gestión de usuarios, la generación de credenciales digitales y la generación de reportes de acceso.

2. Lector de Códigos QR (Prototipo): Un lector de códigos QR se utiliza actualmente como prototipo para la verificación de la identidad de los estudiantes. Este lector escanea el código QR único asociado a cada credencial digital, permitiendo el registro de entrada y salida.

3. Subpágina de Visualización: Una subpágina web que muestra la credencial digital del estudiante, incluyendo su información personal, fotografía y el código QR para el acceso al plantel.

Metodología de Desarrollo:

La metodología de desarrollo se basó en un ciclo iterativo de diseño, desarrollo y pruebas. Se realizó una investigación exhaustiva para determinar los requisitos del sistema y comprender las necesidades de los usuarios. El diseño del sistema se enfocó en la seguridad, la usabilidad y la eficiencia. El desarrollo se realizó utilizando las tecnologías mencionadas anteriormente (PHP, MySQL, AJAX, JSON, HTML, CSS y JavaScript), siguiendo las mejores prácticas de desarrollo de software. Se realizaron pruebas exhaustivas para garantizar la seguridad, la eficiencia y la estabilidad del sistema. El proceso de pruebas incluyó pruebas unitarias, pruebas de integración y pruebas de usuario. El sistema se sometió a pruebas continuas para la detección y corrección de errores ("bugs").

Resultados del Prototipo:

El prototipo de DGETI ACCESS ha demostrado ser eficaz en la limitación de accesos a dos por día y por estudiante, mejorando significativamente la seguridad del plantel. Las pruebas realizadas indican una reducción significativa en los costos asociados con la emisión y reemplazo de credenciales (estimada en un 80%). El registro de acceso es más rápido y cómodo para los estudiantes, y el sistema ofrece una mayor seguridad en comparación con las credenciales físicas.

Futuras Mejoras:

El prototipo actual es una versión inicial del sistema. Se prevén las siguientes mejoras para futuras versiones:

- Aplicación Móvil: Desarrollo de una aplicación móvil para facilitar el acceso a las credenciales digitales y el registro de entrada y salida para los estudiantes.

- Diseño de Credencial Digital: Diseño de una credencial digital completa que incluya toda la información relevante del estudiante.

- API de Generación de Códigos QR: Desarrollo de una API que genere automáticamente los códigos QR de manera diaria para cada estudiante, asegurando la actualización constante y la seguridad del sistema.

En resumen, el prototipo de DGETI ACCESS ha demostrado la viabilidad y la eficacia de un sistema de credenciales digitales para mejorar la seguridad y eficiencia del control de acceso en el DGETI. Las futuras mejoras previstas fortalecerán aún más el sistema, ofreciendo una solución integral y robusta a la problemática actual.