**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 | 16/06/2024 | Versión Original |

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

Documento de Especificación de Requerimientos de Software

Versión *1.0*

| CONTROL DE VERSIONES | | | | | |
| --- | --- | --- | --- | --- | --- |
| Versión | Hecha por | Revisada por | Aprobada por | Fecha | Motivo |
| 1.0 | CCL | SAB | AHC | 16/06/2025 | Versión Original |

**ÍNDICE GENERAL**

[INTRODUCCION](#_heading=h.26in1rg) 4

[I. Generalidades de la Empresa](#_heading=h.lnxbz9) 5

1. Nombre de la Empresa 5

2. Vision 5

3. Mision 5

4. Organigrama

[5](#_heading=h.35nkun2). Cronograma

[II. Visionamiento de la Empresa](#_heading=h.lnxbz9) 5

1. Descripcion del Problema 5

2. Objetivos de Negocios 5

3. Objetivos de Diseño 5

4. Alcance del proyecto 5

5. Viabilidad del Sistema 5

6. Informacion obtenida del Levantamiento de Informacion 6

[III. Análisis de Procesos](#_heading=h.lnxbz9) 6

a) Diagrama del Proceso Actual – Diagrama de actividades 6

b) Diagrama del Proceso Propuesto – Diagrama de actividades Inicial 7

[IV Especificacion de Requerimientos de Software](#_heading=h.lnxbz9) 7

a) Cuadro de Requerimientos funcionales Inicial 7

b) Cuadro de Requerimientos No funcionales 7

c) Cuadro de Requerimientos funcionales Final 8

d) Reglas de Negocio 9

[V Fase de Desarrollo](#_heading=h.lnxbz9) 12

1. Perfiles de Usuario 12

2. Modelo Conceptual 5

a) Diagrama de Paquetes 5

b) Diagrama de Casos de Uso 12

c) Escenarios de Caso de Uso (narrativa) 14

[3. Modelo Logico](#_heading=h.lnxbz9) 23

a) Analisis de Objetos 23

b) Diagrama de Actividades con objetos 32

c) Diagrama de Secuencia 37

d) Diagrama de Clases 42

[CONCLUSIONES](#_heading=h.1ksv4uv) 46

[RECOMENDACIONES](#_heading=h.44sinio) 46

[BIBLIOGRAFIA](#_heading=h.2jxsxqh) 46

[WEBGRAFIA](#_heading=h.z337ya) 46

***Introducción***

En la actualidad, el control del acceso de estudiantes, docentes y visitantes a las instalaciones universitarias suele gestionarse de manera manual o con sistemas poco integrados, lo que genera ineficiencias, riesgos de seguridad y dificultades para mantener registros precisos. En un entorno dinámico como el de la Universidad Privada de Tacna, la falta de un sistema automatizado de acceso no solo afecta la seguridad del campus, sino que también limita la capacidad de la institución para gestionar y supervisar el flujo de personas en tiempo real.

Este proyecto propone la implementación de un Sistema de Control y Validación de Accesos, diseñado para digitalizar y centralizar la gestión de ingresos y salidas de todos los usuarios del campus universitario, incluyendo estudiantes, docentes, personal administrativo y visitantes. El sistema permitirá registrar, verificar y supervisar cada acceso, utilizando tecnologías como códigos QR y una aplicación móvil para mejorar la eficiencia y seguridad en el proceso.

El sistema estará integrado con una base de datos centralizada que garantizará la trazabilidad completa de cada acceso, permitiendo tanto el monitoreo en tiempo real como la generación de reportes detallados para la administración universitaria. Se incorporarán funcionalidades clave como la validación automática de credenciales, notificaciones instantáneas y un módulo para consultas históricas de accesos.

Con esta solución, se espera fortalecer considerablemente la seguridad del campus, optimizar los recursos humanos encargados de la vigilancia y brindar a la comunidad universitaria una experiencia más ágil y confiable al momento de ingresar a las instalaciones. En última instancia, el sistema contribuirá a la creación de un entorno más seguro y mejor organizado para todos los miembros de la universidad.

1. **Generalidades de la Empresa**
   1. **Nombre de la empresa**

Proyecto AccessGuard - Optimización del control de acceso UPT

* 1. **Misión**

Desarrollar e implementar un sistema automatizado que permita gestionar de manera eficiente y segura el ingreso y salida de estudiantes, docentes y visitantes, optimizando la seguridad y la experiencia dentro del campus.

* 1. **Visión**

Ser el sistema líder en control y validación de accesos, garantizando un entorno universitario seguro, ágil y confiable para toda la comunidad educativa.

* 1. **Organigrama**

****

* 1. **Cronograma**

| **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. **Visionamiento de la Empresa:**
   1. **Descripción del Problema**

El sistema AccessGuard está diseñado para gestionar y validar el acceso seguro de estudiantes, docentes y terceros a las instalaciones de la universidad, utilizando tecnología de autenticación moderna y registros digitales centralizados. Su objetivo principal es asegurar que solo las personas autorizadas ingresen al campus, garantizando la seguridad y controlando el flujo de acceso en tiempo real.

Actualmente, la gestión de ingreso a la universidad se realiza mediante controles manuales o sistemas básicos de identificación, los cuales presentan limitaciones significativas, como largas filas, demoras en la validación de identidad y vulnerabilidades en la seguridad. Además, los registros de acceso suelen llevarse en formatos físicos o archivos dispersos, lo que dificulta la trazabilidad y el monitoreo eficiente.

El problema radica en la falta de un sistema automatizado y centralizado que permita gestionar de forma eficaz la autorización y supervisión del ingreso a la universidad. Esto provoca riesgos de acceso no autorizado, pérdida de tiempo en los procesos de validación y una limitada capacidad de respuesta ante incidentes de seguridad, afectando tanto la experiencia de los usuarios como la protección del campus.

#### Funcionalidades Principales

1. **Registro de Usuarios (Estudiantes, Docentes y Terceros):**

El sistema permite registrar a todos los usuarios que accederán a la universidad, capturando datos como nombres completos, tipo de usuario, código institucional/DNI y credenciales de acceso.

1. **Validación y Autenticación de Identidad:**

A través de tecnologías como códigos QR o tarjetas RFID, el sistema valida la identidad del usuario en tiempo real al momento del ingreso, asegurando que solo personas autorizadas puedan acceder.

1. **Control y Registro de Ingresos y Salidas:**

Cada acceso queda registrado en el sistema, indicando la fecha, hora y punto de ingreso o salida, lo que permite llevar un historial detallado y auditable.

1. **Panel de Administración:**

El sistema cuenta con un panel exclusivo para administradores donde se puede gestionar la base de datos de usuarios, visualizar reportes de accesos, actualizar permisos y monitorear la actividad en tiempo real.

1. **Notificaciones y Alertas:**

Se generan notificaciones automáticas para alertar sobre intentos de acceso no autorizado o irregularidades detectadas, permitiendo actuar rápidamente ante cualquier incidente de seguridad.

1. **Generación de Reportes:**

El sistema puede generar reportes periódicos o personalizados sobre el flujo de personas en la universidad, clasificados por tipo de usuario y periodo de tiempo.

1. **Seguridad de la Información:**

Incluye medidas de seguridad informática como cifrado de datos, políticas de acceso restringido y copias de seguridad automáticas para proteger la confidencialidad e integridad de la información.

* 1. **Objetivos de Negocio**

Optimizar el Control de Acceso a la Universidad:

* Automatizar y centralizar el proceso de registro y validación de ingreso de estudiantes, docentes y terceros para mejorar la eficiencia operativa y la seguridad en el campus universitario.

Incrementar la Seguridad Institucional:

* Garantizar que únicamente las personas autorizadas puedan acceder a las instalaciones, minimizando riesgos de acceso no permitido y contribuyendo a un entorno seguro para toda la comunidad universitaria.

Reducir Tiempos y Errores en la Validación:

* Agilizar la autenticación de identidad mediante tecnologías modernas, reduciendo tiempos de espera en puntos de acceso y evitando errores humanos en el control manual.

