**UNIVERSIDAD PRIVADA DE TACNA**

**FACULTAD DE INGENIERÍA**

**Escuela Profesional de Ingeniería de Sistemas**

****

**“Proyecto AccessGuard - Sistema de control de acceso a las instalaciones físicas de la UPT aplicando tecnología de respuesta de validación por voz”**

Curso: ***Soluciones Móviles I***

Docente: ***Ing. Elard Rodríguez Marca***

Integrantes:

**Arce Bracamonte, Sebastian Rodrigo (2019092986)**

**Chávez Linares, César Fabián (2019063854)**

**Hernández Cruz, Angel Gadiel (2021070017)**

**Tacna – Perú**

***2025***

| CONTROL DE VERSIONES | | | | | |
| --- | --- | --- | --- | --- | --- |
| Versión | Hecha por | Revisada por | Aprobada por | Fecha | Motivo |
| 1.0 | CCL | SAB | AHC | 30/06/2025 | Versión Original |

**Proyecto AccessGuard - Sistema de control de acceso a las instalaciones físicas de la UPT aplicando tecnología de respuesta de validación por voz**

Propuesta de Proyecto

Versión *1.0*

| CONTROL DE VERSIONES | | | | | |
| --- | --- | --- | --- | --- | --- |
| Versión | Hecha por | Revisada por | Aprobada por | Fecha | Motivo |
| 1.0 | CCL | SAB | AHC | 30/06/2025 | Versión Original |

**Tabla de contenido**

Resumen Ejecutivo

I Propuesta narrativa

1. Planteamiento del Problema
2. Justificación del proyecto
3. Objetivo general
4. Beneficios
5. Alcance
6. Requerimientos del sistema
7. Restricciones
8. Supuestos
9. Resultados esperados
10. Metodología de implementación
11. Actores claves
12. Papel y responsabilidades del personal
13. Plan de monitoreo y evaluación
14. Cronograma del proyecto
15. Hitos de entregable

II Presupuesto

1. Planteamiento de aplicación del presupuesto
2. Presupuesto

3. Análisis de Factibilidad

4. Evaluación Financiera

Anexo 01 – Requerimientos del Sistema Proyecto AccessGuard

1. **Planteamiento del problema**

En la actualidad, las universidades enfrentan desafíos significativos en la gestión del acceso físico a sus instalaciones, especialmente en contextos donde el control se realiza de forma manual o con mecanismos poco eficientes. En el caso de nuestra universidad, el proceso de validación de ingreso para estudiantes que no porten su carné universitario o lo han extraviado se realiza mediante registros manuales, lo cual genera múltiples inconvenientes.

Esta modalidad no solo representa una carga operativa adicional para el personal de seguridad, sino que también incrementa el riesgo de errores humanos, suplantación de identidad y demoras en el ingreso. Además, la falta de un sistema automatizado impide el registro y seguimiento eficiente de los accesos, dificultando la toma de decisiones en casos de emergencia, control de aforo o verificación de movimientos dentro del campus.

La ausencia de un canal tecnológico moderno que centralice la gestión de acceso limita la capacidad de la universidad para brindar un entorno más seguro, organizado y acorde con las demandas tecnológicas actuales de la comunidad estudiantil. Esta situación pone en evidencia la necesidad de implementar un sistema automatizado, accesible desde dispositivos móviles, que permita validar el ingreso a las instalaciones de forma rápida, segura y confiable, incluso en ausencia del carné físico.

1. **Justificación del proyecto**

El presente proyecto surge como respuesta a una problemática concreta que afecta la operatividad diaria y la seguridad de la universidad: el limitado control de acceso a sus instalaciones físicas. La dependencia de métodos manuales para el registro de ingreso de estudiantes que no portan su carné universitario representa una solución poco eficiente, propensa a errores y vulnerable a suplantaciones de identidad.

En un contexto donde la transformación digital es esencial para optimizar los procesos institucionales, la implementación de un Sistema de Control de Acceso mediante un Aplicativo Móvil representa una alternativa innovadora, accesible y segura. Este sistema permitirá a los estudiantes validar su identidad desde sus dispositivos móviles mediante autenticación digital, evitando la necesidad del carné físico y reduciendo los tiempos de espera en los puntos de ingreso.

Asimismo, el proyecto aporta valor tanto al personal administrativo como a los equipos de seguridad, al proporcionar una plataforma centralizada desde la cual se podrá monitorear, registrar y auditar los accesos en tiempo real. Esta información será clave para mejorar la toma de decisiones en temas de seguridad, gestión de aforo y trazabilidad en casos de emergencia.

