

UNIVERSIDAD NACIONAL DE SAN ANTONIO ABAD DEL CUSCO

FACULTAD DE INGENIERÍA ELÉCTRICA, ELECTRÓNICA, INFORMÁTICA Y MECÁNICA

ESCUELA PROFESIONAL DE INGENIERÍA INFORMÁTICA Y DE SISTEMAS



EduSecure: Plataforma de Control de Acceso, Asistencia y Seguridad Académica

Asignatura: Formulación de Proyectos de Tecnología de Información

Docente: Dr. Ing. Emilio Palomino Olivera

Integrantes:

- | | |
|--|--------|
| • Aguilar Mainicta Gian Marco | 174905 |
| • Conde Padín George Adolfo | 141664 |
| • Condorcahua Ayllone Ferdinand Junior | 184194 |
| • Huahuachampi Hinojosa Zahid | 200878 |

CUSCO - PERÚ

2025

INTRODUCCIÓN

El presente proyecto, titulado: “*EduSecure*”, tiene como objetivo abordar los desafíos relacionados con la seguridad y el control de acceso en entornos académicos para estudiantes y docentes, considerando estos aspectos como factores cruciales para garantizar el resguardo de equipos, la protección de los estudiantes y la eficiencia en los procesos administrativos para la escuela profesional de *Ingeniería Informática y Sistemas* de la *Universidad Nacional de San Antonio Abad del Cusco*.

Las universidades modernas enfrentan retos significativos en cuanto al control de ingreso, la gestión de asistencias y la optimización del uso de aulas y laboratorios. En respuesta a estas necesidades, *EduSecure* propone la implementación de un sistema de seguridad inteligente que integre tecnologías de reconocimiento facial y análisis en tiempo real. Esta solución busca modernizar los procesos de acceso, registro de asistencia y monitoreo de espacios universitarios, ofreciendo mayor confiabilidad, ahorro de tiempo y eficiencia operativa a la institución que adopte el sistema.

ÍNDICE

INTRODUCCIÓN.....	2
1. FINALIDAD PÚBLICA.....	5
1.1 Finalidad Académica.....	5
1.2 Finalidad Económica:.....	5
1.3 Finalidad Social.....	5
2. ANTECEDENTES DEL PROBLEMA.....	6
3. PLANTEAMIENTO DEL PROBLEMA.....	6
3.1 Definición del Problema.....	7
4. OBJETIVOS.....	7
4.1 Objetivo General.....	7
4.2. Objetivos Específicos.....	7
5. MARCO TEÓRICO.....	8
5.1. Sistemas de Control de Acceso Biométricos.....	8
5.2 Reconocimiento Facial: Fundamentos y Algoritmos para Control de Acceso.....	8
5.3. Gestión de Identidades y Accesos (IAM) para Acceso Físico.....	9
5.4 Cámaras IP y su Rol en Sistemas de Seguridad Inteligente.....	10
5.5 Servidor Local y Almacenamiento.....	10
5.6 Cableado Estructurado.....	11
5.7 Seguros de puerta inteligente.....	11
5.8 Sensores de Seguridad para Laboratorios.....	11
5.9. Protección de Datos Personales (Ley N° 29733) en Sistemas Biométricos.....	12
5.10 Marco Conceptual.....	12
6. ANÁLISIS DE REQUERIMIENTOS.....	13
6.1. Requerimientos Funcionales.....	13
6.2. Requerimientos No Funcionales.....	14
7. ESTUDIO DE VIABILIDAD.....	16
7.1 Viabilidad Técnica.....	17
7.1.1 Análisis de Tecnologías Disponibles.....	17
7.1.2 Capacidad de Infraestructura Existente vs. Requerida.....	18
7.1.3 Identificación de Riesgos Técnicos y Plan de Mitigación.....	18
7.2 Viabilidad Económica.....	19
7.2.1 Análisis Costo-Beneficio.....	19
7.3 Viabilidad Operativa.....	19
7.4 Viabilidad Legal.....	20
7.5 Alcance y Delimitaciones.....	20
Alcance.....	20
Limitaciones.....	20
8. DISEÑO DE LA SOLUCIÓN.....	21
8.1 Arquitectura del Sistema.....	21

8.1.1 Concepto General.....	21
8.1.2 Arquitectura General del Sistema.....	21
a) Capa de Dispositivos Físicos (Percepción y Actuación).....	21
b) Capa de Procesamiento y Gestión (Lógica del Sistema - Edge Server).....	22
c) Capa de Aplicación y Servicios (Interfaz y Administración).....	22
8.1.3 Flujo General de Operación.....	23
8.1.4 Modelo de Comunicación.....	23
9. FORMA DE PAGO.....	23
10. PENALIDADES.....	24
11. PLAN DE TRABAJO.....	24
● Fase 1: Diagnóstico Inicial e Infraestructura (2 Semanas).....	24
● Fase 2: Estudio de Viabilidad y Adquisiciones (2 Semanas).....	24
● Fase 3: Diseño del Entorno e Instalación Física (2 Semanas).....	24
● Fase 4: Despliegue de Software e Integración (2 Semanas).....	25
● Fase 5: Capacitación, Mantenimiento y Cierre (1 Semana).....	25
12. SUPERVISIÓN Y MEDIDAS DE CONTROL DURANTE EL SERVICIO.....	25
13. RESPONSABILIDAD POR VICIOS OCULTOS.....	25
13.1 Definición de vicios ocultos.....	25
13.2 Responsabilidad del contratista.....	25
13.3 Procedimiento de reclamación.....	26
13.4 Consecuencias del incumplimiento.....	26
14. CARACTERÍSTICAS TÉCNICAS DEL SISTEMA.....	26
14.1 Sistema de Videovigilancia y Biometría.....	26
14.2 Sistema de Seguridad de Activos (RFID).....	26
14.3 Infraestructura de Red.....	26
14.4 Seguridad Perimetral y Acceso.....	27
15. PLAZOS DE EJECUCIÓN.....	27
16. VALOR REFERENCIAL.....	27
17. EXPERIENCIA DEL POSTOR.....	27
18. RESPONSABILIDAD DEL CONTRATISTA.....	28
19. CONSIDERACIONES FINALES.....	28
ANEXOS.....	29
Cámara Seleccionada: Hikvision DS-2CD2083G2-IU.....	40
Ventajas para EduSecure:.....	41
Proveedor y Precio:.....	41

1. FINALIDAD PÚBLICA

El proyecto aporta un valor significativo a la proyección institucional de la universidad frente a la sociedad. Al implementar un sistema de seguridad inteligente basado en reconocimiento facial, la universidad no solo fortalece la confianza de estudiantes, docentes y padres de familia, sino que también transmite un mensaje de modernización y responsabilidad hacia la comunidad. Este tipo de iniciativas posiciona a la institución como pionera en la adopción de tecnologías de vanguardia, promoviendo un entorno educativo seguro, innovador y alineado con las demandas de la transformación digital en el sector público y privado. Además, la transparencia y confiabilidad de los procesos de asistencia y control de acceso contribuyen a reforzar la credibilidad institucional ante organismos reguladores, entidades gubernamentales y la opinión pública en general.

1.1 Finalidad Académica

El sistema propuesto contribuye a mejorar la gestión educativa mediante la automatización de procesos clave como el control de asistencia de estudiantes y profesores. Al eliminar registros manuales y reducir errores, se garantiza la confiabilidad de los datos académicos, se optimiza el uso de aulas y laboratorios, y se libera tiempo para actividades pedagógicas. Además, el monitoreo en tiempo real permite una mejor planificación institucional y facilita la toma de decisiones basada en evidencia. Gracias al sistema se podrá verificar la asistencia de los estudiantes y docentes, como la hora de ingreso y salida, se podrá plantear acciones en base a los datos registrados en el sistema para la mejora del rendimiento académico universitario.

1.2 Finalidad Económica

La inversión en este proyecto genera beneficios financieros sostenibles:

- **Prevención de pérdidas patrimoniales:** Protege equipos y materiales de alto valor en laboratorios y aulas mediante sensores y vigilancia automatizada.
- **Reducción de costos administrativos:** Automatiza tareas repetitivas como el registro de asistencia, disminuyendo la carga laboral y los

errores humanos como los medios tradicionales que aún se evidencian en la universidad.

1.3 Finalidad Social

El proyecto contribuye al bienestar de la comunidad universitaria de diversas formas:

- Brinda mayor seguridad a estudiantes y docentes, creando un entorno académico confiable.
- Promueve la equidad y transparencia en la asistencia, al eliminar registros manipulables.
- Refuerza la imagen institucional de la universidad como innovadora y responsable socialmente, al implementar soluciones tecnológicas que cuidan tanto la seguridad como el bienestar de su comunidad.

2. ANTECEDENTES DEL PROBLEMA

Las universidades peruanas enfrentan una creciente preocupación por la falta de control en el acceso a sus instalaciones, lo que ha derivado en casos de infiltración, robo y suplantación de identidad. Estos problemas comprometen tanto la seguridad física como la integridad académica de las instituciones.

En mayo del presente año, la Universidad Nacional del Santa en Chimbote fue víctima de un robo de equipos valorizados en S/ 200.000 (La República). El incidente afectó directamente a los laboratorios de dicha universidad, donde se sustrajeron insumos y dispositivos esenciales para el desarrollo académico y científico. Este hecho no solo representa una pérdida económica significativa, sino que también evidencia la vulnerabilidad de los espacios universitarios frente a intrusiones no autorizadas.

En otro caso alarmante, en junio de 2024, la Universidad Andina del Cusco descubrió que una joven había asistido a clases y rendido exámenes durante cinco años haciéndose pasar por otra estudiante que residía en Turquía. La suplantadora recibía

pagos mensuales por este acto, y el fraude sólo fue descubierto tras una denuncia interna. Este tipo de situaciones pone en evidencia las fallas estructurales en los sistemas de verificación de identidad y control de asistencia, que aún dependen de métodos fácilmente manipulables como listas impresas o tarjetas sin validación biométrica.

Estos antecedentes demuestran que los sistemas tradicionales de seguridad y control académico no son suficientes para enfrentar los desafíos actuales. La implementación de tecnologías como el reconocimiento facial y el análisis en tiempo real permitiría prevenir la suplantación, restringir el acceso a personas no autorizadas, y proteger los activos institucionales, fortaleciendo así la confianza en la gestión universitaria.

3. PLANTEAMIENTO DEL PROBLEMA

Actualmente, los laboratorios y aulas de la escuela profesional Ingeniería Informática y Sistemas de la Universidad Nacional San Antonio Abad del Cusco presentan dificultades en la gestión de accesos y asistencia. Los métodos tradicionales, como el uso de llaves físicas y registros manuales, generan:

- Inseguridad en el acceso a laboratorios y aulas.
- Pérdida de tiempo en procesos de verificación.
- Falta de confiabilidad en los datos de asistencia y ocupación.

3.1 Definición del Problema

El problema central radica en la falta de un sistema automatizado y confiable para el control de acceso y monitoreo en los espacios universitarios. Esto genera:

- Riesgo de ingreso de personas no autorizadas.
- Procesos lentos para la apertura de aulas.
- Ausencia de datos confiables sobre asistencia y ocupación de espacios.
- Posibles pérdidas materiales en laboratorios por falta de control.
- Desconexión entre la seguridad física y los sistemas administrativos.

4. OBJETIVOS

4.1 Objetivo General

Diseñar e implementar una plataforma integral de seguridad académica, que combine tecnologías de reconocimiento facial, videovigilancia y sensores inteligentes para el control de acceso, asistencia y protección de espacios universitarios. El sistema estará orientado a prevenir el robo de materiales, monitorear la ocupación de aulas y laboratorios, y fortalecer la seguridad física y administrativa, promoviendo un entorno académico confiable, eficiente y protegido.

4.2. Objetivos Específicos

- Diseñar la arquitectura tecnológica del sistema (cámaras IP, servidor de reconocimiento, base de datos, etc).
- Implementar el módulo de control de acceso biométrico mediante reconocimiento facial.
- Evaluar la precisión del sistema con un índice de acierto superior al 92%.
- Automatizar el registro de asistencia con tolerancia de tiempos.
- Generar reportes de asistencia y uso de espacios según los períodos establecidos para cada parcial dentro del semestre académico.
- Integrar un sistema de alertas en tiempo real para accesos no autorizados y situación de robo.
- Desarrollar funcionalidades de monitoreo de ocupación y conteo de estudiantes por aula.
- Evaluar la precisión y eficiencia del sistema en escenarios reales.