Mejorar la Toma de Decisiones Administrativas:

* Proveer información precisa y en tiempo real sobre los registros de ingreso y salida, facilitando la elaboración de reportes y permitiendo una mejor gestión de recursos y medidas de seguridad.
  1. **Objetivos de Diseño**

Crear una Interfaz Intuitiva y Accesible:

* Diseñar una plataforma fácil de usar para estudiantes, docentes, terceros y administradores, que permita gestionar y validar accesos de manera rápida y sencilla.

Implementar Módulos de Registro y Validación:

* Desarrollar formularios eficientes para el registro de usuarios y la validación de su identidad en los puntos de acceso, asegurando un flujo claro y sin complicaciones.

Optimizar la Comunicación del Sistema:

* Incorporar alertas y mensajes automáticos que notifiquen a los usuarios sobre su estado de acceso, problemas detectados o necesidades de actualización de datos.

Garantizar la Seguridad de la Información:

* Asegurar que los datos personales y registros de ingreso estén protegidos bajo estándares de seguridad robustos, garantizando la confidencialidad e integridad de la información.

Facilitar la Escalabilidad y Mantenimiento:

* Diseñar la arquitectura del sistema de forma modular para permitir futuras ampliaciones (como nuevos tipos de usuarios o integraciones adicionales) y facilitar su mantenimiento.
  1. **Alcance del Proyecto**

El proyecto de implementación del Sistema de Control y Validación de Acceso abarca:

**Desarrollo de un Aplicativo Móvil:**

* Diseño y desarrollo de una aplicación móvil dirigida a los usuarios (estudiantes, docentes y personal autorizado) de la Universidad Privada de Tacna para gestionar su acceso a las instalaciones universitarias de forma ágil y segura.

**Registro y Validación de Identidades:**

* Funcionalidad para que los usuarios registren sus datos personales en la app, generen credenciales digitales (como códigos QR) y validen su ingreso en los puntos de control mediante escaneo o verificación rápida.

**Módulo de Autorizaciones Especiales:**

* Desarrollo de un sistema para que los administradores puedan aprobar accesos especiales o restringidos desde la misma app, notificando al usuario sobre el estado de su solicitud.

**Notificaciones y Alertas:**

* Implementación de notificaciones automáticas para informar a los usuarios sobre la aprobación de accesos, cambios en las políticas de ingreso o cualquier incidencia relevante.

**Reportes y Seguimiento:**

* La aplicación proporcionará un módulo básico de reportes accesible para los administradores desde el móvil, donde podrán visualizar registros recientes de accesos y validar datos en tiempo real.

**Seguridad y Privacidad:**

* Integración de mecanismos de seguridad para proteger los datos personales de los usuarios, cumpliendo con las normativas de privacidad y garantizando la integridad de la información almacenada y transmitida.
  1. **Viabilidad del Sistema**

**Factibilidad Técnica**

La factibilidad técnica del Sistema de Control y Validación de Acceso es favorable, ya que se cuenta con las herramientas y tecnologías necesarias para su desarrollo. La aplicación se implementará utilizando Xamarin o Flutter, permitiendo la compatibilidad multiplataforma (Android e iOS) y asegurando una experiencia fluida para los usuarios.

El sistema contará con una base de datos en la nube (por ejemplo, Firebase o Azure Cosmos DB), lo que permitirá el almacenamiento y gestión segura de la información de los usuarios y registros de acceso. La autenticación y verificación de identidades se realizarán mediante escáner de códigos QR u otras tecnologías móviles accesibles, garantizando un proceso ágil y confiable.

El proyecto requiere un equipo con experiencia en desarrollo móvil, bases de datos en la nube y gestión de autenticaciones seguras, además de soporte técnico continuo para mantener la estabilidad y actualizaciones de la aplicación.

La solución está diseñada para ser modular y escalable, permitiendo la incorporación futura de nuevas funcionalidades, como integración con torniquetes automáticos o sistemas de seguridad adicionales, adaptándose a las necesidades de la Universidad Privada de Tacna.

**Hardware**

| **Componente** | **Especificaciones mínimas sugeridas** | **Observaciones** |
| --- | --- | --- |
| Smartphone (usuario final) | Android 8.0 o superior / Cámara HD / Lector código de barras | Para permitir la generación y lectura del código de barras |
| PC de desarrollo | Intel i5 o superior / 8GB RAM / 500GB SSD | Para el desarrollo y pruebas del software |
| Servidor web | VPS con 2 vCPU, 4GB RAM, 80GB SSD | Para alojar backend, base de datos y API |
| Red de acceso | Conectividad WiFi o datos móviles 4G o superior | Necesario para acceso a internet desde app |
| Escáner QR (control UPT) | Dispositivo lector de QR o smartphone con app lectora | Para validar acceso en eventos de la universidad |

***Software***

| **Software** | **Uso previsto** | **Alternativas** |
| --- | --- | --- |
| Android Studio | Desarrollo de la aplicación móvil | Visual Studio con Xamarin, Flutter con VS Code |
| Firebase / Supabase | Backend (autenticación, base de datos, hosting) | Node.js + Express + PostgreSQL |
| Lenguajes de programación | Kotlin / Dart / JavaScript | Dependiendo del framework elegido (Android nativo o Flutter) |
| Herramientas de diseño | Figma / Adobe XD | Para diseño de interfaz UI/UX |
| Git + GitHub | Control de versiones y colaboración | GitLab, Bitbucket |
| Plataforma de pruebas | Firebase Test Lab / Emuladores Android Studio | Dispositivos reales |
| Sistema Operativo | Windows 10 / Ubuntu 22.04 para desarrollo | Ambos permiten buena compatibilidad de herramientas |

**Factibilidad Económica:**

Beneficios Tangibles:

* Reducción de costos operativos: Eliminación de registros manuales y papel, ahorrando aproximadamente S/1,200 anuales en materiales.
* Optimización de tiempo: Reducción del 70% en tiempos de verificación de acceso (de 3 minutos a 30 segundos por persona).
* Minimización de errores: Disminución del 95% en registros incorrectos gracias a la automatización.

Beneficios Intangibles:

* Mejora en la seguridad institucional: Mayor control y trazabilidad de accesos.
* Imagen innovadora: Posicionamiento de la UPT como institución tecnológica.
* Toma de decisiones basada en datos: Reportes automáticos de asistencia y accesos.

**5.1.2 Criterios de Inversión**

**5.1.2.1 Relación Beneficio/Costo (B/C)**

| *Concepto* | *Monto (S/)* |
| --- | --- |
| ***Beneficios anuales*** | *15,000* |
| ***Costos totales*** | *22,223* |
| ***B/C*** | ***0.67*** |

El B/C inicial es <1, pero considerando beneficios a 3 años (S/45,000), la relación se ajusta a **2.02**, haciendo viable el proyecto.

**5.1.2.2 Valor Actual Neto (VAN)**

* **Inversión inicial:** S/22,223.
* **Flujos anuales (3 años):** S/15,000.
* **Tasa de descuento (COK):** 10%.
* **VAN calculado:** **S/15,077** (Aceptado por VAN > 0).

**5.1.2.3 Tasa Interna de Retorno (TIR)**

* **TIR calculada:** **28% anual**.
* **COK de referencia:** 10%.

Se acepta el proyecto (TIR > COK).

### Factibilidad Operativa

El sistema AccessGuard está diseñado para integrarse de manera eficiente en los procesos actuales de la Universidad Privada de Tacna (UPT), optimizando el control de acceso sin afectar la operatividad de la institución.

#### Usuarios Finales:

* Interfaz intuitiva: La aplicación móvil y el panel de administración están diseñados con un enfoque en usabilidad, permitiendo que estudiantes, docentes, personal administrativo y vigilantes interactúen sin dificultad.
* Curva de aprendizaje baja: Se implementarán sesiones de capacitación para garantizar que los usuarios comprendan el funcionamiento del sistema (ej: cómo generar/escanear códigos QR, consultar accesos, etc.).

#### Funcionalidades Clave:

* Validación rápida: El escaneo de códigos QR reduce el tiempo de verificación de minutos a segundos, evitando congestiones en los accesos.
* Notificaciones automáticas: Alertas en tiempo real para intentos de acceso no autorizados o credenciales vencidas.