Desde una perspectiva tecnológica y social, el proyecto contribuye a la modernización de los servicios universitarios, fortaleciendo la confianza de la comunidad estudiantil en los sistemas institucionales. Además, promueve la eficiencia operativa y la sostenibilidad, al reducir el uso de papel y los procesos burocráticos asociados a los registros manuales.

En resumen, el desarrollo de este sistema no solo responde a una necesidad actual, sino que también posiciona a la universidad como una institución comprometida con la innovación, la seguridad y la mejora continua de sus procesos administrativos y académicos.

1. **Objetivo del proyecto**

Desarrollar un aplicativo móvil que permita gestionar de manera eficiente y segura el acceso de los estudiantes a las instalaciones físicas de la universidad, mediante la validación digital de identidad, con el fin de optimizar los procesos de ingreso, reducir el uso del registro manual y fortalecer el control institucional.

1. **Beneficios**

* **Mejora en el control de acceso**Permite validar la identidad de los estudiantes de forma rápida y confiable, reduciendo el ingreso no autorizado a las instalaciones.
* **Reducción del registro manual**Disminuye la dependencia de procesos escritos y físicos, lo cual evita errores, pérdidas de información y colas innecesarias.
* **Disponibilidad y comodidad**Los estudiantes pueden ingresar utilizando su dispositivo móvil, incluso si han olvidado su carnet físico.
* **Seguridad de la información**La validación digital protege los datos personales de los usuarios mediante protocolos de cifrado y autenticación.
* **Ahorro de recursos**Minimiza el uso de papel y el tiempo del personal encargado del control de ingreso, permitiendo que se concentren en otras tareas.
* **Datos en tiempo real**Permite a los administradores y supervisores conocer en tiempo real quién ha ingresado, mejorando la trazabilidad y la toma de decisiones.
* **Escalabilidad del sistema**El aplicativo puede ser escalado en el futuro para incorporar nuevas funciones como control de asistencia a clases, eventos o acceso a laboratorios y bibliotecas.

1. **Alcance**

El proyecto abarca todos los siguientes campos en los respectivos temas;

**Desarrollo de un aplicativo móvil** Permitirá a los estudiantes identificarse utilizando su teléfono inteligente, reemplazando parcial o totalmente el uso del carnet físico.  
**Funcionalidad de validación de identidad** El sistema integrará un código QR dinámico o token único asociado a cada usuario, que podrá ser escaneado por el personal de seguridad para permitir o denegar el acceso.  
**Registro automático de ingresos** Cada validación quedará registrada automáticamente en una base de datos, permitiendo el monitoreo y generación de reportes históricos.  
**Panel de control administrativo (mínimo en versión web o de escritorio)** Para personal autorizado, que podrá consultar reportes, gestionar usuarios y revisar el historial de accesos por día, hora y ubicación.  
**Gestión de usuarios y roles** El sistema incluirá perfiles diferenciados (estudiante, seguridad, administrador) con funcionalidades específicas para cada uno.

**Notificaciones al usuario** En caso de que el acceso sea rechazado por vencimiento de matrícula, sanción u otra razón, el estudiante será notificado mediante la app.

1. **Requerimientos del sistema**

**Hardware:** Smartphones con cámara, servidores en la nube.

**Software:** Flutter (app), Firebase (BD), Android Studio.

**6.1 Hardware Necesario**

Para guardias:

Smartphones con cámara básica (5MP+ suficiente para leer códigos de barras)

Servidores:

Firebase, almacenamiento para 10,000+ códigos de barras únicos

**6.2 Software Esencial**

Aplicación móvil (Flutter):

flutter\_barcode\_scanner: Para leer códigos de barras

firebase\_database: Almacenamiento centralizado

Backend (Firebase):

Firebase Realtime Database (estructura optimizada para búsquedas por código de barras)

FireStorage

**6.3 Flujo de Trabajo**

Validación:

