EDUCACIÓN
SECRETARÍA DE EDUCACIÓN PÚBLICA

TECNOLÓGICO NACIONAL DE MÉXICO

# CASO DE NEGOCIO SIA (Sistema Integral de Acceso)

## *1. Introducción y Resumen Ejecutivo*

El sistema Integral de Acceso (SIA ) está diseñado para optimizar la gestión de accesos dentro de la institución.El propósito del SIA es facilitar un control eficiente , mejorar la seguridad y aumentar la rapidez con la que pueden gestionar permisos y accesos. Este documento pretende delimitar las necesidades actuales , justificar la implementación de SIA , y evaluar tanto los posibles riesgos como la visibilidad financiera del proyecto.

**Descripción del Proyecto**: SIA es una solución integral para gestionar el acceso en el Instituto Tecnológico Superior de Atlixco (ITSA) mediante el uso de códigos QR, con funcionalidades para la creación de informes, monitoreo de acceso y control avanzado de seguridad.

**Objetivo General**: Agilizar, controlar y mejorar la seguridad del acceso a las instalaciones, facilitando a los usuarios un proceso rápido y seguro al ingresar y egresar del campus.

**Plazo de Desarrollo Estimado**: 6 meses para la implementación de la aplicación en Android Studio con Kotlin y React Native para la integración de sistemas externos.

## 2. Definición del Problema

Muchas Organizaciones enfrentan desafíos significativos en la gestión de accesos . Los sistemas tradicionales suelen ser lentos , difíciles de manejar y vulnerables a errores manuales que complementan la seguridad. Estos problemas generan ineficiencias operativas e incrementan el riesgo de accesos no autorizados

**Problema**: Procesos manuales de acceso generan demoras, poca capacidad de respuesta y vulnerabilidad ante accesos no autorizados.
**Impacto**: Afecta la experiencia del usuario, aumenta los costos operativos de seguridad y expone a la institución a riesgos de seguridad.

## 3. Justificación de la Solución

La implementación del SIA proporciona un enfoque centralizado y automatizado que garantiza la correcta asignación de permisos mientras disminuye el tiempo y esfuerzo requerido por estas tareas. La solución es escalable , segura , y se adapta a diferentes tamaños y tipos de organizaciones, esta implementación reducirá los riesgos de fallos manuales y mejorará la seguridad general.

**Beneficios Esperados**:

- Reducción en tiempos de acceso, mejor seguimiento de usuarios, y seguridad avanzada gracias a la autenticación multifactor (MFA).
- Capacidad de generar informes y auditorías en tiempo real para la administración.
- Integración con cámaras y sistemas de monitoreo para una vigilancia continua.

**Regulaciones y Cumplimiento**: Con el SIA, la institución cumple con normativas de protección de datos personales y gestión de accesos.

## *4. Análisis de Riesgo*

Los riesgos Identificados incluyen:

Integración técnica con sistemas existentes, que puede ser complejo.
Resistencia al cambio por parte del personal ,afectando la adopción del sistema.
Posibles costos ocultos durante la implementación.
Para mitigar estos riesgos, se establecerán sesiones de formación y se asignará a un equipo técnico para abordar los problemas de integración.

**Riesgos Identificados y Estimaciones de Impacto**:

**Falla de Infraestructura Tecnológica**: Probabilidad alta, impacto alto. Mitigación: Redundancia.

**Compromiso de Datos Personales**: Probabilidad media, impacto alto. Mitigación: Módulos de encriptación y auditoría.

**Capacitación Insuficiente del Personal**: Probabilidad media, impacto medio. Mitigación: Capacitación continua y guías de respuesta rápida

| ID de Riesgo | Descripción | Probabilidad | Impacto | Nivel de Riesgo | Estrategia de Mitigación |
|---|---|---|---|---|---|
| R-01 | Falla en la infraestructura tecnológica | Alta | Alta | Alto | Implementar redundancia realizar respaldos periódicos y pruebas de carga |
| R-02 | Compromiso de datos personales | Media | Alta | Alto | Usar encriptación de datos, realizar auditorías de seguridad y control de accesos |
| R-03 | Capacitación insuficiente del personal | Media | Medio | Medio | Programar capacitaciones regulares y proporcionar guías de usuario |
| R-04 | Incumplimiento de plazos de desarrollo | Media | Alto | Alto | Definir sprints realistas, monitorear avances y hacer ajustes continuos |
| R-05 | Fallo en la integración con cámaras de seguridad | Media | Alto | Alto | Realizar pruebas de integración tempranas y establecer planes de contingencia |
| R-06 | Fallo en la autenticación multifactor (MFA) | Baja | Alta | Medio | Implementar autenticación de respaldo y pruebas extensivas de MFA |

| | | | | | |
|---|---|---|---|---|---|
| R-07 | Aumento de usuarios que sobrecargue la infraestructura | Baja | Medio | Medio | Escalabilidad en la infraestructura de servidores y realizar pruebas de estrés |
| R-08 | Fallo en la generación automática de informes | Media | Medio | Medio | Programar validaciones regulares y pruebas de generación de reportes |
| R-09 | Mal manejo de permisos de usuario que afecte la seguridad | Media | Alta | Alto | Establecer revisiones periódicas de permisos y controles de acceso |
| R-10 | Dificultad en la adaptación de los usuarios al sistema de acceso | Media | Medio | Medio | Diseñar una interfaz intuitiva, con tutoriales y soporte en línea |

## *5. Viabilidad Financiera*

El costo del proyecto integridad se estima , con un retorno de inversión proyectado en dos años debido a los ahorros  en tiempo gestión y reducciones de incidentes  de seguridad. Un análisis detallado de costos y beneficios sugiere una eficacias en la inversión de  a largo  plazo

**Costos Iniciales Estimados**:

- **Desarrollo del Sistema**: Alrededor de $20,000 USD, considerando desarrollo, pruebas y ajustes de seguridad.
- **Infraestructura  localmente y Bases de Datos**: Aproximadamente $5,000 USD anuales para almacenamiento y procesamiento en tiempo real.
- **Capacitación**: $2,000 USD para la capacitación inicial y recursos de formación.

**Retorno de Inversión (ROI)**:

- **Ahorro en Personal y Tiempo**: Se estima un ahorro anual del 20% en costos operativos de seguridad.
- **Optimización Operativa**: Reducción de cuellos de botella y de errores en el acceso, mejorando la experiencia de estudiantes y personal.
- **Escalabilidad para Futuras Necesidades**: Proyectado para soportar hasta 1,500 usuarios, con posibles expansiones en la base de datos.

## *6. Estimaciones*

**Historias de Usuario y Puntos Estimados**: Cada historia de usuario está cuantificada con puntos de esfuerzo y riesgos de desarrollo, priorizadas según la funcionalidad crítica.

- **Alta de Usuarios**: Puntos estimados: 8. Riesgo: medio.
- **Generación de Informes de Acceso**: Puntos estimados: 10. Riesgo: alto.
- **Autenticación Multifactor (MFA)**: Puntos estimados: 12. Riesgo: alto.
- **Integración con Cámaras de Seguridad**: Puntos estimados: 10. Riesgo: alto.
- **Registro de Acceso mediante Código QR**: Puntos estimados: 8. Riesgo: medio.

**Total de Puntos de Esfuerzo Estimado**: 70 puntos para el proyecto completo, distribuidos en sprints, con un enfoque de desarrollo iterativo para priorizar y ajustar según las necesidades de la institución.