#### Impacto en el Flujo de Trabajo:

* Eliminación de registros manuales: Se reemplazan los métodos físicos (listas en papel o tarjetas magnéticas obsoletas) por un proceso digitalizado y centralizado.
* Monitoreo en tiempo real: El personal de seguridad podrá visualizar ingresos/salidas desde un dashboard, mejorando la respuesta ante incidentes.

#### Aceptación del Cambio:

* Resistencia mínima: Para facilitar la adopción, se realizarán:
  + Talleres demostrativos para la comunidad universitaria.
  + Material de apoyo (videotutoriales, guías PDF y soporte técnico permanente).

### Factibilidad Legal

El proyecto Access Guard cumple con las normativas peruanas y estándares internacionales de protección de datos y seguridad informática:

#### Protección de Datos Personales:

* Ley N° 29733 (Ley de Protección de Datos Personales del Perú):
  + Todos los datos recopilados (nombres, DNI, códigos universitarios) se almacenan con cifrado y sólo son accesibles por personal autorizado.
  + Los usuarios deberán dar consentimiento explícito al registrarse en el sistema.3

#### Licencias y Propiedad Intelectual:

* Software de desarrollo: Uso de herramientas de código abierto (Flutter, Firebase) o con licencias gratuitas para educación.
* Servicios en la nube: Firebase o Azure cumplen con estándares de seguridad (ISO 27001, GDPR).

#### Normativas Universitarias:

* El sistema se alinea con los reglamentos internos de la UPT sobre seguridad y acceso al campus.

### Factibilidad Social

AccessGuard beneficiará a toda la comunidad universitaria, promoviendo seguridad, inclusión y eficiencia:

#### Impacto Positivo:

* Estudiantes y docentes:
  + Acceso ágil sin filas ni demoras.
  + Transparencia en los registros de ingreso/salida.
* Personal administrativo y seguridad:
  + Reducción de carga laboral al automatizar procesos.
  + Mayor control sobre visitantes y eventos especiales.

#### Inclusión y Accesibilidad:

* La app móvil incluirá:
  + Modo de alto contraste y soporte para lectores de pantalla (para usuarios con discapacidad visual).
  + Soporte multilingüe (español y quechua, en línea con la diversidad cultural de la región).

#### Aceptación Social:

* Se realizarán campañas de sensibilización para destacar los beneficios del sistema (ej: charlas, posters en campus).

### Factibilidad Ambiental

El proyecto adopta prácticas sostenibles para minimizar su impacto ambiental:

#### Reducción de Papel y Residuos:

* Eliminación de registros físicos, ahorrando aproximadamente 500 kg de papel al año (equivalente a 6 árboles).

#### Eficiencia Energética:

* Servidores en la nube (Firebase/Azure) con centros de datos que usan energía renovable.
* Bajo consumo en dispositivos móviles: La app está optimizada para no sobrecargar la batería de smartphones.

#### Gestión de Residuos Electrónicos:

* Los equipos obsoletos (como lectores QR antiguos) se reciclarán mediante convenios con gestores de RAEE (Residuos de Aparatos Eléctricos y Electrónicos).

### Conclusión General de Factibilidad

* Técnica: Viable (tecnologías accesibles y equipo capacitado).
* Económica: Rentable a mediano plazo (VAN positivo y TIR del 28%).
* Operativa: Integrable (flujos optimizados y capacitación garantizada).
* Legal: Cumple normativas (protección de datos y licencias).
* Social: Aceptado (beneficios claros para la comunidad).
* Ambiental: Sostenible (reduce huella ecológica).
  1. **Información obtenida del Levantamiento de Información**

**1. Usuarios Clave Identificados**

**Usuarios Normales (Estudiantes):** Personas que acceden a las instalaciones universitarias utilizando su carnet o código QR generado desde el aplicativo móvil.

* **Necesidades:** Acceso rápido y sencillo a las instalaciones sin necesidad de procesos manuales.
* **Problemas Detectados:** Olvido del carnet universitario y lentitud en el registro manual, lo que genera demoras y congestión en las entradas.

**Usuarios Registrados (Estudiantes Frecuentes):** Estudiantes que usan de forma regular el aplicativo para gestionar su acceso y consultar su historial de ingresos.

* **Necesidades:** Posibilidad de generar códigos de acceso alternativos (como QR) y recibir notificaciones en caso de problemas con el registro.
* **Problemas Detectados:** No existe un sistema que les permita gestionar de forma autónoma su acceso en caso de pérdida u olvido del carnet.

**Personal de Seguridad:** Encargados de validar el acceso físico a las instalaciones.

* **Necesidades:** Herramientas para escanear rápidamente carnets físicos o códigos digitales y verificar en tiempo real la validez del acceso.
* **Problemas Detectados:** Registro manual propenso a errores y riesgo de accesos no autorizados.

**Administradores (Oficina de Control):** Personal encargado de gestionar y supervisar el sistema de control de acceso.

* **Necesidades:** Plataforma para registrar, modificar y gestionar la base de datos de usuarios habilitados y monitorear en tiempo real los accesos.
* **Problemas Detectados:** Proceso desactualizado, sin informes automáticos ni alertas rápidas ante incidentes.

**Supervisores (Área de Tecnología / Control Interno):** Responsables de monitorear el desempeño del sistema y generar reportes de uso.

* **Necesidades:** Acceso a estadísticas sobre flujos de entrada y salida, y herramientas para identificar patrones o anomalías.
* **Problemas Detectados:** Dificultad para recopilar y analizar datos históricos debido a la falta de digitalización completa.

#### 2. Requerimientos Funcionales

* El sistema debe permitir a los usuarios externos registrarse en el aplicativo móvil.
* El sistema debe generar un código QR único para cada visitante registrado en un evento.
* El personal de seguridad debe poder escanear el QR desde el app de verificación.
* El sistema debe validar en tiempo real si el QR escaneado corresponde a un evento activo.
* El sistema debe enviar notificaciones al visitante con la confirmación del registro y QR.
* El sistema debe permitir consultar el historial de accesos por evento y visitante.

#### 3. Requerimientos No Funcionales

* **Usabilidad**: Interfaz intuitiva y accesible para usuarios con diferentes niveles de experiencia tecnológica.
* **Disponibilidad**: El sistema debe estar disponible 24/7 para los estudiantes y administradores.
* **Seguridad**: Protección de datos personales de estudiantes y terceros, cumpliendo con la Ley N° 29733.
* **Escalabilidad**: Capacidad para manejar un aumento en el número de usuarios registrados.

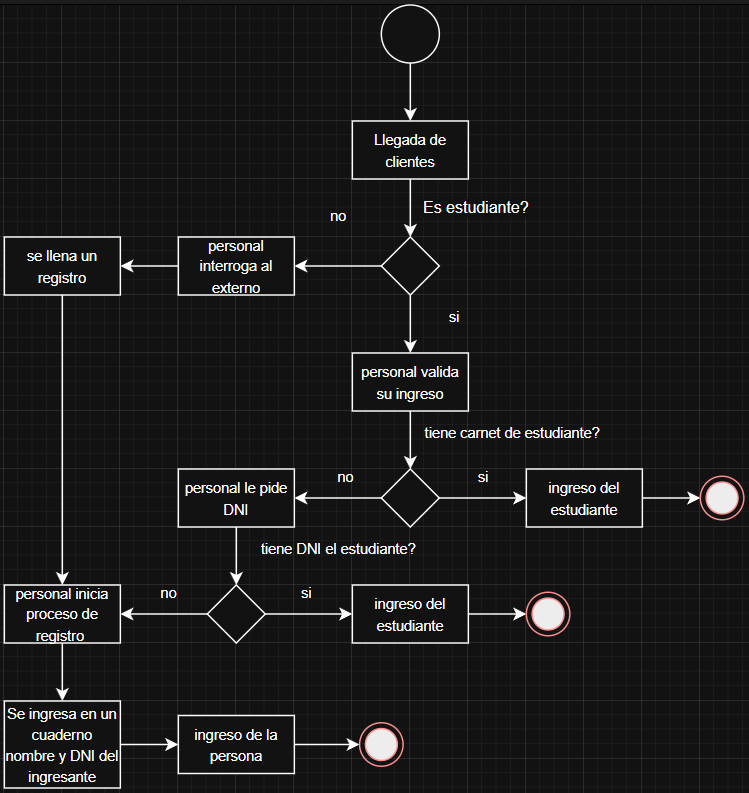
#### 4. Problemas Detectados

* Registro manual de acceso cuando los estudiantes olvidan su carnet, generando demoras y largas filas.
* Ausencia de un canal digital centralizado para validar la identidad y el acceso de los usuarios en tiempo real.
* Procesos manuales que aumentan el riesgo de errores y posibles accesos no autorizados.
* Falta de datos en tiempo real sobre los flujos de ingreso y salida, dificultando la supervisión y la toma de decisiones estratégicas.