5. MARCO TEÓRICO

5.1. Sistemas de Control de Acceso Biométricos

Un Sistema de Control de Acceso (ACS) es un conjunto de componentes hardware y software cuya función primordial es restringir el ingreso a un espacio físico o lógico únicamente a personas autorizadas. Este proyecto se enfoca específicamente en los sistemas biométricos, los cuales utilizan características fisiológicas únicas e intransferibles para la autenticación. La base teórica de un ACS biométrico se centra en tres principios de seguridad:

- Autenticación: Verificar la identidad de la persona mediante "algo que se es" (biometría). Este método es superior a "algo que se tiene" (tarjetas, que se pueden perder o robar) o "algo que se sabe" (contraseñas, que se pueden olvidar o hackear).
- Autorización: Determinar si la identidad autenticada tiene permisos para acceder al recurso en un momento específico, basándose en políticas predefinidas (roles y horarios).
- Auditoría: Registrar todos los intentos de acceso—exitosos, fallidos o de identidades no reconocidas—para generar trazas auditables y permitir el seguimiento forense.

5.2 Reconocimiento Facial: Fundamentos y Algoritmos para Control de Acceso

El reconocimiento facial es la tecnología biométrica elegida para este proyecto. Su idoneidad para control de acceso se debe a su naturaleza contactless (sin contacto físico, higiénica) y pasiva (el usuario no necesita realizar una acción consciente más que mirar a la cámara). El proceso técnico consta de:

1. **Detección de Rostro:** Localizar y aislar la región del rostro dentro del flujo de video. Se utilizarán algoritmos preentrenados como Haar

Cascades o un Multi-Task Convolutional Neural Network (MTCNN) integrados en OpenCV para esta etapa, garantizando alta eficacia incluso con variaciones de iluminación y ángulo.

2. **Preprocesamiento:** Normalizar la imagen del rostro detectado para homogenizar la entrada al modelo de reconocimiento. Esto incluye corrección de iluminación, alineación basada en puntos de referencia faciales (ojos, nariz), redimensionamiento y conversión a escala de grises.
3. **Extracción de Características (Embedding):** Convertir el rostro preprocesado en una representación numérica única (vector de características de 128 a 512 dimensiones) que capture sus atributos distintivos. Esta es la etapa crucial donde bibliotecas como Face Recognition (construida sobre Dlib) o OpenCV's FaceRecognizer sobresalen, utilizando modelos de Deep Learning como FaceNet.
4. **Comparación y Decisión:** Comparar el "embedding" generado con los vectores almacenados en la base de datos de usuarios autorizados. Si la distancia Euclídea (o coseno) entre el vector de entrada y un vector almacenado está por debajo de un umbral predefinido, se confirma la identidad y se procede a la etapa de autorización.
 - **OpenCV (Open Source Computer Vision Library):** Será la columna vertebral para la captura de video, la detección inicial de rostros y las tareas básicas de procesamiento de imágenes.
 - **Dlib & Face Recognition Library:** Se emplearán como el núcleo del motor de reconocimiento debido a su equilibrio perfecto entre alta precisión, facilidad de uso y eficiencia computacional, ideal para un prototipo que puede desplegarse en hardware embebido como una Raspberry Pi o Jetson Nano.

5.3. Gestión de Identidades y Accesos (IAM) para Acceso Físico

El sistema propuesto es, en esencia, un sistema de Gestión de Identidades y Accesos (IAM) aplicado al acceso físico. Sus principios se adaptan de la siguiente manera:

- **Ciclo de Vida de la Identidad Digital-Física:** Gestionar el proceso completo de un usuario, desde el registro biométrico (captura facial y creación del embedding), la actualización de sus permisos (asignación/remoción de roles), hasta la baja definitiva (eliminación de sus vectores biométricos de la base de datos) cuando ya no requiera acceso.
- **Acceso Basado en Roles (RBAC):** La autorización no se gestiona a nivel individual sino mediante roles (e.jT., "Estudiante", "Docente", "Administrador de Lab"). A cada rol se le asignan políticas de acceso que definen a qué espacios y en qué horarios puede ingresar.
- **Políticas de Acceso Contextual:** El sistema evalúa en milisegundos no solo "quién es" sino también "si tiene permiso para entrar ahora". Esto crea una capa de seguridad adicional basada en el contexto temporal.

En escenarios más avanzados, los sistemas de control de acceso pueden vincularse con **seguros inteligentes**, donde las aseguradoras ajustan automáticamente la cobertura o las primas según los reportes de acceso, asistencia y seguridad generados por el sistema. Esta integración ofrece una capa adicional de valor al permitir que las instituciones educativas reduzcan costos de aseguramiento mientras mantienen un entorno seguro y auditável.

5.4 Cámaras IP y su Rol en Sistemas de Seguridad Inteligente

Para el sistema EduSecure se ha optado por utilizar cámaras IP tipo domo con capacidad de procesamiento en el borde (edge computing). Estas cámaras permiten realizar tareas básicas de reconocimiento facial directamente en el

dispositivo, reduciendo la carga sobre el servidor central y mejorando la velocidad de respuesta.

Características clave:

- Diseño discreto y antivandálico, ideal para aulas y pasillos.
- Resolución Full HD con visión nocturna.
- Compatibilidad con protocolos ONVIF para integración sencilla.
- Capacidad de detección facial en tiempo real.

Su forma compacta y su capacidad de procesamiento local las hacen ideales para entornos educativos, donde se requiere vigilancia constante sin generar incomodidad visual. Además, su integración con el sistema de reconocimiento facial permite registrar asistencia sin intervención manual.

5.5 Servidor Local y Almacenamiento

El sistema se implementará sobre un servidor local con almacenamiento SSD de 2 TB, equipado con una GPU dedicada para acelerar el procesamiento de imágenes y modelos de reconocimiento facial.

Características clave:

- Procesador Intel i7 o superior.
- GPU NVIDIA con soporte CUDA (mínimo 6 GB VRAM).
- 32 GB de RAM para procesamiento simultáneo de múltiples cámaras.
- Base de datos cifrada alojada localmente.

La elección de un servidor local garantiza la protección de datos sensibles, evita la dependencia de servicios en la nube y permite operar incluso en condiciones de conectividad limitada. El almacenamiento SSD asegura velocidad en la lectura/escritura de registros y grabaciones.

5.6 Cableado Estructurado

Se utilizará cableado estructurado Cat6 con tecnología PoE (Power over Ethernet) para conectar cámaras y sensores al servidor.

Características clave:

- Transmisión de datos a 1 Gbps.
- Alimentación eléctrica integrada en el mismo cable.
- Reducción de puntos de falla y simplificación del diseño físico.

El uso de PoE permite instalar cámaras en ubicaciones estratégicas sin requerir tomas eléctricas adicionales, lo que reduce costos y facilita el mantenimiento. El cableado Cat6 asegura estabilidad y velocidad en la transmisión de video y datos biométricos.

5.7 Seguros de puerta inteligente

Para el acceso de docentes se instalarán seguros electromagnéticos con cámara integrada y lector facial embebido en la puerta principal del aula.

Características clave:

- Activación automática tras reconocimiento facial exitoso.
- Cámara frontal para registro visual del acceso.
- Registro de eventos en la base de datos del sistema.

Este tipo de seguro permite un control de acceso autónomo, sin necesidad de llaves ni tarjetas. La cámara integrada refuerza la trazabilidad de los ingresos, mientras que el lector facial garantiza que solo personal autorizado pueda ingresar.

5.8 Sensores de Seguridad para Laboratorios

Se incorporará un sistema de sensores de movimiento y peso en las salidas de los laboratorios, capaces de detectar la extracción no autorizada de equipos o materiales.

Características clave:

- Detección de objetos en movimiento con peso superior a un umbral definido.
- Activación de alarma sonora y notificación al sistema central.
- Integración con cámaras IP para verificación visual del evento.

Justificación:

Estos sensores permiten proteger activos valiosos sin interferir con la dinámica académica. Al detectar anomalías en tiempo real, se puede actuar preventivamente ante intentos de robo o mal uso del equipamiento.

5.9. Protección de Datos Personales (Ley N° 29733) en Sistemas Biométricos

El tratamiento de datos biométricos está categorizado como dato personal sensible según la Ley N° 29733. Por lo tanto, el diseño del sistema se rige por los siguientes principios:

- **Principio de Finalidad:** Los datos biométricos se recogen exclusivamente para los fines de control de acceso y registro de asistencia académica dentro de la universidad. Queda explícitamente prohibido su uso para cualquier otra finalidad (e.g., vigilancia general, análisis de comportamiento no autorizado).
- **Principio de Consentimiento Previo y Explícito:** Todo usuario deberá ser informado de manera clara e inequívoca sobre el tratamiento de sus datos biométricos y deberá firmar un formato de consentimiento informado antes de ser registrado en el sistema.
- **Principio de Seguridad:** Se implementarán medidas técnicas robustas para proteger los datos. Esto incluye:
 - Cifrado de la Base de Datos: Los vectores biométricos y la información personal asociada se almacenarán en una base de datos cifrada.
 - Almacenamiento Local: Los datos se almacenarán en un servidor local dentro de la red de la universidad, sin conexión a cloud pública, para minimizar riesgos de exposición externa.
 - Acceso Restringido: Solo el personal administrativo autorizado tendrá acceso a la base de datos de gestionar usuarios.

5.10 Marco Conceptual

- Biometría: Tecnología de autenticación que utiliza características fisiológicas (rostro, huellas) únicas e intransferibles para verificar la identidad de un individuo.
- Autenticación Contactless: Proceso de verificación de identidad que no requiere contacto físico entre el sensor y el usuario, favoreciendo la higiene y la fluidez del acceso.
- Embedding (Vector de Características): Representación numérica compacta y abstracta de un rostro, generada por una red neuronal, que permite comparar similitudes de forma eficiente.
- Falso Aceptación (FAR): Error que ocurre cuando el sistema incorrectamente identifica a una persona no autorizada como si fuera un usuario registrado. (Crítico para la seguridad).
- Falso Rechazo (FRR): Error que ocurre cuando el sistema no reconoce a un usuario legítimo. (Crítico para usabilidad).
- Umbral de Confianza: Valor numérico ajustable que define el grado de similitud requerido para una coincidencia. Un umbral bajo aumenta la FAR (menos segura) y disminuye la FRR (más usable), y viceversa.

6. ANÁLISIS DE REQUERIMIENTOS

6.1. Requerimientos Funcionales

- **RF01: Gestión de Usuarios y Roles**

El sistema debe permitir registrar, modificar y eliminar usuarios con diferentes roles (administrador, docente, estudiante, personal administrativo), garantizando la trazabilidad de sus accesos.

- Registrar, modificar y eliminar usuarios con diferentes perfiles (estudiante, docente, administrador)
- Gestionar permisos de acceso basados en roles (RBAC)

- **RF02: Registro y Codificación Biométrica**

El sistema debe capturar imágenes de rostros y codificarlas mediante algoritmos de reconocimiento facial para su posterior identificación.

- Capturar imágenes faciales mediante cámaras IP.
- Generar vectores de características (embeddings) mediante algoritmos de IA.

- **RF03: Control de Acceso Inteligente**

El sistema debe validar el acceso a las instalaciones en función del reconocimiento facial y el horario establecido para cada usuario.

- Validar identidad mediante reconocimiento facial.
- Verificar autorización según horarios y espacios permitidos.
- Activar/desactivar seguros electromagnéticos automáticamente.

- **RF04: Registro Automático de Asistencia**

El sistema debe generar de manera automática el registro de asistencia de estudiantes y personal al momento de su ingreso.

- Registrar ingreso/salida de estudiantes y docentes.
- Aplicar tolerancias de tiempo configurables.
- Sincronizar con el sistema académico existente.

- **RF05: Sistema de Alertas en Tiempo Real**

El sistema debe emitir notificaciones inmediatas ante intentos de ingreso no autorizados o fuera de horario.

- Notificar intentos de acceso no autorizado.
- Alertar sobre extracción no autorizada de equipos.
- Generar notificaciones por múltiples canales (panel, app, etc).

- **RF06: Generación de Reportes de Asistencia y Accesos**

El sistema debe generar reportes periódicos (diarios, semanales, mensuales) que consoliden la información de accesos y asistencias.

- Reportes de asistencia (diarios, semanales, mensuales)
- Estadísticas de uso de espacios académicos.
- Auditoría de eventos de seguridad.

- **RF07: Monitoreo de Ocupación.**

- Contar personas en aulas y laboratorios en tiempo real.
- Alertar sobre sobrecupo o subutilización.