Guardias escanean con sus smartphones

App muestra datos básicos del usuario

Registra timestamp de acceso

**6.4 Ventajas Clave**

Más económico: No requiere cámaras de alta gama

Universal: Funciona hasta con los celulares más básicos

Robusto: Códigos de barras son legibles incluso dañados parcialmente

Fácil implementación: Librerías maduras y documentadas

1. **Restricciones**

**7.1 Restricciones Técnicas**

**Compatibilidad de Dispositivos:**

Solo smartphones con Android 8.0+ o iOS 12+

Cámaras deben tener enfoque automático para lectura óptima de códigos

**Limitaciones de Firebase:**

Límite de 50,000 operaciones diarias en el plan gratuito

Máximo 1GB de almacenamiento en la versión básica

**Conectividad**:

Requiere conexión mínima de 3G para operaciones en tiempo real

**7.2 Restricciones Operativas**

**Capacidad de Usuarios:**

Máximo 500 usuarios activos simultáneos

Hasta 1,000 escaneos por hora en un solo punto de acceso

**Procesos Manuales:**

Registro inicial de usuarios requiere validación presencial

Actualización de datos personales con aprobación administrativa

**Seguridad:**

Los códigos de barras deben renovarse cada semestre

No admite autenticación biométrica

**7.3 Restricciones Legales**

**Protección de Datos:**

Almacenamiento limitado a información esencial

Historial de accesos se purga automáticamente después de 6 meses

**Normativas Institucionales:**

Horarios de acceso definidos por reglamento universitario

Visitantes externos requieren autorización previa por escrito

**7.4 Restricciones de Implementación**

**Tiempos de Respuesta:**

Validación de códigos: 2-3 segundos en condiciones óptimas

Generación de reportes: 5-10 minutos para conjuntos grandes de datos

**Disponibilidad:**

No incluye soporte 24/7 en la versión inicial

1. **Supuestos**

**8.1 Supuestos Técnicos**

Infraestructura Existente:

* La universidad cuenta con conexión WiFi estable en todas las áreas de acceso
* Los dispositivos móviles de guardias tienen capacidad para instalar y ejecutar la aplicación

Adopción Tecnológica:

* El 90% de los estudiantes posee smartphones compatibles
* Los usuarios estarán dispuestos a instalar y utilizar la aplicación móvil

Rendimiento:

* Firebase mantendrá sus niveles de servicio actuales (99.9% uptime)
* Los códigos de barras tendrán una tasa de lectura exitosa >95%

**8.2 Supuestos Operativos**

Procesos Institucionales:

* La oficina de registro mantendrá actualizada la base de datos de estudiantes
* Los guardias de seguridad recibirán capacitación adecuada

Comportamiento de Usuarios:

* Los estudiantes portarán sus carnets físicos como respaldo
* No habrá intentos masivos de falsificación de códigos

**8.3 Supuestos Organizacionales**

Apoyo Institucional:

* La administración universitaria apoyará la implementación
* Se asignará personal para la gestión inicial del sistema

Recursos Humanos:

* Habrá un administrador del sistema designado
* El equipo de TI brindará soporte básico

**8.4 Supuestos de Segurid**ad

Protección de Datos:

* No habrá requerimientos de integración con otros sistemas sensibles
* La información personal estará protegida por políticas institucionales

Contingencias:

* Los fallos técnicos no excederán 4 horas continuas
* Existirá un protocolo manual de respaldo para emergencias

**8.5 Supuestos Económicos**

Costos Operativos:

* Firebase permanecerá en su plan gratuito durante el primer año
* No se requerirá hardware adicional significativo

Mantenimiento:

* Las actualizaciones menores no requerirán presupuesto adicional
* El personal existente podrá manejar el soporte básico

1. **Resultados Esperados**

**1. Optimización del proceso de ingreso**

Reducción del tiempo de validación de identidad a menos de 5 segundos por estudiante, eliminando colas y demoras en los puntos de acceso.

Disminución del 90% en registros manuales, gracias a la validación digital mediante códigos QR dinámicos.

**2. Fortalecimiento de la seguridad institucional**

Eliminación de suplantaciones de identidad mediante códigos QR únicos y renovables semestralmente.

Registro automatizado del 100% de los accesos en una base de datos centralizada, con detalles de hora, fecha y ubicación.

**3. Funcionalidades técnicas implementadas**

Aplicativo móvil operativo en Android 8.0+ e iOS 12+, integrado con Firebase para gestión de usuarios, escaneo de códigos QR y notificaciones en tiempo real.

Panel administrativo web con capacidad para generar reportes de acceso históricos, gestionar roles (estudiante, seguridad, administrador) y bloquear usuarios por sanciones o matrículas vencidas.

**4. Mejora en la toma de decisiones**

Acceso a datos en tiempo real para el personal de seguridad y administrativo, permitiendo el control de aforo y la respuesta rápida en emergencias.

Generación automática de métricas (p. ej., horarios pico de acceso, zonas más transitadas) para optimizar la distribución de recursos humanos y físicos.

**5. Adopción y satisfacción de la comunidad universitaria**

Cobertura inicial para 500 usuarios simultáneos, con posibilidad de escalar a 10,000+ estudiantes mediante actualizaciones en servidores.

Encuestas de satisfacción que reflejen una mejora del 80% en la percepción de seguridad y eficiencia en los accesos.