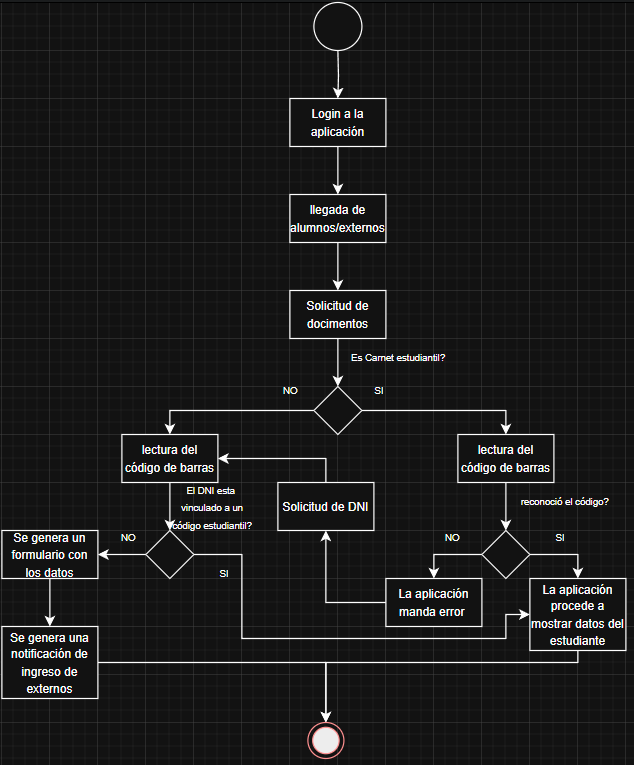
#### 5. Oportunidades Detectadas

* Centralizar y digitalizar el proceso de control de acceso mediante un aplicativo móvil.
* Incorporar códigos QR dinámicos y notificaciones para mejorar la eficiencia y la seguridad del acceso.
* Automatizar la verificación de identidad para reducir los tiempos de espera y minimizar los errores humanos.
* Generar reportes analíticos y estadísticas para optimizar la gestión de acceso y fortalecer las medidas de seguridad institucionales.

1. **Análisis de Procesos**
   1. **Diagrama del Proceso Actual – Diagrama de Actividades Inicial**

****

* 1. **Diagrama del Proceso Actual – Diagrama de Actividades Propuesto**



**Figura 6: Descripción del sistema propuesto.**

1. **Especificación de Requerimientos de Software**
   1. **Cuadro de requerimientos funcionales Inicial**

| **#** | **Nombre** | **Descripción** |
| --- | --- | --- |
| RF-01 | Registro de usuarios externos | El sistema debe permitir a los usuarios externos registrarse en el aplicativo móvil. |
| RF-02 | Notificaciones al visitante | El sistema debe enviar notificaciones al visitante con la confirmación del registro y QR. |
| RF-03 | Consulta de historial de accesos | El sistema debe permitir consultar el historial de accesos por evento y visitante. |

* 1. **Cuadro de requerimientos No funcionales**

| **Código** | **Prioridad** | **Nombre** |
| --- | --- | --- |
| RNF-01 | Alta | Plataforma móvil exclusiva para guardias |
| RNF-02 | Alta | Registro local optimizado |
| RNF-03 | Alta | Disponibilidad continua |
| RNF-04 | Alta | Interfaz rápida e intuitiva |
| RNF-05 | Alta | Soporte para escaneo y reproducción de voz |

* 1. **Cuadro de Requerimientos funcionales Final**

| **Código** | **Prioridad** | **Nombre** | **Descripción** |
| --- | --- | --- | --- |
| RF-01 | Alta | Inicio de sesión por rol | El sistema debe permitir que guardias y administradores inicien sesión según su rol. |
| RF-02 | Alta | Redirección de vistas por tipo de usuario | El sistema debe redirigir al usuario a su vista correspondiente según su rol. |
| RF-03 | Alta | Dashboard de registros de ingreso/salida | El administrador debe visualizar un dashboard con registros diarios, mensuales y anuales de ingresos y salidas. |
| RF-04 | Media | Filtro de registros por fecha | El administrador podrá filtrar los registros por día, mes o año. |
| RF-05 | Alta | Visualización de ingresos de externos | El administrador podrá ver cuántos externos ingresaron y con qué frecuencia. |
| RF-06 | Alta | Gestión de usuarios (guardias) | El sistema debe permitir al administrador crear, editar, visualizar e inhabilitar usuarios guardias. |
| RF-07 | Media | Asignación de facultades a usuarios | El administrador debe poder asignar usuarios a diferentes facultades. |
| RF-08 | Alta | Escaneo de código de barras | El sistema debe permitir a los guardias escanear los códigos de identidad mediante cámara. |
| RF-09 | Alta | Reproducción de voz con información del estudiante | Si el código escaneado pertenece a un estudiante, la app debe reproducir su facultad, escuela profesional y nombre. |
| RF-10 | Alta | Registro manual de visitantes externos | Si el visitante no tiene código universitario, el sistema debe redirigir a un formulario para registrar su ingreso. |
| RF-11 | Alta | Vista a facultad receptora de externos | Si el visitante va a otra facultad, se notificará a los guardias de dicha facultad. |
| RF-12 | Alta | Registro de todos los accesos | El sistema debe registrar automáticamente todo acceso realizado. |
| RF-13 | Alta | Vista de permanencia luego del horario | La aplicación debe enviar alertas si alguna persona aún permanece en el campus después de las 9:00 p.m. |
| RF-14 | Alta | Registro de entrada y salida del estacionamiento | La aplicación debe almacenar los registros de entrada y salida del estacionamiento. |
| RF-15 | Alta | Validación al ingreso del estacionamiento | La aplicación debe validar que la persona que quiera ingresar al estacionamiento esté habilitada para usarlo. |