6.2. Requerimientos No Funcionales

- **RNF01: Rendimiento**

El sistema debe responder en un tiempo inferior a 3 segundos en las operaciones críticas (reconocimiento facial y validación de acceso).

- Tiempo de respuesta menor a 3 segundos para reconocimiento facial.

- Procesamiento simultáneo: Mayor o igual a 4 flujos de vídeo HD.
 - Latencias de red: < 100 ms entre cámaras y servidor.
-
- **RNF02: Seguridad (Cifrado de datos, cumplimiento de LOPD)**

Toda la información personal y biométrica deberá estar cifrada y cumplir con la Ley de Protección de Datos Personales (Ley N° 29733).

- Cifrado AES-256 para datos biométricos.
 - Autenticación multifactor para acceso administrativo.
 - Cumplimiento integral de Ley N° 29733
-
- **RNF03: Usabilidad**

La interfaz debe ser intuitiva, con menús simples y de fácil comprensión para usuarios con distintos niveles de alfabetización digital.

- Tiempo de entrenamiento para administradores: < 2 horas.
 - Interfaz responsive para dispositivos móviles.
 - Documentación completa en español.
-
- **RNF04: Confidencialidad (Disponibilidad del 95%)**

El sistema debe asegurar una disponibilidad mínima del 95%, reduciendo al mínimo las interrupciones en la operación.

- Disponibilidad: 95% en horario académico (7:00 AM - 10:00 PM)
- Tiempo medio de recuperación (MTTR): < 30 minutos.
- Backup automático diario.

- **RNF05: Escalabilidad**

El sistema debe poder adaptarse al crecimiento de la institución (mayor número de usuarios, más cámaras y dispositivos).

- Soporte para 50 cámaras adicionales sin cambios arquitectónicos.
- Capacidad para 5,000 usuarios registrados.
- APIs estandarizadas para integración futura.

- **RNF06: Mantenibilidad**

- Código documental al 90%.
- Tiempo de despliegue de actualizaciones: < 1 hora.
- Logs detallados para diagnóstico.

7. ESTUDIO DE VIABILIDAD

En los últimos años, diversas instituciones educativas alrededor del mundo han comenzado a implementar sistemas biométricos, especialmente el reconocimiento facial, como herramienta clave para mejorar la seguridad, prevenir suplantaciones de identidad y optimizar la gestión administrativa. Esta tendencia responde a la necesidad de modernizar los procesos de ingreso, asistencia y control de acceso en entornos académicos cada vez más digitalizados.

En Perú, la Universidad Continental se convirtió en pionera al desarrollar una aplicación de reconocimiento facial basada en inteligencia artificial para sus exámenes de admisión. Este sistema, creado por su equipo de Tecnología Informática en colaboración con la Comisión Permanente de Admisión, permite verificar la identidad de los postulantes mediante fotografías cargadas en una base de datos oficial, cumpliendo con los lineamientos de la SUNEDU. Esta iniciativa no solo

refuerza la seguridad del proceso, sino que también marca un precedente en la integración de IA en la educación superior peruana. Claro que en este contexto con el fin de la no suplantación de identidad frente a una prueba.

Asimismo, la Universidad Ricardo Palma (URP) ha desarrollado un sistema de reconocimiento facial para gestionar el acceso de estudiantes a sus instalaciones. El proyecto, liderado por la Escuela Profesional de Ingeniería Mecatrónica, busca agilizar el ingreso y fortalecer la seguridad interna mediante una solución tecnológica que combina cámaras de alta resolución con algoritmos de detección facial entrenados en entornos universitarios.

En otro caso, la Universidad Nacional Intercultural de la Selva Central Juan Santos Atahualpa ha explorado el uso de reconocimiento facial para identificar postulantes durante el proceso de admisión, como parte de una tesis de investigación en Ingeniería de Sistemas e Informática. Este trabajo demuestra el creciente interés académico en aplicar tecnologías biométricas a contextos educativos específicos.

A diferencia de países como China, Estados Unidos o Corea del Sur, donde el reconocimiento facial ya se utiliza ampliamente en universidades para controlar el acceso a bibliotecas, residencias y aulas, en América Latina su adopción aún es incipiente. Esta brecha tecnológica representa una oportunidad estratégica para innovar en la región, posicionando a las instituciones que adopten estas soluciones como referentes en transformación digital educativa.

En cuanto a las tecnologías empleadas, proyectos como los mencionados han utilizado herramientas concretas como MediaPipe Face Detection de Google, que permite una detección facial rápida y precisa en dispositivos móviles, y FaceNet, un modelo de aprendizaje profundo que genera representaciones vectoriales de rostros para comparaciones eficientes. Estas soluciones superan el enfoque genérico de bibliotecas como OpenCV y TensorFlow, al ofrecer modelos preentrenados y optimizados para tareas específicas de reconocimiento facial en tiempo real, incluso en condiciones adversas como iluminación variable o uso de mascarillas.

7.1 Viabilidad Técnica

El sistema propuesto plantea una arquitectura híbrida que integra IoT (Internet de las Cosas) e Inteligencia Artificial. La solución combina terminales de reconocimiento facial para control de acceso, cámaras IP para asistencia automatizada y un sistema de sensores/RFID para la protección perimetral de activos.

7.1.1 Análisis de Tecnologías Disponibles

Para la selección del stack tecnológico se realizó un análisis comparativo priorizando precisión, velocidad y costo computacional:

1. Motor de Reconocimiento Facial:

- Tecnología Seleccionada: FaceNet + MediaPipe (Google).
- Justificación: A diferencia de métodos tradicionales (Haar Cascades) o bibliotecas genéricas (OpenCV estándar), FaceNet genera "embeddings" (vectores numéricos) del rostro que permiten comparaciones con una precisión superior al 99% incluso con occlusiones parciales (mascarillas) o cambios de iluminación. MediaPipe se utiliza para la detección ultrarrápida de rostros antes del reconocimiento, optimizando el uso de la GPU.

2. Protección de Activos (Anti-Robo):

- a. Tecnología Seleccionada: RFID UHF (Ultra High Frequency).
- b. Justificación: Se descartaron los sensores de movimiento simples porque no discriminan objetos. La tecnología RFID UHF permite etiquetar activos críticos (PCs, Cañones) con tags anti-metal. Si un activo etiquetado cruza el umbral de la puerta sin autorización, las antenas lo detectan y activan la alerta específica, algo inviable con tecnologías convencionales.

7.1.2 Capacidad de Infraestructura Existente vs. Requerida

La viabilidad técnica depende de la actualización de la infraestructura de red del laboratorio piloto:

- Infraestructura Existente: Red eléctrica estándar y puntos de red Cat5e (insuficientes para video 4K y PoE).
- Infraestructura Requerida (Implementación):
 - Cableado Estructurado: Migración a cableado Cat 6 (100% Cobre) para soportar transmisión Gigabit y alimentación PoE (Power over Ethernet) sin sobrecalentamiento.
 - Switching: Implementación de Switches PoE+ (IEEE 802.3at) con un budget energético >120W para alimentar cámaras y antenas RFID simultáneamente sin necesidad de cableado eléctrico adicional.
 - Servidor Local: Estación de trabajo con GPU dedicada (NVIDIA CUDA) para el procesamiento de los vectores faciales en tiempo real (Edge Computing) para evitar latencia de red hacia la nube.

7.1.3 Identificación de Riesgos Técnicos y Plan de Mitigación

Riesgo Técnico	Impacto	Plan de Mitigación (Contramedida)
Falsos Negativos por Contraluz	Alto (No abre la puerta)	Uso de cámaras con WDR (Rango Dinámico Amplio) de 120dB y luz de relleno automática.

Fallo de Red / Sistema Caído	Crítico (Bloqueo de aula)	Las cerraduras inteligentes seleccionadas (Rav Bariach T7) cuentan con llave física de emergencia y batería de respaldo independiente.
Bloqueo de señal RFID (Metal)	Medio (No detecta robo)	Adquisición estricta de Tags RFID Anti-Metal (espuma/ABS) diseñados específicamente para chasis de computadoras.
Latencia alta en asistencia	Bajo (Retraso en reporte)	Procesamiento asíncrono: La asistencia no bloquea el acceso; se procesa en segundo plano para no afectar el flujo de ingreso.

7.2 Viabilidad Económica

7.2.1 Análisis Costo-Beneficio

La inversión inicial (CAPEX) se justifica mediante la reducción de costos operativos y la mitigación de riesgos (pérdidas):

- Beneficios Tangibles (Ahorro directo):
 - Prevención de Pérdidas: El costo de reposición de un solo Proyector Multimedia equivale aproximadamente al 80% del costo total del sistema de sensores antirrobo propuesto. Evitar un solo incidente de robo justifica la inversión en seguridad perimetral.
 - Recuperación de Horas Lectivas: Se estima un ahorro promedio de 10 a 15 minutos por sesión de clase, tiempo que actualmente se pierde en el llamado de lista manual y la gestión logística de llaves físicas.
- Beneficios Intangibles:

- Mejora sustancial en la imagen institucional, proyectándose como una universidad de vanguardia tecnológica.
- Trazabilidad forense exacta que permite saber quién entró y a qué hora ante cualquier incidente, mejorando el clima de seguridad.

7.3 Viabilidad Operativa

El sistema está diseñado para integrarse de manera transparente en el flujo diario universitario sin requerir habilidades técnicas avanzadas por parte de los usuarios finales:

- Docentes: No requieren llaves físicas ni tarjetas que puedan perderse. Su "llave" es su rostro. La curva de aprendizaje es mínima (solo requieren un registro biométrico inicial de 1 minuto).
- Administrativos: La gestión se centraliza en un Dashboard Web intuitivo. Las alertas de robo (RFID) o intrusión (ventanas) llegan en tiempo real al personal de seguridad, mejorando el tiempo de respuesta de minutos a segundos.
- Mantenimiento: Al utilizar tecnología PoE y sensores estándar de mercado, el mantenimiento se reduce a limpieza de lentes y revisión de conectividad semestral, sin requerir paradas críticas del sistema.

7.4 Viabilidad Legal

El proyecto ha sido diseñado cumpliendo estrictamente con la normativa peruana vigente:

- Ley N° 29733 (Ley de Protección de Datos Personales): Se implementará el principio de Consentimiento Informado. Los datos biométricos (rostros) no se almacenarán como imágenes jpg, sino

como vectores numéricos encriptados (hashes), haciendo imposible la reconstrucción del rostro original por terceros (Privacidad por Diseño).

- Registro de Banco de Datos: El sistema contempla el registro formal de la base de datos ante la Dirección General de Protección de Datos Personales del Ministerio de Justicia y Derechos Humanos (MINJUSDH).

7.5 Alcance y Delimitaciones

Alcance

- Implementación completa (Hardware y Software) en un Laboratorio Piloto de la facultad.
- Precisión del algoritmo de reconocimiento facial superior al 95% en condiciones de iluminación controlada.
- Sistema de control de asistencia automatizado con generación de reportes exportables.
- Sistema de seguridad perimetral integrado (RFID en puerta + Sensores magnéticos en ventanas) con sirena local y notificación digital.

Limitaciones

- Condiciones Extremas: El reconocimiento facial puede disminuir su eficacia en condiciones de oscuridad total (ej. corte de luz nocturno sin energía de respaldo).
- Alcance RFID: El sistema antirrobo detecta la salida no autorizada del activo por la puerta, pero no realiza un rastreo de ubicación posterior (no incluye GPS).
- Reconocimiento de Emociones: Esta funcionalidad se mantendrá en fase beta experimental con fines puramente académicos y no influirá en la calificación ni asistencia del estudiante.

8. DISEÑO DE LA SOLUCIÓN

8.1 Arquitectura del Sistema

8.1.1 Concepto General

El sistema EduSecure se concibe como una plataforma integral de Inmótica (Automatización de Edificios) aplicada al entorno académico. Su núcleo operativo busca la convergencia de tres pilares fundamentales: Identidad Digital (biometría facial), Seguridad de Activos (RFID UHF) y Protección Perimetral (sensores de intrusión).

El propósito del sistema trasciende el simple control de puertas; busca crear un ecosistema de "Aula Inteligente" donde la asistencia se registra de manera transparente (sin intervención activa), el acceso es estrictamente validado por algoritmos de Inteligencia Artificial y los activos críticos de la universidad (equipos de cómputo, proyectores) están protegidos digitalmente contra sustracciones no autorizadas.