**6. Sostenibilidad operativa y reducción de costos**

Eliminación del 95% del uso de papel en registros manuales, alineándose con políticas institucionales de sostenibilidad.

Reducción del 70% en tiempo invertido por el personal de seguridad en validaciones, permitiéndoles enfocarse en labores prioritarias.

**7. Preparación para futuras integraciones**

Arquitectura escalable que permitirá incorporar funcionalidades adicionales, como control de asistencia a clases, acceso a laboratorios o integración con sistemas biométricos.

Base técnica para implementar módulos de visitantes externos, previa autorización administrativa, en una segunda fase.

**8. Cumplimiento normativo y ético**

Almacenamiento seguro de datos bajo estándares de protección (Ley de Protección de Datos), con purga automática del historial después de 6 meses.

Operatividad dentro de las restricciones técnicas definidas (límites de Firebase, compatibilidad con dispositivos básicos y conectividad 3G).

1. **Metodología de implementación**

La metodología para la implementación del Sistema de Control de Acceso en la universidad se basará en un enfoque **iterativo e incremental**, permitiendo desarrollar el sistema en fases, obtener retroalimentación continua y ajustar el desarrollo según las necesidades reales de los usuarios.

1. **Levantamiento y Análisis de Requisitos**

* Se recopilarán los requerimientos funcionales y no funcionales mediante entrevistas, encuestas y observación directa con usuarios clave (administradores, guardias y estudiantes).
* Se documentaron los procesos actuales para identificar mejoras y establecer los objetivos del sistema.

1. **Diseño del Sistema**

* Se diseñará la arquitectura del sistema, diagramas de casos de uso, modelos de datos y la interfaz de usuario.
* Se validará el diseño con los interesados para asegurar que cumple con los objetivos.

1. **Desarrollo Iterativo**

* El desarrollo se realizará en ciclos cortos (sprints), donde se implementarán funcionalidades específicas.
* Cada ciclo finalizará con una revisión y pruebas para asegurar la calidad y funcionalidad entregada.

1. **Pruebas y Validación**

* Se realizarán pruebas unitarias, de integración y de aceptación por parte de los usuarios para detectar y corregir errores.
* Se implementarán ajustes basados en la retroalimentación recibida.

1. **Capacitación y Documentación**

* Se capacitará al personal administrativo y de seguridad para el uso efectivo del sistema.
* Se entregarán manuales y documentación técnica para soporte y mantenimiento.

1. **Implementación y Monitoreo**

* El sistema será desplegado en el entorno real de la universidad.
* Se monitoreará su funcionamiento para garantizar la estabilidad y efectividad, realizando ajustes si es necesario.

1. **Actores claves**

| **Actor** | **Rol** |
| --- | --- |
| Jefe de Seguridad (Administrador General) | Coordinador del sistema, validador de reportes e incidencias |
| Guardias de seguridad | Usuarios del aplicativo para registrar accesos |
| Oficina de Sistemas | Encargados del soporte técnico y mantenimiento del sistema |
| Área Administrativa / Rectorado | Supervisores del cumplimiento del proyecto |
| Estudiantes y Personal | Usuarios indirectos que interactúan con el sistema a través del escaneo de carnet |

1. **Papel y responsabilidad personal**

Como miembro del equipo desarrollador (y posiblemente líder del proyecto), tu rol implica:

* **Levantamiento de información:** Realizar entrevistas, encuestas o análisis de campo para entender los procesos actuales.
* **Diseño del sistema:** Participar activamente en la elaboración de la arquitectura funcional y la interfaz del aplicativo.
* **Desarrollo técnico:** Programar el aplicativo móvil, gestionar la base de datos y probar su funcionamiento.
* **Capacitación:** Preparar material de entrenamiento para los guardias y asistir a sesiones prácticas.
* **Monitoreo:** Recoger feedback y realizar mejoras en base a los informes generados por el sistema.

1. **Plan de monitoreo y evaluación**

**Plan de Monitoreo y Evaluación del Proyecto**

El presente plan de monitoreo y evaluación tiene como finalidad garantizar el correcto funcionamiento, mejora continua y sostenibilidad del Sistema de Control de Acceso Universitario mediante un aplicativo móvil. Este plan será liderado por el Administrador General (Jefe de Seguridad) y ejecutado con apoyo de los usuarios operativos (guardias).