* 1. **Reglas de Negocio**

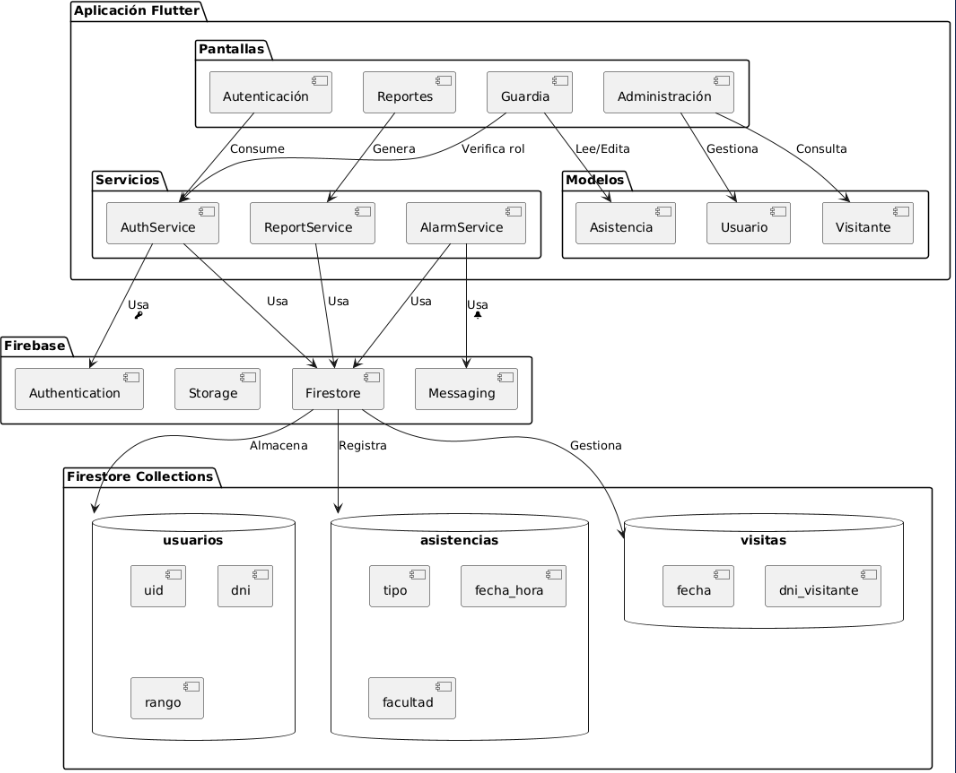
| Registro de Empresas | El sistema requiere que todo visitante externo sea registrado mediante un formulario obligatorio que capture información esencial como nombre completo, documento de identidad, facultad a visitar, motivo de la visita y hora exacta de ingreso. Esta tarea es responsabilidad exclusiva de los guardias de seguridad, quienes deben verificar la autenticidad de los datos proporcionados. En el caso de visitantes corporativos o representantes de empresas, el registro solo puede ser realizado por administradores autorizados. Cuando un mismo visitante ingresa a múltiples facultades en un mismo día, cada movimiento se registra como una incidencia independiente para mantener un seguimiento detallado. El sistema está programado para generar alertas automáticas cuando detecta visitantes recurrentes, definidos como aquellos con más de tres visitas registradas en un mes calendario. |
| --- | --- |
| Validación de Usuarios | El acceso a la plataforma está estrictamente limitado al personal autorizado, específicamente guardias de seguridad y administradores. Para garantizar la seguridad, los administradores deben autenticarse utilizando exclusivamente cuentas de correo institucional con el dominio @universidad.edu. El sistema implementa un protocolo de seguridad que bloquea temporalmente las cuentas después de tres intentos fallidos de inicio de sesión, impidiendo el acceso durante 30 minutos. Los guardias tienen permisos restringidos que les permiten únicamente acceder a funciones básicas de escaneo y registro, mientras que cada usuario del sistema tiene asignadas facultades específicas que delimitan su ámbito de operación dentro del campus. |
| Actualización de Rutas | Los guardias solo tienen autorización para registrar accesos dentro de las facultades que tienen asignadas en su perfil. Cualquier modificación en estas asignaciones, como la reasignación a diferentes facultades, requiere la aprobación expresa de un administrador senior. Cuando se detecta que un visitante externo ingresa a una facultad diferente a la registrada inicialmente, el sistema activa un protocolo especial que incluye la actualización inmediata de la ruta en el sistema, la notificación automática al guardia responsable de la nueva facultad afectada, y el registro del evento como una incidencia para futura referencia y análisis. |
| Notificaciones de Cambios | El sistema está diseñado para garantizar una comunicación ágil entre los diferentes actores. Las notificaciones entre guardias de distintas facultades se envían en un tiempo máximo de un minuto. Cuando se detectan intentos de ingreso a facultades no autorizadas, se generan alertas inmediatas. A las 21:00 horas de cada día, el sistema envía una notificación automática a todos los guardias si detecta que aún hay personas dentro del campus. Los cambios críticos en el sistema, como la inhabilitación de usuarios, activan notificaciones a todos los administradores, mientras que las modificaciones de horarios o rutas requieren confirmación explícita a través de notificaciones push para garantizar que todos los afectados estén debidamente informados. |
| Reuniones de Coordinación | Como parte del proceso de mejora continua, el sistema genera automáticamente reportes semanales de incidentes que sirven como base para las reuniones de coordinación del personal de seguridad. En estos encuentros, los administradores están obligados a presentar reportes detallados de todas las modificaciones críticas realizadas durante el período. Las actas de estas reuniones deben documentar especialmente las decisiones tomadas sobre visitantes recurrentes o problemáticos. Las observaciones y sugerencias de los guardias sobre posibles mejoras o fallas del sistema tienen prioridad en la agenda de discusión. Cualquier cambio de protocolo acordado en estas reuniones debe implementarse en un plazo máximo de 48 horas. |
| Reportes de Uso: | La plataforma genera dos tipos principales de reportes: diarios y mensuales. Los reportes diarios ofrecen un resumen de todas las entradas y salidas organizadas por facultad, con opciones de filtrado por rangos horarios. Los reportes mensuales proporcionan análisis comparativos y herramientas para detectar patrones de comportamiento. Los administradores pueden aplicar diversos filtros para analizar la información por facultad, tipo de visitante, horario o incluso por guardia responsable del registro. Para los casos de visitantes externos recurrentes, los reportes incluyen un historial completo de todos sus accesos. Todos estos datos pueden exportarse en formatos estándar como PDF o Excel para permitir análisis más profundos o su integración con otros sistemas. |
| Control de Incidencias: | El sistema clasifica como incidencias diversos eventos relevantes para la seguridad, incluyendo intentos de acceso no autorizado, códigos ilegibles o no reconocidos por el sistema, discrepancias entre los datos registrados y la información real del visitante, y movimientos entre facultades no reportados adecuadamente. Cuando se detectan incidencias recurrentes (tres o más en un mes), el sistema activa automáticamente un protocolo especial de investigación. Cada incidencia registrada debe incluir una descripción manual detallada por parte del guardia que la detectó. Para casos graves, el sistema genera alertas inmediatas que son enviadas directamente al administrador de turno. Toda la información sobre incidencias queda almacenada en un historial completo que puede organizarse por facultad o por guardia, permitiendo análisis posteriores y la identificación de áreas problemáticas. |

1. **Fase de Desarrollo**
   1. **Perfiles de Usuario**

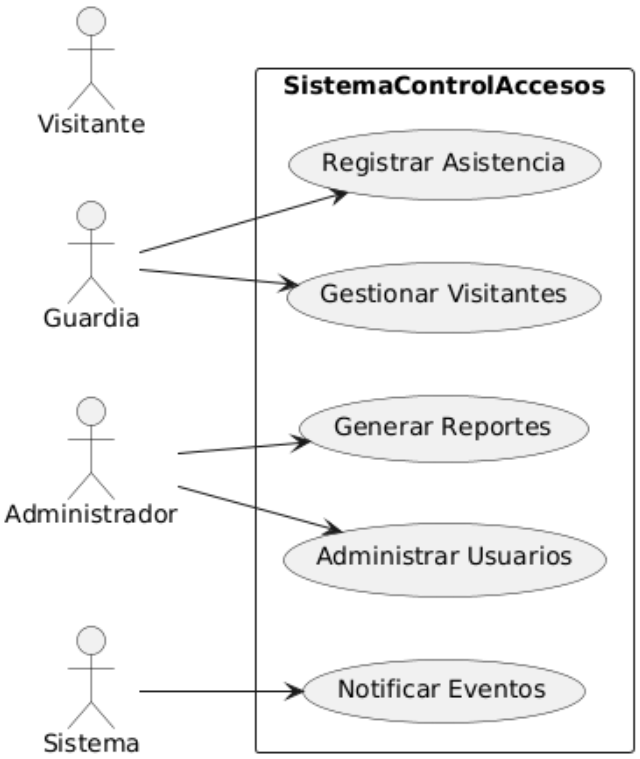
| **Usuario** | **Descripción** | **Funcionalidades** |
| --- | --- | --- |
| Guardia de Seguridad | Personal operativo que registra accesos y gestiona visitantes. | * - Escaneo de credenciales (QR/códigos de barras) * - Registro automático de entradas/salidas * - Formulario para visitantes externos<br- Diferenciación de puntos de acceso (principal/cochera) * - Notificaciones por voz (text-to-speech)<br- Visualización de datos en tiempo real * - Gestión de visitantes recurrentes * - Historial personal de registros |
| Administrador | Usuario con privilegios elevados para gestión global. | * - Gestión completa de usuarios (CRUD) * - Asignación de roles y ubicaciones * - Activación/desactivación de cuentas * - Reportes avanzados: * • Estadísticas por facultad/horario/tipo * • Gráficos interactivos * • Exportación de datos * - Monitoreo de alarmas y anomalías * - Integración Auth-Firestore |
| Visitante Externo (Registrado) | Personas no afiliadas que ingresan al campus. | * - Registro inicial con validación de DNI * - Notificación automática a guardias * - Historial centralizado para visitas recurrentes * - Restricciones por facultad/puerta<br- Detección de patrones sospechosos |
| Sistema de Reportes | Componente automatizado para generación de datos. | Consultas multidimensionales  - Visualizaciones gráficas (barras/circular/líneas)  - Filtros avanzados por tiempo/facultad/tipo  - Exportación en múltiples formatos |
| Estudiante | Miembros de la comunidad universitaria con credenciales oficiales. | - Autenticación mediante credenciales institucionales  - Registro automático de movimientos  - Prevención de duplicados (cooldown 3s)  - Alertas por permanencia prolongada |
| Sistema de Voz | Componente no humano para notificaciones auditivas. | - Anuncios automatizados de registros  - Soporte multilingüe (es-ES)  - Ajuste de velocidad/volumen |