8.1.2 Arquitectura General del Sistema

El sistema se basa en una arquitectura de Computación en el Borde (Edge Computing) distribuida en tres capas jerárquicas, diseñadas para minimizar la latencia y garantizar la operatividad incluso ante fallos de conexión externa:

a) Capa de Dispositivos Físicos (Percepción y Actuación)

Es la frontera física del sistema, encargada de la digitalización del entorno.

Incluye:

- Nodo de Acceso Biométrico: Constituido por cámaras IP de alta resolución (8MP) con WDR de 120dB situadas a la entrada, encargadas de capturar el flujo de video para la detección de rostros.
- Nodo de Seguridad de Activos (RFID): Pórticos o antenas UHF situadas en el marco de la puerta, operando en la frecuencia 902-928 MHz, capaces de leer etiquetas pasivas (tags) adheridas a los equipos.

- Nodo de Protección Perimetral: Sensores magnéticos de grado industrial instalados en las hojas de las ventanas y sensores de ruptura de cristal, conectados a una central de alarma local.
- Actuadores: Cerraduras electromagnéticas inteligentes (Modelo Rav Bariach T7 o similar) y sirenas estroboscópicas para disuasión audiovisual.

b) Capa de Procesamiento y Gestión (Lógica del Sistema - Edge Server)

Ubicada en un servidor local dentro del laboratorio o facultad, esta capa procesa la información cruda sin necesidad de ir a la nube:

- Motor de Inferencia Biométrica: Ejecuta los modelos de IA (MediaPipe para detección + FaceNet para reconocimiento). Transforma la imagen facial en un vector numérico (embedding) y lo compara con la base de datos local.
- Middleware RFID: Filtra las lecturas de los tags, discriminando entre lecturas erróneas y movimientos reales de salida de activos.
- Lógica de Negocio (Business Logic): Determina si una persona tiene permiso en ese horario específico o si un activo tiene autorización de salida.
- Gestor de Eventos: Orquesta la respuesta (abrir puerta / activar sirena / enviar alerta silenciosa).

c) Capa de Aplicación y Servicios (Interfaz y Administración)

La capa superior donde interactúan los usuarios humanos:

- Dashboard Administrativo (Web): Panel para el alta/baja de usuarios, asignación de horarios, registro de inventario RFID y visualización de logs de seguridad.
- App Móvil (Notificaciones): Canal de comunicación Push para alertar al personal de seguridad en tiempo real sobre intrusiones o intentos de robo.
- Módulo de Reportes: Generación automática de listas de asistencia (Excel/PDF) y estadísticas de uso del laboratorio.

8.1.3 Flujo General de Operación

Escenario A: Control de Acceso y Asistencia

1. El usuario se aproxima a la puerta. La cámara IP detecta presencia mediante análisis de video.
2. El sistema captura el rostro y ejecuta la prueba de "Liveness" (detección de vida) para evitar suplantación con fotos.
3. Si la identidad es válida y el horario coincide con una clase programada:
 - Se envía pulso de apertura a la cerradura inteligente.
 - Se registra el evento como "Asistencia: Presente" en la base de datos.
4. Si la identidad no es válida o no corresponde al horario, la puerta permanece bloqueada y se registra un "Intento de Acceso Fallido".

Escenario B: Seguridad de Activos (Anti-Robo)

1. Un activo (ej. Proyector) etiquetado con un Tag RFID Anti-metal es movido hacia la salida.
2. Las antenas del pórtico RFID detectan el código EPC único del activo.
3. El sistema consulta en milisegundos: *¿Existe una orden de salida autorizada para este activo?*
4. Si la respuesta es NO: Se activa la sirena estroboscópica local y se envía una alerta crítica a la App de seguridad y administración.

8.1.4 Modelo de Comunicación

- Protocolo de Red: TCP/IP sobre cableado estructurado Cat6 para la transmisión de video (RTSP) y datos de control.
- Protocolo de Sensores: Señales digitales (I/O) para sensores magnéticos y comunicación Wiegand/OSDP o TCP/IP para los lectores RFID.
- Seguridad en Transmisión: Implementación de túneles SSL/TLS para la comunicación entre el servidor local y la interfaz web/nube.

9. FORMA DE PAGO

La Universidad (o la Entidad Contratante) realizará el pago del servicio de implementación del proyecto EduSecure bajo la modalidad de suma alzada, distribuido en los siguientes hitos o valorizaciones, previa conformidad del Supervisor del Proyecto:

1. Pago Inicial (30%): A la firma del contrato y aprobación del Plan de Trabajo (Fase 1), destinado a la adquisición de hardware importado (Cámaras 8MP, Lectores RFID, Servidor GPU).
2. Primer Pago Parcial (30%): A la culminación de la Fase 3: Diseño del Entorno y Soluciones Tecnológicas, acreditando la instalación del cableado estructurado y montaje de dispositivos físicos.
3. Segundo Pago Parcial (30%): A la culminación de la Fase 4: Formulación del Plan de Implementación, que incluye la puesta en marcha del software, integración de bases de datos y pruebas funcionales exitosas (marcha blanca).
4. Pago Final (10%): A la entrega del Informe Final, Manuales de Usuario, Capacitación al personal y Carta de Garantía por vicios ocultos (Cierre de Fase 5).

10. PENALIDADES

En caso de retraso injustificado en la ejecución de las prestaciones objeto del contrato, la Entidad aplicará al CONTRATISTA una penalidad por cada día de atraso, hasta por un monto máximo equivalente al diez por ciento (10%) del monto del contrato vigente.

Penalidades Específicas por Nivel de Servicio (SLA):

- Falsos Positivos Críticos: Se aplicará una penalidad del 0.5% de la UIT por cada evento donde el sistema de seguridad falle en detectar la sustracción simulada de un activo durante las pruebas de aceptación.
- Indisponibilidad del Sistema: Si el sistema presenta caídas no programadas superiores a 4 horas durante el periodo de prueba, se aplicará una penalidad por día de inoperatividad.

11. PLAN DE TRABAJO

El desarrollo del proyecto se estructura en cinco fases secuenciales y críticas para asegurar la calidad técnica:

- **Fase 1: Diagnóstico Inicial e Infraestructura (2 Semanas)**
 - Levantamiento de información in-situ: Medición de niveles de luz (luxometría) para calibración de cámaras.
 - Inspección de ductería existente y análisis de interferencias electromagnéticas para el sistema RFID.
 - Verificación de la carga eléctrica y disponibilidad de puntos de red.
- **Fase 2: Estudio de Viabilidad y Adquisiciones (2 Semanas)**
 - Confirmación de especificaciones técnicas finales (validación de modelos de hardware).
 - Gestión de compras y logística de equipos importados (Tags RFID, Cámaras con IA).
 - Configuración del entorno de desarrollo (Servidor, Base de Datos, Entorno Python/FaceNet).
- **Fase 3: Diseño del Entorno e Instalación Física (2 Semanas)**
 - Tendido de Cableado Estructurado Cat6 (100% Cobre) certificado.
 - Montaje de cámaras, antenas RFID y sensores magnéticos en ventanas.
 - Instalación de cerraduras inteligentes Rav Bariach T7 en puertas.
 - Conectorización y peinado de Gabinete de Comunicaciones (Rack).
- **Fase 4: Despliegue de Software e Integración (2 Semanas)**
 - Despliegue del software EduSecure en el servidor local.
 - Entrenamiento inicial del modelo biométrico con data de prueba.
 - Etiquetado masivo de activos (pegado de Tags RFID anti-metal).
 - Pruebas de estrés y calibración de sensibilidad de sensores.
- **Fase 5: Capacitación, Mantenimiento y Cierre (1 Semana)**
 - Capacitación a docentes (uso de biometría) y administradores (uso del dashboard).
 - Entrega de manuales técnicos y de usuario.
 - Firma del acta de conformidad y recepción del proyecto.

12. SUPERVISIÓN Y MEDIDAS DE CONTROL DURANTE EL SERVICIO

La supervisión del proyecto estará a cargo de un Coordinador Técnico designado por la Facultad (Ingeniería de Sistemas/Informática), quien tendrá las siguientes atribuciones:

- Control de Calidad de Hardware: Verificación de que los equipos instalados coincidan con las fichas técnicas propuestas (ej. verificar que el cable sea Cobre Puro y no CCA).
- Pruebas de Aceptación (FAT/SAT):
 - *Prueba de Anti-Suplantación*: Intentar ingresar usando una fotografía o video en celular frente a la cámara (el sistema debe rechazarlo).
 - *Prueba de Fuga de Activos*: Intentar sacar un equipo etiquetado oculto en una mochila (el sistema debe activar la alarma).
- Validación de Código: Revisión de que el software cumpla con estándares de seguridad (encriptación de vectores faciales y contraseñas).

13. RESPONSABILIDAD POR VICIOS OCULTOS

13.1 Definición de vicios ocultos

Se consideran vicios ocultos a aquellos defectos físicos en la instalación (cableado, anclajes) o lógicos en el software (bugs, fallos de seguridad no detectados) que no pudieron ser advertidos en el momento de la recepción del proyecto, pero que afectan su funcionamiento o vida útil.

13.2 Responsabilidad del contratista

El equipo desarrollador/contratista asume la plena responsabilidad por la calidad de los equipos y la estabilidad del software. Esta responsabilidad incluye la reparación, reemplazo o corrección del defecto sin costo alguno para la Universidad.

13.3 Procedimiento de reclamación

La Universidad notificará por escrito al contratista sobre el vicio oculto detectado. El contratista tendrá un plazo máximo de 72 horas para presentar un plan de corrección y no más de 7 días calendario para subsanar el fallo.

13.4 Consecuencias del incumplimiento

El no levantamiento de las observaciones por vicios ocultos habilitará a la Universidad a ejecutar las cartas fianza o garantías retenidas, y a inhabilitar al proveedor para futuros proyectos.

14. CARACTERÍSTICAS TÉCNICAS DEL SISTEMA

Este apartado detalla los requerimientos mínimos obligatorios para garantizar la funcionalidad descrita en la arquitectura:

14.1 Sistema de Videovigilancia y Biometría

- Cámaras IP: Resolución mínima 2MP (4K), Lente varifocal motorizado o fijo de 6mm, WDR 120dB (Hardware Real), Compresión H.265+, Soporte nativo de API/SDK para integración.
- Servidor de Procesamiento: Procesador Intel i7/i9 o equivalente, mínimo 32GB RAM, GPU dedicada (NVIDIA RTX 3060 o superior con núcleos Tensor) para aceleración de IA, Almacenamiento SSD NVMe para sistema y HDD Grado Vigilancia para logs.

14.2 Sistema de Seguridad de Activos (RFID)

- Lector/Antenas: Frecuencia UHF 902-928 MHz (Región Perú), Protocolo EPC Gen2 (ISO 18000-6C), Conectividad Ethernet TCP/IP, Ganancia de antena > 8dBi, Polarización Circular.
- Etiquetas (Tags): Tipo pasivo. Para equipos de cómputo: Tags Anti-Metal (ABS/Foam). Para mobiliario: Inlays adhesivos estándar.

14.3 Infraestructura de Red

- Cableado: Categoría 6 o 6A, conductor 100% Cobre sólido, chaqueta LSZH (baja emisión de humos).
- Switching: Switch Gigabit con soporte PoE+ (802.3at) en todos los puertos, presupuesto de potencia (Power Budget) suficiente para alimentar todas las cámaras y lectores simultáneamente.

14.4 Seguridad Perimetral y Acceso

- Sensores Ventana: Contacto magnético de montaje superficial, gap operativo > 20mm.
- Controlador Lógico Programable: Modelo tipo PLC compacto 14 I/O, alimentación 24 V DC, con ~14 entradas digitales para sensores y ~10–14 salidas digitales compatibles con relés para controlar cerraduras y alarmas, soporta módulos de expansión para agregar más E/S, comunicación Ethernet/Modbus para integrar cámaras y servidores, ciclo de escaneo rápido para control en tiempo real y montaje en riel DIN o gabinete de control.
- Relé: Módulo de relé con bobina 24 V DC, contactos capaces de manejar 12 V o 24 V DC hasta 10 A, activación mediante salida de PLC
- Cerradura Eléctrica: Modelo tipo embutir, compatible con alimentación 12 V o 24 V DC

15. PLAZOS DE EJECUCIÓN

El plazo total para la implementación del proyecto "EduSecure" es de sesenta (60) días calendario, contabilizados a partir del día siguiente de la firma del contrato y la entrega del adelanto directo.