**1. Objetivos del Monitoreo y Evaluación**

* Supervisar el uso correcto del aplicativo por parte del personal de seguridad.
* Verificar la eficiencia y precisión del sistema en tiempo real.
* Detectar errores, cuellos de botella o inconsistencias en el proceso de validación de acceso.
* Recoger feedback para mejoras futuras.

| **Indicador** | **Descripción** | **Frecuencia** | **Responsable** |
| --- | --- | --- | --- |
| Porcentaje de accesos validados correctamente | Mide cuántos accesos fueron escaneados y registrados exitosamente | Semanal | Administrador General |
| Tiempo promedio de validación por persona | Mide la eficiencia del proceso de validación por parte del guardia | Diario | Guardia |
| Incidencias reportadas | Número de fallas técnicas o errores reportados por los guardias | Semanal | Administrador General |
| Satisfacción del usuario operativo | Encuesta breve sobre usabilidad y efectividad del sistema | Mensual | Administrador General |
| Sincronización de datos sin errores | Mide si todos los registros se almacenan correctamente sin pérdidas | Semanal | Soporte Técnico / Administrador General |

1. **Cronograma del proyecto**

| **CRONOGRAMA** | |
| --- | --- |
| **Evento** | Fecha programada |
| 1. **Inicio** | Martes 04 de marzo |
| 1. **Elaboración** | Del 05 de marzo al 15 de Mayo |
| 1. **Construcción** | Del 15 de Mayo al 28 de Junio |
| 1. **Cierre** | 29 de Junio |
| 1. **Mantenimiento** | Del 30 de Junio en adelante |

1. **Hitos de entregable**

**Levantamiento de Requisitos**

* Documento con análisis detallado de necesidades, usuarios y requerimientos funcionales y no funcionales.

**Diseño del Sistema**

* Diagramas arquitectónicos (como el Diagrama 4+1).
* Diseño de base de datos y modelo de datos.
* Diseño de interfaces y flujo de usuario.

**Desarrollo del Prototipo Inicial**

* Versión básica del aplicativo móvil con funciones principales (registro y validación de accesos).

**Implementación del Sistema Completo**

* Desarrollo de todas las funcionalidades del sistema.
* Integración con hardware (lector de carnet, sensores, etc.).

**Pruebas y Validación**

* Resultados de pruebas funcionales, pruebas de integración y pruebas de usuario.
* Corrección de errores detectados.

**Capacitación y Manuales**

* Manuales de usuario y administrador.
* Capacitación al personal de seguridad y administración.

**Implementación en Producción**

* Despliegue del sistema en el entorno real de la universidad.
* Puesta en marcha y monitoreo inicial.

**RESUMEN EJECUTIVO**

| **Nombre del Proyecto propuesto**:  *Proyecto AccessGuard - Sistema de control de acceso a las instalaciones físicas de la UPT aplicando tecnología de respuesta de validación por voz, UPT y 2025* | |
| --- | --- |
| **Propósito del Proyecto y Resultados esperados:**  El propósito del proyecto es El propósito del proyecto es diseñar e implementar un sistema móvil de control de acceso para la universidad, que permita al personal de seguridad verificar la identidad de estudiantes, docentes y personal administrativo mediante el escaneo de códigos QR o el registro manual en caso de olvido del carnet universitario. Esta solución busca mejorar la seguridad, optimizar el tiempo de ingreso y fortalecer la trazabilidad de las entradas y salidas en las instalaciones, eliminando los procesos manuales actuales que son propensos a errores y demoras. El sistema será operado por los guardias y supervisado por el jefe de seguridad como administrador general.  Los resultados esperados son:   * *Implementación exitosa de un sistema móvil que permita el control eficiente y seguro del acceso a las instalaciones universitarias.* * *Reducción significativa de errores y retrasos en el ingreso de estudiantes y personal por el uso del sistema digitalizado.* * *Mejora en la trazabilidad y registro de entradas y salidas, facilitando la supervisión y auditoría por parte del jefe de seguridad.* * *Aumento en la satisfacción del personal de seguridad y usuarios finales gracias a la simplificación del proceso de verificación.* * *Centralización de la información de acceso en una base de datos segura, accesible solo para el personal autorizado.* * *Disminución del uso de registros manuales y papeleo, contribuyendo a un proceso más ecológico y eficiente.* | |
| **Población Objetivo:**  La población objetivo del sistema de control de acceso está conformada principalmente por los estudiantes de la Universidad Privada de Tacna (UPT), quienes requieren un acceso seguro y eficiente a las instalaciones universitarias. Además, incluye al personal administrativo, docentes y personal de seguridad, quienes participan en la gestión y supervisión del acceso a las áreas restringidas de la universidad. El sistema está diseñado para facilitar el control, registro y autorización de ingreso, mejorando la seguridad y organización dentro del campus. | |
| **Monto de Inversión (En Soles):**  ***S/.* 22,223.00** | **Duración del Proyecto (En Meses):**  ***3 meses*** |