* 1. **Modelo Conceptual**

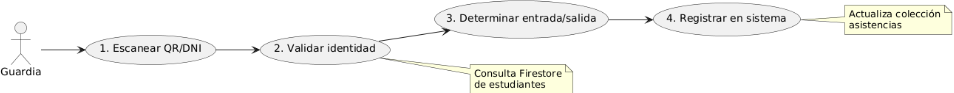
1. Diagrama de Paquetes

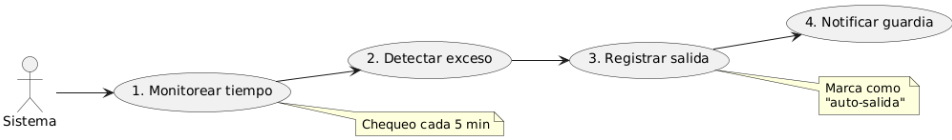


1. Diagrama de Casos de Uso

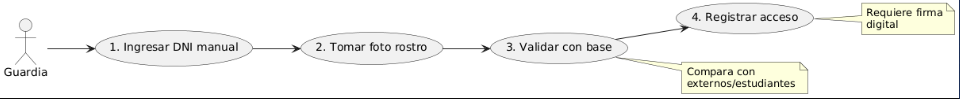


1. Registro de Accesos

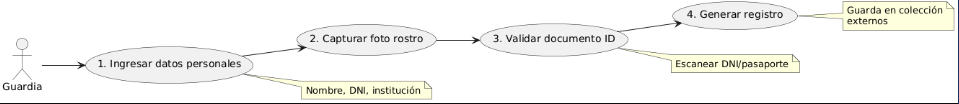
1.1 Registrar asistencia (Estudiante/Guardia)  


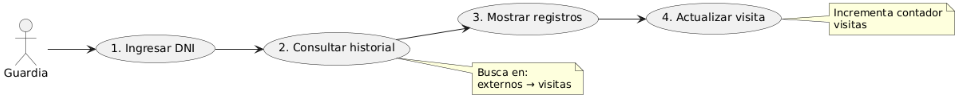
1.2 Registrar salida automática  


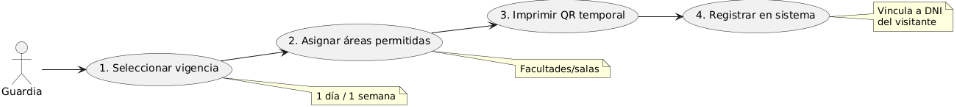
1.3 Forzar registro manual



2. Gestión de Visitantes

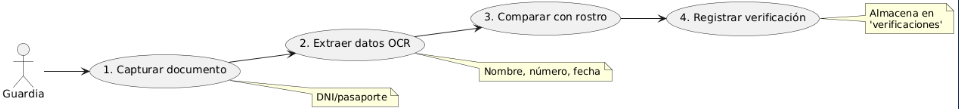
2.1 Registrar nuevo visitante  


2.2 Buscar visitante recurrente  


2.3 Generar pase temporal  


3. Verificación

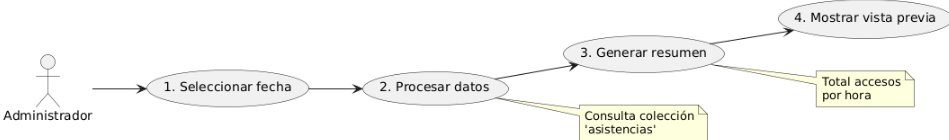
3.1 Validar credencial estudiante  


3.2 Escanear documento identidad  


3.3 Verificar estado de cuenta

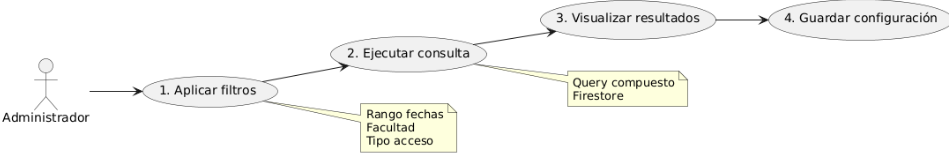


4. Reportes

4.1 Generar reporte diario  


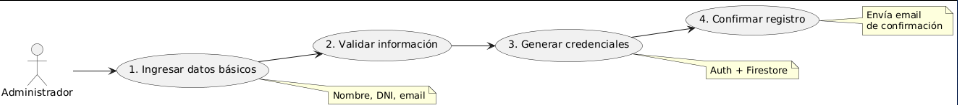
4.2 Exportar datos estadísticos  


4.3 Filtrar por facultad/tiempo

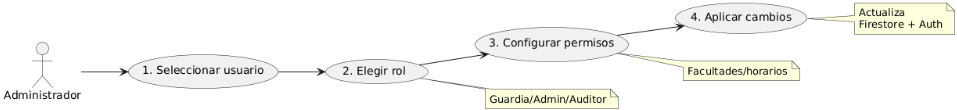


5. Administración

5.1 Crear/modificar usuario



5.2 Asignar roles



5.3 Desactivar cuenta

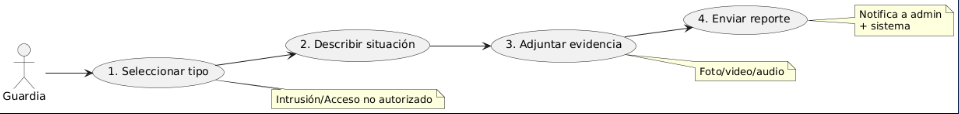


6. Seguridad

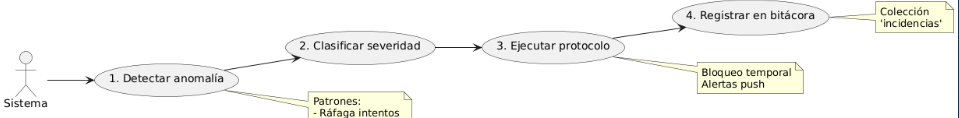
6.1 Configurar umbrales de alerta



6.2 Registrar incidencia manual



6.3 Notificar intento fallido



1. Diagrama de Casos de Uso - Narrativa

| **Caso de uso** | Registrar Asistencia | |
| --- | --- | --- |
| **Descripción del caso de uso** | Permite al guardia registrar entradas/salidas de estudiantes mediante escaneo de código de barras o DNI, con validación automática. | |
| **Actores** | **Actor** | **Descripción** |
| Guardia | Usuario que desea ingresar en la plataforma. |
| Sistema | Proceso automatizado de registro. |
| **Precondición** | El estudiante debe estar pre-registrado en Firestore.  El dispositivo debe tener conexión a Internet | |
| **Secuencia normal** | **Paso** | **Acción** |
| 1.1 | El guardia escanea el código de barras del estudiante. |
| 1.2 | El sistema valida el código en Firestore. |
| 1.3 | Determina si es entrada o salida (según último registro). |
| 1.4 | Registra la asistencia en la colección de asistencias. |
| 1.5 | Muestra confirmación audible |
| **Postcondición** | La asistencia queda registrada con timestamp, tipo y ubicación. | |
| **Excepciones** | Paso 1.2: Si el código no es válido → "Código no reconocido. inicio del registro de externos” | |