- Días 1-15: Fases 1 y 2 (Diagnóstico y Compras).
- Días 16-45: Fases 3 y 4 (Instalación y Desarrollo).
- Días 46-60: Fase 5 (Pruebas finales, capacitación y cierre).

16. VALOR REFERENCIAL

El valor referencial del proyecto incluye todos los costos directos (hardware, licencias, materiales), costos indirectos (transporte, personal técnico), gastos generales y utilidad. El presupuesto se desglosa en:

1. Equipamiento Tecnológico (Hardware): S/.
2. Desarrollo de Software e Integración: S/.
3. Materiales de Instalación e Infraestructura: S/.

4. Servicios de Mano de Obra y Capacitación: S/.

17. EXPERIENCIA DEL POSTOR

El equipo técnico o empresa postora deberá acreditar experiencia en:

- Capacidad Técnica: Haber implementado al menos un (01) proyecto de seguridad electrónica, desarrollo de software con IA o cableado estructurado en los últimos 2 años.
- Personal Clave: Contar en su equipo con al menos un Ingeniero de Sistemas/Electrónico y un técnico certificado en cableado estructurado.

18. RESPONSABILIDAD DEL CONTRATISTA

El contratista es el único responsable ante la Universidad por la correcta ejecución del servicio, la calidad de los materiales y equipos suministrados, y la idoneidad del personal técnico. Asimismo, es responsable de cumplir con las normas de Seguridad y Salud en el Trabajo durante la fase de instalación física en los laboratorios.

19. CONSIDERACIONES FINALES

El proyecto EduSecure representa un salto tecnológico necesario hacia la modernización universitaria. Su éxito no solo depende de la tecnología instalada, sino de la apropiación del sistema por parte de la comunidad académica. Por ello, se enfatiza la importancia de la fase de capacitación y el soporte post-implementación para garantizar la sostenibilidad de la inversión.

ANEXOS

1. Centro de Datos

Este es el núcleo del sistema encargado de procesar por medio de Inteligencia Artificial el ingreso a un aula o laboratorio.

Ítem	Especificación Técnica Recomendada	Función
Servidor de Procesamiento (GPU)	Proc: Intel i7/i9, RAM: 32GB+, GPU: NVIDIA RTX 3060+ (Mínimo 6GB VRAM).	Ejecuta los códigos de Python (FaceNet/MediaPipe) para reconocer rostros en tiempo real.
Almacenamiento (HDD + SSD)	1x SSD NVMe (Sistema Operativo) + 2x HDD 4TB "Purple/Skyhawk" (Video).	SSD para velocidad del software. HDD grado vigilancia para grabar las clases (evidencia).
Switch PoE+ (Gigabit)	De 24 o 48 puertos (necesitarás varios según el nro. de aulas). Standard IEEE 802.3at.	Alimenta de energía y datos a todas las cámaras y terminales faciales por un solo cable.

Rack de Comunicaciones	Gabinete de piso o pared (ej. 12RU o 24RU).	Para ordenar el servidor, switches y organizadores de cables.
UPS (Respaldo de Energía)	Online o Interactivo (ej. 2KVA o 3KVA).	Mantiene el sistema vivo si se va la luz y protege contra picos de voltaje.

1.1 Servidor de Procesamiento (GPU)

1.2 Almacenamiento (HDD + SSD)

1.3 Switch PoE+ (Gigabit)

1.4 Rack de Comunicaciones

1.5 UPS (Respaldo de Energía)

2. Aulas y Laboratorios

Ítem	Especificación	Función

Terminal de Reconocimiento Facial	Tipo Hikvision MinMoe o ZKTeco SpeedFace. IP65.	Acceso Docente. Va en la pared exterior. Escanea la cara y manda la señal al servidor. Reemplaza a la Rav Bariach T7.
Cerradura Electromagnética (Maglock)	Fuerza de sujeción 600lbs (280kg).	Mantiene la puerta cerrada físicamente. Se abre cuando el Terminal Facial corta la energía.
Botón "Push to Exit"	Botón físico (verde/acero).	Salida. Permite a los alumnos salir del aula libremente (seguridad civil).
Cámara IP Domo	Resolución 4MP u 8MP, Lente 2.8mm, PoE ³ .	Asistencia. Va en la esquina interior del aula mirando a los alumnos.
Caja de paso / Roseta	PVC o Metal 10x10.	Para guardar las conexiones detrás de la cámara y el terminal.

3. Seguridad Antirrobo (Laboratorios y Salida Principal)

Ítem	Especificación	Función
Antenas/Arcos RFID UHF	Frecuencia 902-928 MHz (Estándar Perú/USA).	Se colocan en la salida principal (Piso 1) y puertas de Labs críticos. Detectan si sale un equipo.
Lector RFID (Controller)	Si la antena no lo trae integrado, se necesita un lector de 4 puertos.	Procesa la señal de las antenas y avisa al servidor si hay un robo.
Etiquetas (Tags) RFID	"Anti-Metal Tags" (Espuma/ABS) ⁵ .	Se pegan en las computadoras y proyectores. Si no son anti-metal, no funcionarán pegados al chasis de la PC.
Sirena Estroboscópica	12V, Luz Roja + Sonido.	Suena si alguien intenta sacar un equipo sin autorización.

4. Infraestructura y Cableado

Ítem	Especificación	Función
Bobinas de Cable UTP	Categoría 6 (Cat6), 100% Cobre (No usar CCA/Aleación) ⁶ .	Transmisión de datos y energía (PoE). Necesitarás varias cajas de 305mts.
Patch Cords	Cat6 Certificados (de 1m y 3m).	Para conectar el servidor al switch y las cámaras a la pared.
Jacks RJ45 y Faceplates	Cat6.	Las tomas de red en la pared.
Canaletas / Tubería	PVC o EMT (Metal) según norma de la universidad.	Para proteger y ocultar los cables que viajan por pasillos y techos.
Organizadores de Cables	Horizontales y Verticales (para el Rack).	Para que el cuarto de servidores se vea ordenado y profesional.

5. Seguridad Perimetral (Primer Piso)

Ítem	Especificación	Función
Sensores Magnéticos	De sobreponer (blancos) o pesados (metal) para ventanas.	Detectan si abren una ventana.
Sensores de Ruptura (Opcional)	Discriminador de audio.	Detectan si rompen el vidrio.
Panel de Alarma / Expansora	O un módulo de entradas I/O para el servidor.	Recibe la señal de los sensores de ventana.

6. Software y Lógica

Ítem	Detalle
Sistema Operativo	Linux (Ubuntu Server) recomendado para estabilidad y costo, o Windows 10/11 Pro.

Librerías Python	OpenCV, FaceNet (o DeepFace), TensorFlow, PyTorch ⁹ .
Base de Datos	PostgreSQL o MySQL (para guardar asistencias y usuarios).
Dashboard Web	React/Vue/Angular (Frontend) + Flask/Django/FastAPI (Backend) para ver los reportes.

7. Cámaras de Reconocimiento Facial

Característica Técnica	Especificación Requerida (Proyecto EduSecure)	Opción A	Opción B	Opción C	Descripción
Marca / Modelo	(Definir modelo exacto)	Cámara Hikvision tubo IP DS-2CD1643G 2-LIZU 4MP, dual light, IR	Hanwha Wisenet QND-6082R	DS-2CE17D0T-LX TS 2MP Two-Way Audio & Siren Fixed Bullet Camera	

		30 metros, blanco			
Imagen Referencial					
Resolución	2 – 8 Megapíxeles (1080p, 2K o 4K)	4 MP resolution	2 MP (1920 × 1080)	2 MP CMOS	Indica la cantidad de detalle de imagen. A mayor resolución, mejor precisión facial y evidencia.
Lente (Distancia Focal)	≈ 6 mm (Fija o Varifocal)	Lente: 2,8 a 12 mm	Varifocal 3.2 – 10 mm (incluye ~6mm)	2.8 mm, 3.6 mm fixed lens	Determina cuánto se acerca o aleja la imagen. Varifocal permite ajustar zoom y encuadre.

Visión Nocturna	IR + Modo Día/Noche (Automático)	IR, White Light	IR 20 m + ICR automático	IR: Up to 40 m, White Light: Up to 40 m	La cámara debe ver bien en oscuridad. Dual-light mejora color nocturno.
Iluminación Mínima	$\leq 0.01 \text{ Lux (Color) / 0 Lux con IR activado}$	Color: 0.005 Lux @ (F1.6, AGC ON), B/W: 0 Lux with IR	0.095 Lux (Color), 0 Lux IR ON	0.01 Lux @(F1.6, AGC ON), 0 Lux with White Light	Lux mide cuánta luz necesita la cámara para ver. Valores bajos = mejor en poca luz.
Compresión de Video	H.265 / H.265+ (Prioritario para ahorro)	Main stream: H.265+/H.265 / H.264+/H.264, Sub-stream: H.265/H.264/ MJPEG	H.265 / H.264 / MJPEG + WiseStream II	No cuenta	Reduce ancho de banda. H.265+ permite almacenar más días con menos espacio.
Alimentación / Interfaz	PoE (Power over Ethernet) 802.3af	PoE: IEEE 802.3af, Class 3, max. 12 W	PoE IEEE 802.3af / 12V DC	12 VDC $\pm 25\%$, max. 9.9 W	PoE simplifica instalación y reduce cableado. C no es compatible con red IP.

Protección (IP/IK)	IP5X o IP6X (IP67 recomendado para ext.)	IP67: IEC 60529-2013	IP66	IP67	IP67 permite uso en exteriores o ambientes expuestos a polvo/lluvia.
WDR (Rango Dinámico)	120 dB (Necesario para contraluz en puertas)	120 dB	120 dB WDR real	Digital WDR(<i>NO llega a 120 dB</i>)	WDR mejora calidad en contraluz (puertas, ventanas). WDR digital es inferior.
Inteligencia Artificial	Detección Facial / Cruce de línea	Support Human and Vehicle Detection	Analíticas: línea virtual, intrusión, defocus, tampering, enter/exit, movimiento	NO tiene IA	IA reduce falsas alarmas y mejora reconocimiento.
Audio	Micrófono Integrado (Opcional según zona)	Mono sound	Micrófono integrado	Echo Cancellation, AI Noise Reduction, Automatic Gain Control	Útil para auditoría, disuasión y supervisión activa.

Costo Unitario	S/.	S/560.56	S/.1,150,00	S/.105,00	Precio referencial. La opción C es barata pero no cumple requisitos del proyecto.
Url		https://www.colbox.pe/camaras-hikvision-tubo-ip-ds-2cd1643g2-lizu-4mp-dual-light-ir-30mts-blanco-100430278/p?idsku=10054060&gad_source=1&gad_campaignid=20892322506&gbraiding=0AAAAACorML6ktzeA-NA3sHmDC1VBp_T7t&gclid=CjwKCAiA55rJBhByEiwAFkY1QJn1Frbl4BCIxXCe5dF8v9pI	https://smartbusiness.pe/collections/todos-los-productos/product/hanwha-camara-ip-domo-para-interiores-qnd-6082r-alambrico-1920-x-1080-pixeles-dia-noche?_pos=1&_sid=58bbde6ad&_ss=r	https://www.coolbox.pe/tubo-hikvision-2mp-colorvu-con-audio--hk-ds2ce10df0-lpfs-blanco-100431718/p?idsku=10055475&gad_source=1&gad_campaignid=20892322506&gbraiding=0AAAAACorML6ktzeA-NA3sHmDC1VBp_T7t&gclid=CjwKCAiA55rJBhByEiwAFkY1QDfbcgAK2KSo0NdLp8HuKBtPjW58pfHVgU-BRZSErE3XMI4X57uoXBoCAxQAvD_BwE	

		NjBWeIUA6x Ys4lH2bS56w k5ClXwPGho COIQQAvD_B wE			
--	--	---	--	--	--

8. Infraestructura de Red y Cableado (Soporte PoE)

Material / Componente	Especificación Técnica Crítica	Marca / Modelo Seleccionado	URL	Cantidad Estimada	Costo Unit.
Cable de Red (Bobina)	Cat 6, 100% Cobre (No CCA), Calibre 23/24 AWG	Ubiquiti Cat6	https://sodimac.falabellacom.pe/sodimac-pe/product/144359207/Cable-Ubiquiti-Cat6-Cmr-305M%C2-Par-Trenzado-23Awg%C2-Cobre-Solido%C2-Color-Blanco-	1 und.	S/ 1,209.00

