Universidad Nacional Experimental de las Telecomunicaciones e Informática.

Trayecto: 2

U.C: Proyecto Socio – Tecnológico

Ingeniería de Requisitos

Integrantes:

Ángel Mujica

Andrea Algarín.

Luis Fernández

Héctor Pacheco. Yuli Delgado.

Celenia León

Profesor

Yuli Delgado.

Definir la aplicación estableciendo para ello: su alcance, sus usuarios directos, sus aspectos claves (servicios que la aplicación debe proveer a los usuarios o la comunidad) y su ámbito de operación.

Alcance

Esta aplicación está diseñada para mejorar la seguridad y el monitoreo de espacios físicos, como hogares, oficinas o almacenes. Su objetivo es proporcionar a los usuarios notificaciones en tiempo real sobre eventos inusuales o intrusiones, y ofrecer un método de acceso seguro y sin contacto mediante reconocimiento facial.

Usuarios Directos

Los usuarios principales de este sistema serían:

- Propietarios de Viviendas: Personas que desean proteger su hogar y sus bienes, recibiendo alertas instantáneas sobre posibles intrusiones o actividades sospechosas.
- Propietarios de Pequeñas y Medianas Empresas: Empresarios que necesitan un sistema de seguridad eficiente y fácil de usar para sus locales comerciales u oficinas.
- Administradores de Espacios Restringidos: Individuos o equipos a cargo de la seguridad y el control de acceso en áreas que requieren protección especial, como laboratorios o depósitos.
- Personas con Movilidad Reducida: Aquellos que se beneficiarían de un sistema de alarma y acceso remoto que no requiera su presencia física constante

Aspectos Clave (Servicios)

Los servicios principales que esta aplicación ofrecería a sus usuarios o a la comunidad son:

- Monitoreo y Detección de Intrusiones:
    - Alertas Inteligentes: El sistema se conectaría con sensores (movimiento, apertura de puertas/ventanas) para detectar actividades sospechosas y enviaría alertas inmediatas.
    - Control Remoto: Los usuarios podrían armar o desarmar la alarma a distancia desde su teléfono.
    - Zonas Personalizables: Sería posible configurar diferentes áreas de monitoreo para una seguridad más detallada.
- Alertas y Notificaciones en Tiempo Real a Través de Telegram:
    - Mensajes Instantáneos: Todas las alertas (ej. sensor activado, intento de acceso no autorizado) se enviarían directamente al chat de Telegram del usuario o de un grupo designado.
    - Información Detallada: Las notificaciones incluirían el tipo de evento, la hora y la ubicación afectada.
    - Integración con Cámaras (Opcional): Si se conecta con cámaras, podría enviar imágenes o videos cortos del evento.

    - Comandos por Telegram: Los usuarios podrían interactuar con la alarma enviando comandos sencillos por Telegram (ej. "armar", "desarmar").
- Acceso con Reconocimiento Facial:
    - Registro de Usuarios: Se registrarían los perfiles de los usuarios autorizados, asociando sus rostros al sistema. ○ Verificación Automática: La aplicación utilizaría el reconocimiento facial para verificar la identidad de quienes intentan acceder. ○ Control de Acceso Integrado: Al reconocer a un usuario autorizado, el sistema podría abrir puertas automáticamente o desactivar la alarma.
    - Registro de Accesos: Mantendría un historial detallado de todos los intentos de acceso, incluyendo la fecha, hora y una imagen del rostro si es posible.
    - Notificaciones de Acceso: Se enviarían alertas a Telegram cada vez que alguien acceda o intente un acceso no autorizado.
- Gestión de Usuarios y Permisos:
    - Perfiles Personalizables: Se podrían definir distintos niveles de acceso para diferentes usuarios (administrador, usuario regular, etc.).
    - Programación de Acceso: Permitiría establecer horarios o días específicos en los que ciertos usuarios tienen permiso para entrar.
- Historial y Registro de Eventos:
    - Log de Actividad: Un registro completo de todos los eventos del sistema (activaciones, accesos, notificaciones) estaría disponible para consulta.
    - Búsqueda y Filtro: Funcionalidades para buscar y filtrar eventos específicos en el historial.

¿Ámbito de Operación

El sistema podría operar en diversos entornos, incluyendo:

- Residencial: Apartamentos, casas y condominios.
- Comercial: Oficinas, pequeñas y medianas empresas, locales comerciales.
- Almacenes y Depósitos: Espacios de almacenamiento de bienes o equipos.
- Puntos de Acceso: Cualquier entrada que requiera un control de acceso seguro y monitoreado.

Identificar, para cada proceso de negocio, los requisitos (requerimientos) funcionales; esto es, qué funciones deberá realizar la aplicación para que los actores puedan ejecutar el proceso.

1. Proceso de Negocio: Monitoreo y Detección de Intrusión

Este proceso asegura la vigilancia constante del área protegida y la identificación de actividades sospechosas.

- RF1.1. Gestión de Sensores: La aplicación debe permitir al usuario agregar, configurar y eliminar diferentes tipos de sensores (ej., movimiento PIR, contacto de puerta/ventana, vibración).
- RF1.2. Activación/Desactivación del Sistema: El sistema debe permitir al usuario activar (armar) y desactivar (desarmar) la alarma de forma remota a través de la aplicación móvil o comandos de Telegram.
- RF1.3. Detección de Eventos: El sistema debe ser capaz de detectar activaciones de sensores y clasificarlas como eventos de seguridad (ej., intrusión detectada, puerta abierta).
- RF1.4. Configuración de Zonas de Monitoreo: La aplicación debe permitir al usuario definir y asignar sensores a diferentes zonas de monitoreo (ej., "Sala de Estar", "Dormitorio Principal", "Acceso Principal").
- RF1.5. Ajuste de Sensibilidad: La aplicación debe permitir al usuario ajustar la sensibilidad de los sensores para minimizar falsas alarmas (ej., nivel de detección de movimiento).
- RF1.6. Estado del Sistema en Tiempo Real: La aplicación debe mostrar el estado actual del sistema (armado/desarmado, estado de los sensores) en tiempo real.