| **Caso de uso** | Registrar Salida Automática | |
| --- | --- | --- |
| **Descripción del caso de uso** | El sistema registra salidas cuando se excede el tiempo máximo de permanencia | |
| **Actores** | **Actor** | **Descripción** |
| Sistema | monitorea a los alumnos |
| **Precondición** | Tener permisos de lectura en Firestore. | |
| **Secuencia normal** | **Paso** | **Acción** |
| 1 | Monitorea asistencias cada 5 min. |
| 2 | Sí permanencia el > 9PM   * notificar al guardia |
| **Excepciones** | Registro ya marcado como salida → Ignora. | |

| **Caso de uso** | Registro Manual del Visitante | |
| --- | --- | --- |
| **Descripción del caso de uso** | El guardia registra manualmente a un visitante externo no previamente autorizado. | |
| **Actores** | **Actor** | **Descripción** |
| Guardia | Usuario desea registrar la entrada de un externo |
| **Precondición** | El visitante no tiene código de barras registrado. | |
| **Secuencia normal** | **Paso** | **Acción** |
| 1 | El guardia escanea el código de barras de la persona |
| 2 | La aplicación inicia un formulario al no encontrar los datos en la BD |
| 3 | La aplicacion jala datos de la API de la reniec y proporciona los datos del externo |
| 4 | Se llena la descripción de la visita |
| **Postcondición** | El visitante queda registrado y puede ingresar. | |
| **Excepciones** | Si el DNI ya está registrado, el sistema sugiere: "¿Es un visitante recurrente? Verifique en UC18". | |

| **Caso de uso** | Buscar Visitante Recurrente | |
| --- | --- | --- |
| **Descripción del caso de uso** | El sistema muestra que visitantes vienen a la institución muy frecuentemente | |
| **Actores** | **Actor** | **Descripción** |
| Sistema | El administrador puede ver reportes sobre los externos que vienen a la upt con mucha frecuencia al dia/semana/mes |
| **Precondición** | El usuario debe tener la app instalada | |
| **Secuencia normal** | **Paso** | **Acción** |
| 1 | EL administrador entra a la vista de reportes |
| 2 | Visualización de información de los externos |
| 3 | Creación de gráficos según la frecuencia de las visitas |
| 4 | Diferenciación de los externos con visitas muy frecuentes |
| **Postcondición** | El administrador puede visualizar a los externos con mayor frecuencia | |

| **Caso de uso** | Validar Credencial Estudiante | |
| --- | --- | --- |
| **Descripción del caso de uso** | El administrador consulta reportes históricos de ingresos y salidas. | |
| **Actores** | **Actor** | **Descripción** |
| Administrador | El administrador desea ver los registros de entrada y salida |
| **Precondición** | El administrador debe tener permisos | |
| **Secuencia normal** | **Paso** | **Acción** |
| 1 | Accede al módulo "Reportes" en el panel web. |
| 2 | Filtra por fecha, facultad o tipo de usuario. |
| 3 | El sistema genera gráficos y tablas |
| 4 | Opcionalmente imprime el reporte. |
| **Postcondición** | El administrador obtiene datos para análisis de flujos. | |
| **Excepciones** | 2: Si no hay datos en el rango seleccionado, sugiere ampliar fechas. | |

* 1. **Modelo Lógico**

1. Analisis de Objetos
   1. Estudiante

**Descripción**:  
Usuario principal que accede al campus mediante código de barras en su carnet institucional.

**Atributos**:

* Código de estudiante (ID único)
* Nombre completo
* Facultad/programa académico
* Estado (activo/inactivo)

**Responsabilidades**:

* Presentar su carnet para escaneo
* Notificar pérdida/robo de credenciales

**Relaciones**:

→ Interactúa con Guardia durante validaciones

* 1. Visitante Externo

**Descripción**:  
Persona no afiliada a la universidad que ingresa con autorización temporal.

**Atributos**:

* DNI/pasaporte
* Nombre completo
* Facultad/área visitada
* Motivo de visita
* Fecha/hora de expiración del acceso

**Responsabilidades**:

* Portar identificación física

**Relaciones**:

* → Registrado por Guardia
* ← Validado por Sistema
  1. Guardia de Seguridad

**Descripción**:  
Personal encargado de validar accesos en puntos de control.

**Atributos**:

* ID de empleado
* Turno (mañana/tarde/noche)
* Puntos de acceso asignados
* Nivel de permisos

**Responsabilidades**:

* Escanear códigos de barras
* Registrar visitantes manualmente
* Reportar incidentes
* Verificar identidades en casos excepcionales

**Relaciones**:

* → Usa Sistema para validaciones
* ← Recibe alertas de Administrador
  1. Administrador

**Descripción**:  
Usuario con privilegios para gestionar toda la operación del sistema.

**Atributos**:

* Credenciales de acceso (correo institucional)
* Rol (superadmin/departamental)
* Facultades bajo su supervisión
* Historial de actividades

**Responsabilidades**:

* Dar de alta/baja estudiantes y guardias
* Configurar políticas de acceso
* Generar reportes de seguridad
* Resolver incidencias críticas

**Relaciones**:

* → Asigna permisos a Guardias
* ← Recibe datos de Sistema
  1. Sistema de Control de Accesos

**Descripción**:  
Entidad tecnológica que orquesta todos los procesos.

**Atributos**:

* Base de datos de usuarios
* Registro histórico de accesos
* Reglas de validación configuradas

**Responsabilidades**:

* Validar credenciales en tiempo real
* Generar notificaciones automáticas
* Almacenar registros auditables
* Sincronizar datos entre dispositivos

**Relaciones**:

* ↔ Interactúa con todos los actores
* → Provee datos para Reportes

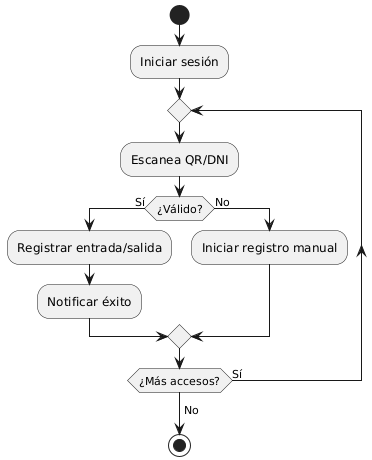
### Relaciones Entre Objetos

* **Estudiante → Sistema:**
  + **Envía código de barras para validación**
  + **Recibe confirmación de acceso/denegación**
* **Guardia ↔ Administrador:**
  + **Reporta incidencias**
  + **Recibe actualizaciones de políticas**
* **Visitante ← Sistema:**
  + **Validar código de acceso**
  + **Registra hora de salida automática**
* **Administrador → Sistema:**
  + **Configura horarios por facultad**