			Alta-Veloci/144359208 ?exp=sodimac		
Conectores (Jacks/Plugs)	RJ45 Cat 6	Jack Keystone Panduit CJ6X88TGBL	https://www.maia.com.pe/producto/jack-rj45-categoria-cat6a-cj6x88tgb-panduit	12 unidades	S/ 38.00
Switch PoE	Gigabit, Estándar IEEE 802.3af/at, Budget >120W	TP-LINK TL-SG108PE 8 Puertos Gigabit PoE Switch	https://maptechperu.com/producto/switch-tp-link-8ptos-4poe-10-100-1000-admi-tl-sg108pe	1 und.	S/ 210.00
Patch Cord	Cat 6 Certificado (Para conexión en rack)	Furukawa / LTT / LTT-PC6A	https://www.sodimac.com.pe/sodimac-pe/articulo/143321175/Cable-Patch-Cord-Dixon-3-Metro-UTP-Cat.-6-24-AWG-COBRE-LSZH-RoHS-Negro/143321176	5 und.	S/ 19.00

Tubería / Canaleta	PVC o EMT (Según sea pared o techo)	Canaleta PVC (tipo Nicoll)	https://modulos.sodima.com.pe/sodimac-pe/product/2053381/Cable-UTP-CAT6-por-Metro-Lineal	30 und.	S/ 4.50
--------------------	-------------------------------------	----------------------------	---	---------	---------

9. Sensores de Ventana y Cerraduras

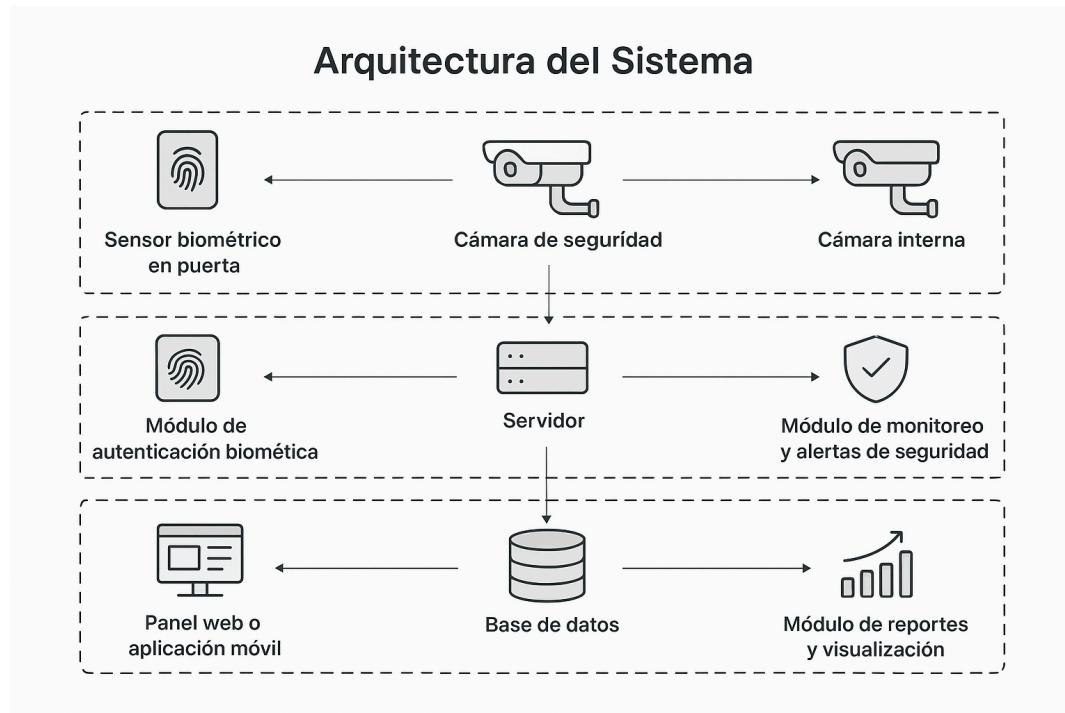
Zona / Ubicación	Dispositivo Requerido	Función Específica	Cantidad	Especificación Técnica Crítica	Opción A	Opción B	Costo Unit. Est. (S.)	Costo Total (S.)
ACTIVO S (Equipos)	Tag RFID Anti-Metal	Etiqueta para pegar en CPUs, Proyectores y Monitores.	(Total de equipos)	UHF (860-960 MHz), Material ABS o Espuma (Para que funcione sobre metal).	Confidex Silverline / Zebra on-metal	Tag UHF Genérico ABS Anti-metal		

ACTIVOS (Mobiliario)	Tag RFID Estándar	Etiqueta adhesiva para sillas, mesas (madera/plástico).	<i>(Total de muebles)</i>	UHF Pasivo, Papel o PET.	Smartrac DogBone / Zebra	<i>Etiqueta RFID Inlay Genérica</i>		
PUERTA (Salida)	Antena / Portal RFID	Detectar los tags al pasar por el marco de la puerta.	1 Kit (2 Antenas)	Ganancia > 8dBi, Polarización Circular (Detecta en cualquier posición).	Zebra FX9600 + Antenas AN440	<i>Portal UHF Integrado (Chino/Genérico)</i>		
PUERTA (Salida)	Lector RFID (Controlador)	"Cerebro" que procesa la lectura y activa la alarma.	1	Protocolo EPC Gen2, Conexión TCP/IP para la red.	<i>(Incluido en Opción A)</i>	<i>(Integrado en el portal)</i>		

AULA (General)	Sirena Estroboscó pica	Sonido y luz fuerte cuando se detecta una salida no autorizad a.	1	12V, >100dB, Luz Roja.	<i>Hagroy / Opalux</i>	<i>Genérica 12V</i>		
VENTAN AS	Sensor Magnético	Detectar si abren la hoja de la ventana.	(Nro. de hojas)	Montaje superficial, conexión cableada o inalámbrica.	<i>Hikvision DS-PD1-M C (Inalámbrico)</i>	<i>Hagroy Magnético Cableado (Pesado)</i>		
VENTAN AS	Sensor de Ruptura	Detectar si rompen el vidrio.	(Nro. de vidrios)	Discriminador de audio o vibración.	<i>DSC Acuity / Honeywell</i>	<i>Sensor Vibración Genérico</i>		
SOFTWA RE	Middleware de Gestión	Base de datos que dice "Este	1 Licenci a	Integración con Base de Datos	<i>Desarrollo Propio</i>	<i>Software del Fabricante</i>		

		proyector NO puede salir".		SQL, Alertas en Pantalla.	(Python/S DK)			
--	--	-------------------------------------	--	------------------------------	------------------	--	--	--

Descripción



Ventajas para EduSecure:

- Precisión AcuSense:** Filtra hasta 90% de falsas alarmas, detectando solo personas y vehículos
- Alta resolución:** 4K permite identificación facial clara a distancia
- Visión nocturna avanzada:** Funciona 24/7 en cualquier condición de luz
- Integración ONVIF:** Compatible con cerradura T7 y sistemas de gestión

5. **Almacenamiento dual:** Local (microSD) y NVR para redundancia
6. **Sopporte local:** Disponible en Perú con garantía y asistencia técnica

Proveedor y Precio:

Proveedor: ARTEUS Perú

Link: [ENLACE: <https://arteus.pe/products/hikvision-ds-2cd2083g2-iu>]

Precio: S/. 551.00 PEN (por unidad)

Disponibilidad: En stock, envío nacional



Imagen 1. Logotipo del Sistema Edu Secure

USO DE JIRA Y METODOLOGÍA KANBAN

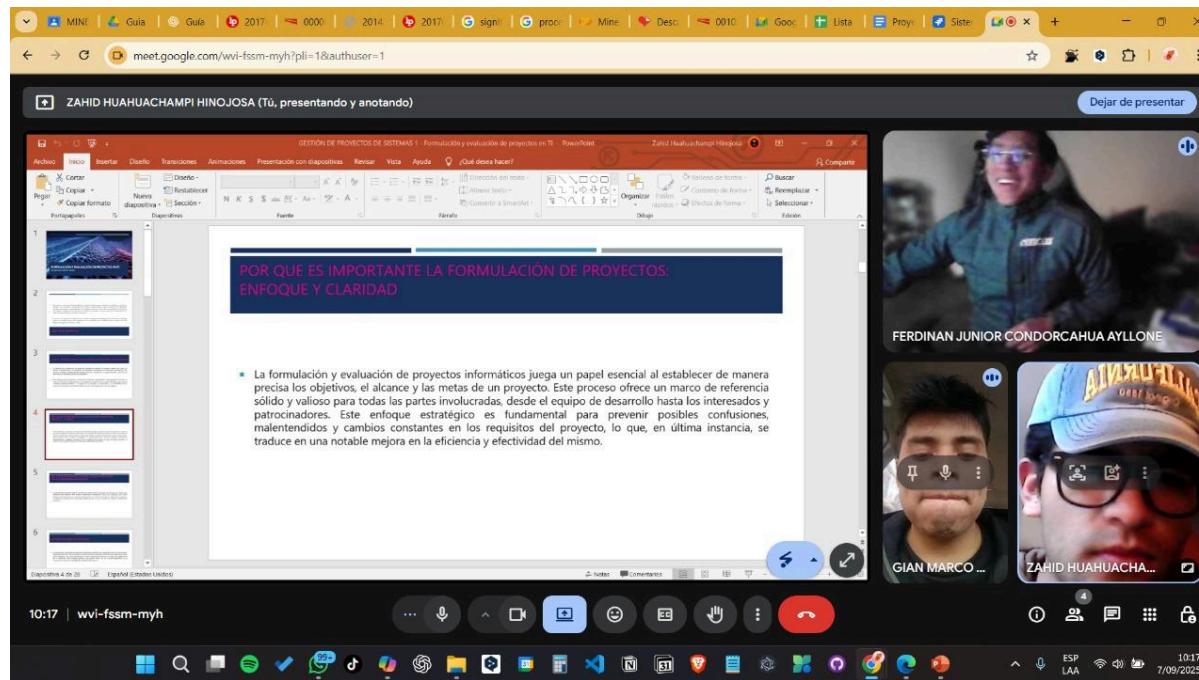


Imagen 2. Captura de sesiones grupales vía Google Meet

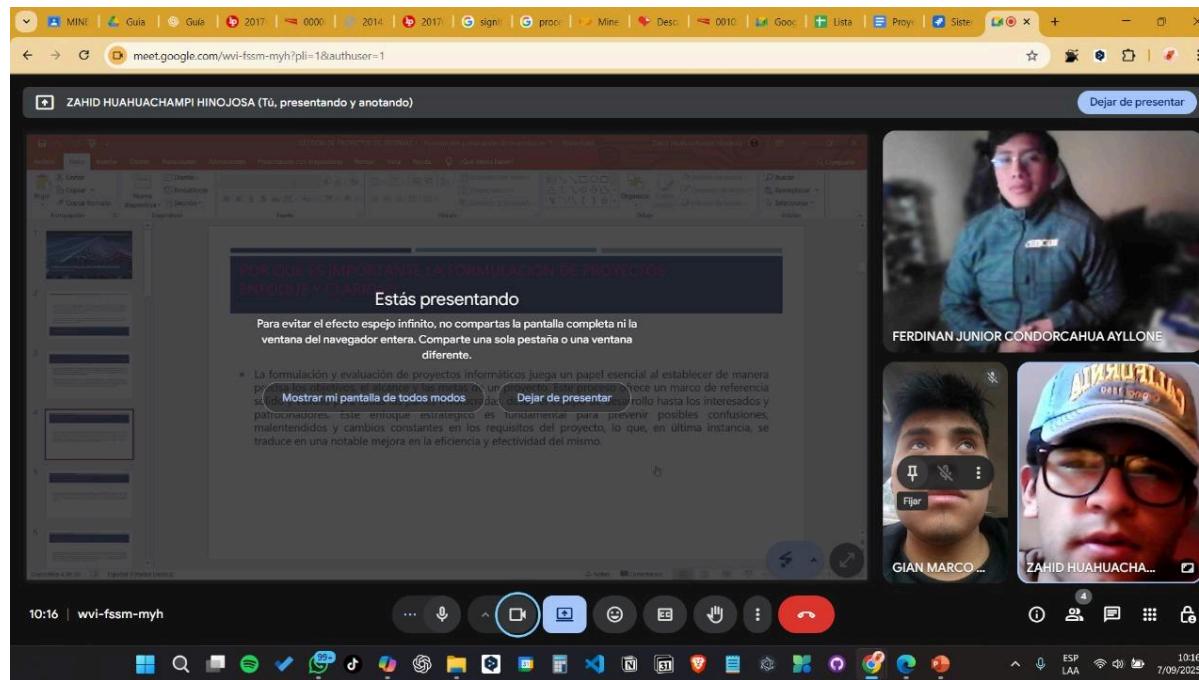


Imagen 3. Captura de sesiones grupales vía Google Meet

Kanban

Usar plantilla X

Kanban (palabra japonesa que significa "señal visual") es un sistema centrado en ayudar a los equipos a visualizar su trabajo, limitar el trabajo en curso y maximizar la eficacia. Utiliza la plantilla de kanban para aumentar la flexibilidad de planificación, reducir los cuellos de botella y fomentar la transparencia a lo largo del ciclo de desarrollo.