1. Diagrama de Actividades con Objetos

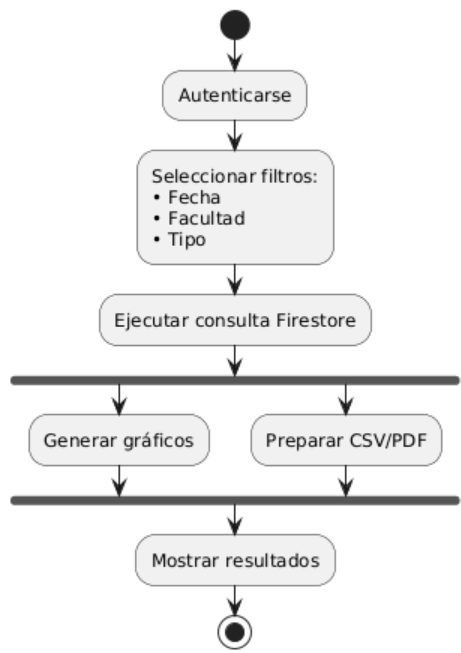
Guardia

Registro de Acceso



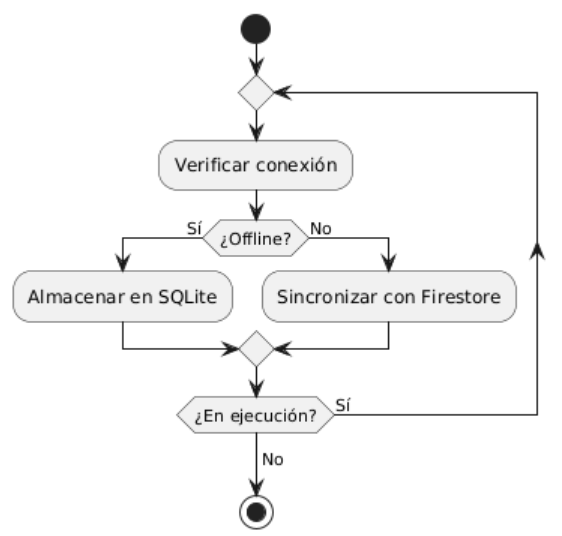
Administrador

Generar Reporte



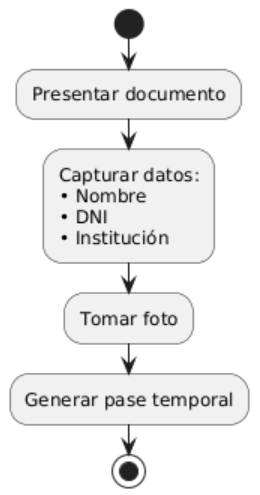
Sistema

Sincronización Offline



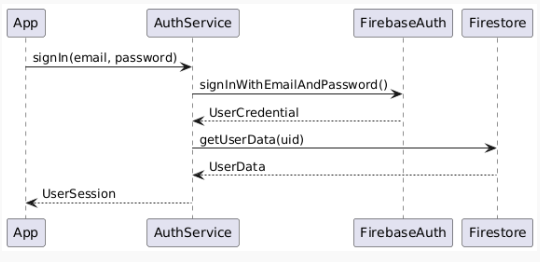
Visitante

Registro Inicial

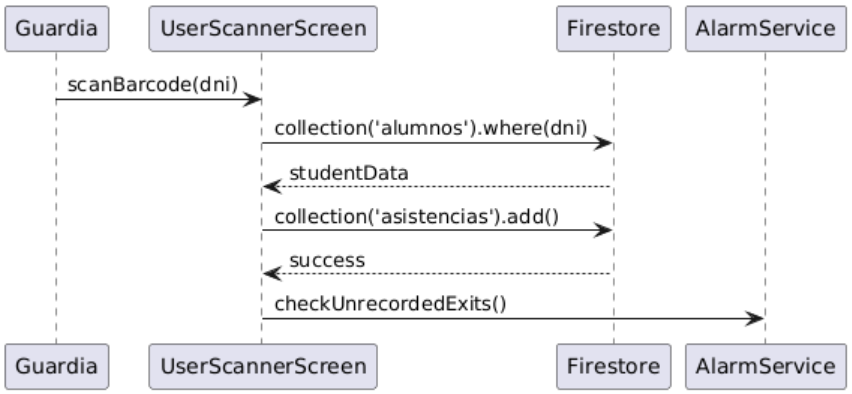


1. Diagrama Secuencial

Secuencia\_Autenticacion



Secuencia\_RegistroAsistencia



Secuencia\_Reportes

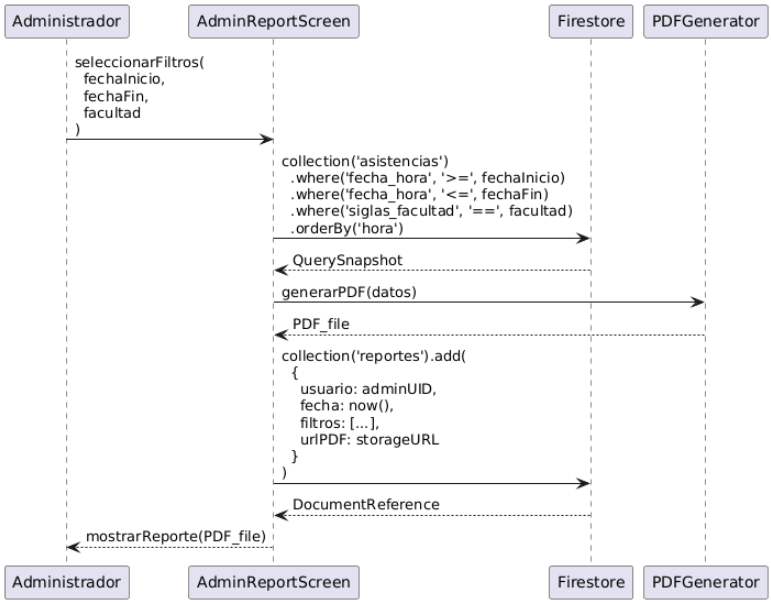
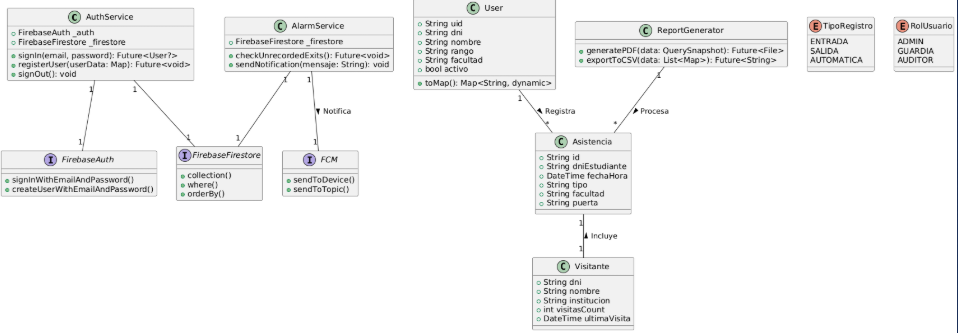


Diagrama de clases



**CONCLUSIONES**

Este proyecto representa una solución innovadora y necesaria para optimizar el control de acceso en la **Universidad Privada de Tacna (UPT)**, abordando problemas críticos como la seguridad, eficiencia y trazabilidad en el ingreso de estudiantes, docentes y visitantes. La implementación de un sistema automatizado basado en tecnologías como **códigos QR, autenticación móvil y registros centralizados** permitirá:

* **Mayor seguridad y control** al restringir el acceso solo a personas autorizadas, reduciendo riesgos de intrusiones no permitidas.
* **Eficiencia operativa** al agilizar el proceso de validación, eliminando filas y errores humanos asociados a métodos manuales.
* **Trazabilidad en tiempo real** mediante registros digitales, facilitando la generación de reportes y la toma de decisiones administrativas.
* **Experiencia mejorada para la comunidad universitaria**, con un sistema intuitivo y accesible desde dispositivos móviles.
* **Escalabilidad y adaptabilidad**, gracias a una arquitectura modular que permitirá futuras integraciones (como RFID o reconocimiento facial).

**Access Guard** no solo resuelve problemas inmediatos de control de acceso, sino que sienta las bases para una gestión más inteligente y segura del campus universitario. Con una implementación bien planificada y un enfoque en la experiencia del usuario por lo que tiene el potencial de convertirse en un referente para otras instituciones educativas.

**RECOMENDACIONES**

* Realizar pruebas controladas con grupos pequeños de usuarios (estudiantes, docentes y personal administrativo) para identificar posibles fallos y ajustar la usabilidad antes del despliegue masivo.
* Implementar talleres o guías interactivas para que la comunidad universitaria comprenda el funcionamiento de la app y los procesos de validación.
* Entrenar al personal de vigilancia y administradores en el uso del panel de control y la interpretación de reportes.
* Asegurar la compatibilidad del sistema con las bases de datos actuales de la UPT (matrículas, horarios, etc.) para evitar redundancias o inconsistencias.
* Implementar medidas adicionales como autenticación en dos pasos (2FA) para usuarios con permisos especiales.
* Cumplir con normativas de protección de datos (Ley de Protección de Datos Personales del Perú) y realizar auditorías periódicas.
* Establecer un equipo de soporte para resolver incidencias rápidamente durante la fase inicial y el mantenimiento posterior.
* Monitorear el rendimiento del sistema para optimizar su escalabilidad, especialmente en horarios pico (ingreso masivo de estudiantes).
* Recopilar opiniones de los usuarios mediante encuestas o análisis de datos para implementar mejoras en futuras actualizaciones.
* Disponer de un método alternativo de acceso temporal (como credenciales físicas) en caso de fallos técnicos o mantenimiento del sistema.