Supervisa el trabajo mediante un tablero sencillo

Los elementos de trabajo se representan visualmente en el tablero de kanban, lo que les permite realizar un seguimiento del estado del trabajo en cualquier momento. Las columnas de tu tablero representan cada paso del flujo de trabajo del equipo, desde lo que hay pendiente hasta lo que está hecho.

[Más información sobre los tableros de kanban](#)

Usa el tablero para limitar el trabajo en curso

Establece la cantidad máxima de trabajo que puede haber en cada estado mediante límites de trabajo en curso (WIP). Al limitar el trabajo en curso, puedes mejorar el enfoque del equipo e identificar mejor las



Producto



Recomendado para

Equipos que controlan el volumen de trabajo desde un backlog

Equipos de DevOps que quieran conectar el trabajo en todas sus herramientas

Tipos de actividad

- Epic
- Historia
- Error
- Tarea
- Subtarea

Flujo de trabajo

PENDIENTE

Siguiente: selecciona un tipo de proyecto

Usar plantilla

Imagen 4. Elección del modelo Kanban en Jira

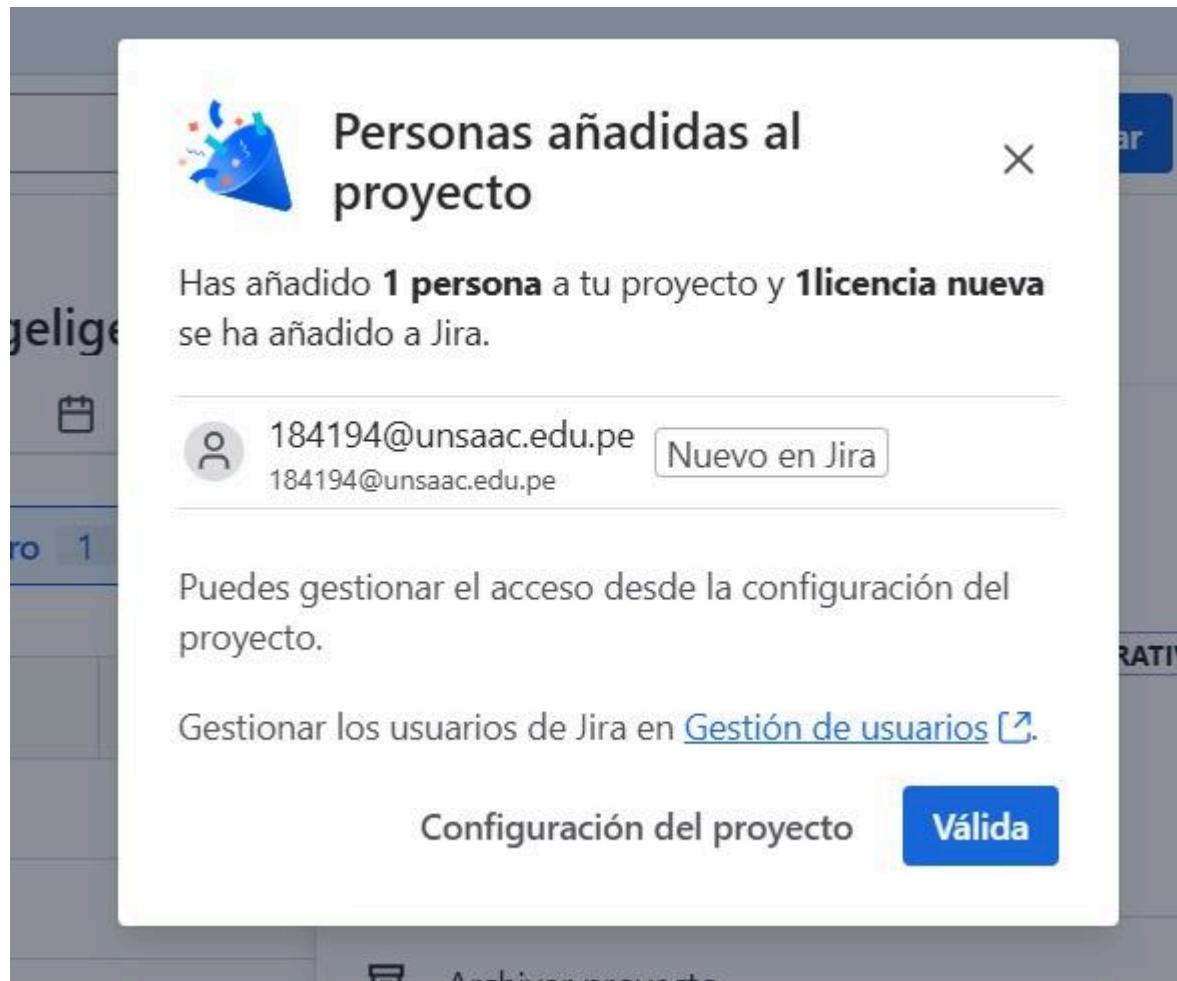


Imagen 5. Agregación de participantes al proyecto en Jira

The screenshot shows the Jira software interface. On the left is a sidebar with navigation links: Para ti, Recientes, Marcados como favorito, Aplicaciones, Planes, Proyectos, Recientes, EduSecure: Plataforma d..., Sistemas de Seguridad l..., Más proyectos, Equipos, Confluence, and Más. The main area is titled 'Proyectos' and shows a 'Tablero' (Dashboard) for 'EduSecure: Plataforma de Control de Acceso, Asistencia y Seguridad Académica'. The dashboard has three columns: 'POR HACER' (7 items), 'EN CURSO' (8 items), and 'LISTO' (0 items). A search bar at the top says 'Buscar tablero' and there are filter options. At the bottom right of the dashboard is a 'Quickstart' button.

Imagen 6. Creación del proyecto en Jira

This screenshot shows the same Jira interface as above, but with more detailed task information visible in the 'EN CURSO' column. The tasks listed are:

- Diseñar Arquitectura técnica del sistema (EPDCAAYSA-1)
- Definir requerimientos funcionales (EPDCAAYSA-2)
- Coordinar integración con Jira (EPDCAAYSA-3)
- Validar fuentes y referencias (EPDCAAYSA-4)
- Investigar marco legal peruano sobre reconocimiento facial (EPDCAAYSA-5)
- Redactar propuestas de solución (EPDCAAYSA-6)
- Coordinar reuniones meet (EPDCAAYSA-7)
- Buscar casos internacionales similares (EPDCAAYSA-10)

Each task has a status indicator (ZH or GM) and a small circular icon next to it. The 'Quickstart' button is also present at the bottom right.

Imagen 7. Jira incorporación de tareas y designaciones en el grupo

<https://formulaciondeprojec.atlassian.net/jira/software/projects/EPDCAAYSA/boards/34>

https://www.canva.com/design/DAGylHbCPJY/jDWEkYvweCDctOjoszw3Mw/edit?utm_content=DAGylHbCPJY&utm_campaign=designshare&utm_medium=link2&utm_source=sharebutton



Imagen 12. Simulación del quitado de rejas en la puerta y posible ubicación de cámara de seguridad incorporada

Ley de protección de datos personales

<https://cdn.www.gob.pe/uploads/document/file/272360/Ley%20N%C2%BA%202029733.pdf.pdf?v=1618338779>

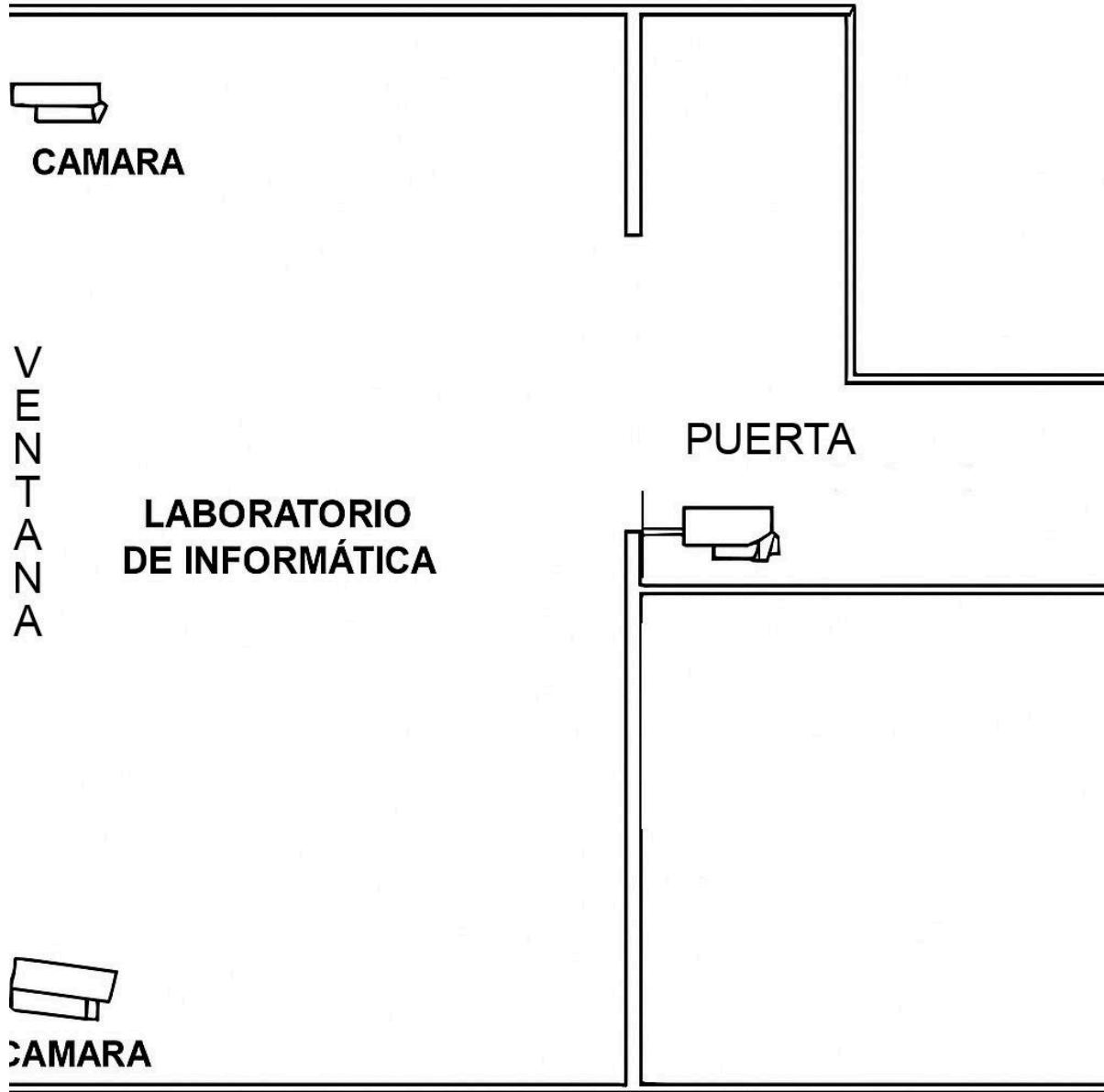


Imagen 13. Plano Referencial de el posicionamiento de las cámaras

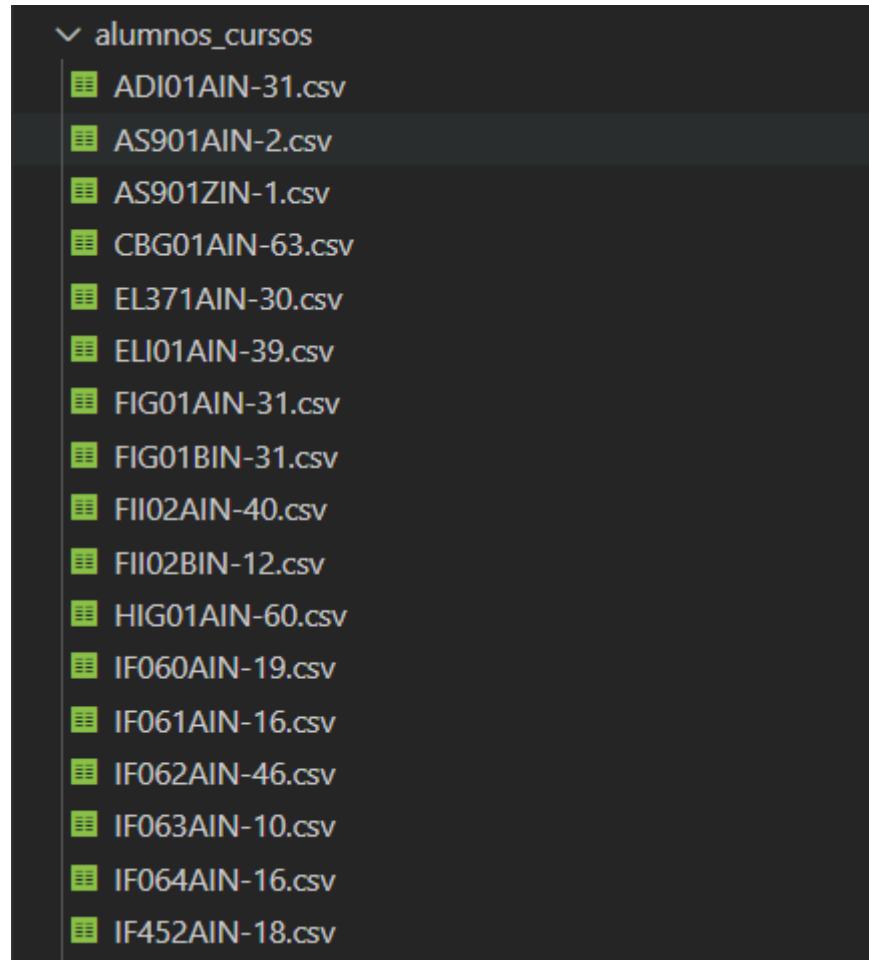


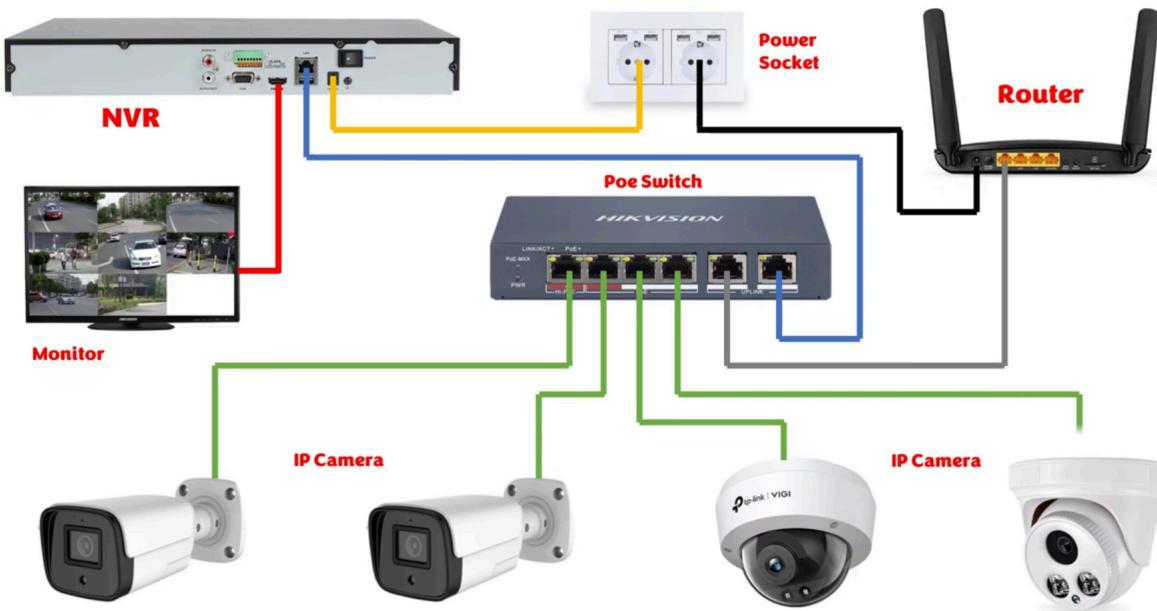
Imagen 14 Resultado del uso de Web Scraping para la obtención de datos de alumnos matriculados.

	CodigoCurso,Nro,Codigo-Alumno,Nombre
1	IF483AIN,1,174905,AGUILAR-MAINICTA-GIAN MARCO
2	IF483AIN,2,215270,ALEGRIA-SALLO-DANIEL
3	IF483AIN,3,210920,BUENO-LESCANO-ANDRIC JEREMY
4	IF483AIN,4,211959,CCASA-POCOHUANCA-LUDVIKA ARLETH
5	IF483AIN,5,193109,COLQUE-GALINDO-JEAN FRANCO
6	IF483AIN,6,141664,CONDE-PADIN-GEORGE ADOLFO
7	IF483AIN,7,215783,CONDE-SALLO-JOHAN MIHAIL
8	IF483AIN,8,184194,CONDORCAHUA-AYLLONE-FERDINAN JUNIOR
9	IF483AIN,9,215784,CRUZ-YUCRA-LUCERO ESMERALDA
10	IF483AIN,10,211855,HUACHO-CRUZ-DAVID ALI
11	IF483AIN,11,200878,HUAHUACHAMPI-HINOJOSA-ZAHID
12	IF483AIN,12,171676,HUAMAN-AYMA-DERLY HAYLEY
13	IF483AIN,13,183067,HUAYLLA-HUILLCA-ROSSBEL
14	IF483AIN,14,215278,HUISA-MAMANI-JUAN GABRIEL
15	IF483AIN,15,211857,HUISA-NINA-YIMY YOHEL
16	IF483AIN,16,211311,MAYTA-TTITO-WILL EDSON
17	IF483AIN,17,164244,MOLOCHO-CONDORI-BRAYAN VLADYMIR
18	IF483AIN,18,110071,MUNIVE-SALAS-CIRO
19	IF483AIN,19,210179,PRIETO-CARDOSO-DAVID FERNANDO
20	IF483AIN,20,204805,PUMACAHUA-CUSIHUAMAN--CHRISTIAN
21	IF483AIN,21,210940,PUMACHOQUE-CHOQUENAIRA-JHON ESAU
22	IF483AIN,22,211862,QUISPE-ARQUE-ETNER YURY
23	IF483AIN,23,200858,QUISPE-CONDORI-MANUEL EDUARDO
24	IF483AIN,24,215422,QUISPE-MACHACA-JHON JESUS
25	IF483AIN,25,200340,QUISPE-TAYÑA-JOSE LUIS
26	IF483AIN,26,211359,QUISPE-VENTURA-IAN LOGAN WILL
27	IF483AIN,27,210441,RAMOS-ALMIREZ-TEMEL SERGIO

Imagen 14. Ejemplo de excel con datos de alumnos y cursos.

Del diseño, arquitectura e implementación

Primera propuesta.-



Segunda propuesta.-

Comparativa Técnica: Propuesta Original vs. Nueva Propuesta EduSecure

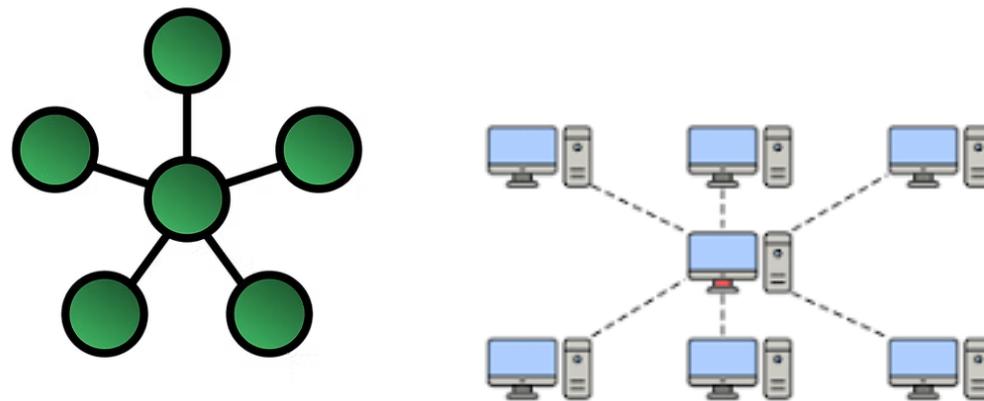
Componente / Sección	Propuesta Anterior (Borrador)	Nueva Propuesta (Ingeniería)	¿Por qué el cambio? (Justificación Técnica)

1. Control de Acceso (Docentes)	Cerradura Inteligente "All-in-One" (Rav Bariach T7) <i>Sistema aislado a baterías.</i>	Terminal Facial IP + Electroimán <i>Sistema cableado PoE.</i>	Centralización: La T7 procesa el rostro en la puerta y no envía video al servidor. El Terminal IP envía la data al servidor Edge, cumpliendo con el requisito de que tu código Python gestione el acceso.
2. Mecanismo de Cierre	Pestillo Motorizado a Baterías Depende de pilas AA/Recargables.	Cerradura Electromagnética (Maglock) Alimentación eléctrica continua.	Seguridad y Mantenimiento: Las baterías fallan y requieren cambio manual. El electroimán se alimenta de la red eléctrica (con respaldo UPS) y se puede abrir remotamente desde el servidor en caso de emergencia.

3. Cámara de Asistencia (Alumnos)	Ubicación Cenital / Central Implícito en diseño estándar. Mira hacia abajo (top-down).	Ubicación Esquina Frontal Mira en diagonal hacia los rostros.	Eficacia del Algoritmo: La vista cenital solo ve cabezas/pelo ("coronillas"). Para que FaceNet/MediaPipe funcionen, necesitan ver ojos, nariz y boca. La esquina frontal captura el rostro natural de los alumnos mirando al profesor.
4. Infraestructura de Red	Híbrida / WiFi La cerradura T7 usa WiFi/Bluetooth.	Cableado Estructurado (Cat6) Todo conectado al Switch PoE.	Estabilidad: El WiFi puede saturarse o bloquearse. Un cable UTP garantiza que el video de 8MP llegue al servidor sin latencia para el procesamiento en tiempo real.

Estructura de red de topología estrella.-

Estructura de red de tipo estrella



Resumen de ambientes por nivel y requerimientos

Nivel / Piso	Ala Izquierda (Oeste)	Ala Derecha (Este)	Zona Central / Servicios	Total Dispositivos Estimados

1º Nivel	4 Laboratorios <i>(Ingreso)</i> <i>(Requieren RFID en puerta + Cámara + Terminal)</i>	4 Aulas Teóricas <i>(Cámara + Terminal)</i>	<ul style="list-style-type: none"> • Escaleras / Ascensor • Baños • 2 Oficinas Admin. 	<ul style="list-style-type: none"> • 8 Terminales Faciales • 8 Cámaras Aulas • 4 Kits RFID (Labs) • Arcos Salida Principal
2º Nivel	4 Aulas/Labs <i>(Servidor)</i> <i>(Cámara + Terminal)</i>	Biblioteca / Sala de Estudio <i>(Zona Abierta)</i>	<ul style="list-style-type: none"> • Escaleras / Ascensor • Baños 	<ul style="list-style-type: none"> • 4 Terminales Faciales • 6 Cámaras (4 Aulas + 2 Biblioteca)

		AQUÍ VA EL SERVIDOR	• Cuarto de Data (MDF)	• Rack Principal (Servidor)
3º Nivel <i>(Cómputo)</i>	4 Laboratorios Informática <i>(Alta densidad de PCs)</i> <i>(Requieren RFID)</i>	4 Laboratorios Informática <i>(Alta densidad de PCs)</i> <i>(Requieren RFID)</i>	• Escaleras / Ascensor • Baños	• 8 Terminales Faciales • 8 Cámaras Labs • 8 Kits RFID (Alto Riesgo)
4º Nivel <i>(Admin)</i>	4 Oficinas/Departamentos <i>(Mesas de reunión/escritorios)</i>	Zona Administrativa <i>(Decanato/Secretaría - Espacios con divisiones)</i>	• Escaleras / Ascensor • Baños	• 4 Terminales (Oficinas) • 4 Cámaras (Pasillos/Admin)

				(Menor prioridad)
--	--	--	--	-------------------