2. Proceso de Negocio: Alertas y Notificaciones en Tiempo Real

Este proceso garantiza que los usuarios sean informados inmediatamente sobre cualquier evento relevante detectado por el sistema.

- RF2.1. Envío de Notificaciones a Telegram: El sistema debe enviar notificaciones instantáneas y detalladas a un chat o grupo de Telegram preconfigurado cuando se detecta un evento (ej., "Intrusión detectada en Sala de Estar - 18:30").
- RF2.2. Personalización de Mensajes de Alerta: La aplicación debe permitir al usuario personalizar el contenido de los mensajes de alerta enviados a Telegram (ej., incluir nombres de zonas, tipos de sensores).
- RF2.3. Envío de Medios (Opcional): Si se integra con cámaras, el sistema debe ser capaz de adjuntar imágenes o clips de video cortos a las notificaciones de Telegram para verificar el evento.
- RF2.4. Comandos Remotos por Telegram: El sistema debe ser capaz de recibir y ejecutar comandos simples enviados a través de Telegram (ej., "desarmar alarma", "solicitar estado").

- RF2.5. Gestión de Destinatarios de Alertas: La aplicación debe permitir al usuario añadir o eliminar destinatarios de Telegram que recibirán las alertas.
- RF2.6. Historial de Notificaciones Enviadas: La aplicación debe mantener un registro de todas las notificaciones enviadas a Telegram, con su estado de entrega.

3. Proceso de Negocio: Acceso con Reconocimiento Facial

Este proceso gestiona el acceso seguro a través de la identificación biométrica.

- RF3.1. Registro de Rostros de Usuarios: La aplicación debe permitir a los administradores registrar y almacenar los patrones faciales de usuarios autorizados, asociándolos a un perfil de usuario único.
- RF3.2. Verificación de Identidad Facial: El sistema debe ser capaz de capturar una imagen del rostro en el punto de acceso y compararla con la base de datos de rostros autorizados para verificar la identidad.
- RF3.3. Concesión de Acceso Automático: Si se verifica la identidad del usuario, el sistema debe desencadenar la apertura de un dispositivo de acceso (ej., cerradura eléctrica, torniquete) o desactivar la alarma en la zona correspondiente.
- RF3.4. Registro de Intentos de Acceso: El sistema debe registrar todos los intentos de acceso, incluyendo la fecha, hora, si fue exitoso o fallido, y, si es posible, una imagen del rostro capturado.
- RF3.5. Notificaciones de Acceso (Exitoso/Fallido): El sistema debe enviar notificaciones a Telegram sobre los intentos de acceso, tanto exitosos (ej., "Acceso concedido a Juan Pérez - Puerta Principal") como fallidos (ej., "Intento de acceso no autorizado detectado - 10:15").
- RF3.6. Gestión de Perfiles Faciales: La aplicación debe permitir a los administradores actualizar o eliminar los patrones faciales de los usuarios.
- RF3.7. Detección de Vidas (Anti-spoofing): (Opcional, pero recomendado para alta seguridad) El sistema debe implementar mecanismos para detectar intentos de suplantación de identidad (ej., uso de fotos o videos).

4. Proceso de Negocio: Gestión de Usuarios y Permisos

Este proceso permite controlar quién tiene acceso al sistema y qué acciones puede realizar.

- RF4.1. Creación y Edición de Perfiles de Usuario: La aplicación debe permitir a un administrador crear, editar y eliminar perfiles de usuario con información relevante (nombre, rol).
- RF4.2. Asignación de Roles y Permisos: La aplicación debe permitir asignar roles a los usuarios (ej., "Administrador", "Usuario Regular") con permisos específicos sobre las funcionalidades del sistema (ej., armar/desarmar, ver historial, añadir usuarios).
- RF4.3. Programación de Acceso por Usuario: La aplicación debe permitir establecer horarios o días específicos en los que un usuario tiene permitido el acceso mediante reconocimiento facial.
- RF4.4. Revocación de Acceso: La aplicación debe permitir revocar de inmediato el acceso de un usuario al sistema o a través del reconocimiento facial.

5. Proceso de Negocio: Historial y Registro de Eventos

Este proceso permite la auditoría y el análisis retrospectivo de la actividad del sistema.

- RF5.1. Registro Detallado de Eventos: El sistema debe registrar de forma persistente todos los eventos significativos, incluyendo activaciones de sensores, cambios de estado del sistema, intentos de acceso (exitosos y fallidos), y notificaciones enviadas.
- RF5.2. Consulta del Historial de Eventos: La aplicación debe permitir al usuario consultar el historial completo de eventos del sistema.
- RF5.3. Filtrado y Búsqueda de Eventos: La aplicación debe proporcionar funcionalidades de filtrado y búsqueda para eventos específicos (ej., por fecha, tipo de evento, zona, usuario).
- RF5.4. Exportación de Registros: La aplicación debe permitir la exportación del historial de eventos en un formato legible (ej., CSV, PDF) para fines de auditoría o respaldo.

Organizar los requisitos: identificarlos, clasificarlos y asignarles prioridades

Clasificación de Prioridades:

- Alta (Obligatorio para MVP): Funcionalidades esenciales que el sistema debe tener para ser operativo y cumplir su propósito principal. Sin ellas, el sistema no es viable.
- Media (Importante para MVP, Mejora Significativa): Funcionalidades que añaden valor considerable y mejoran la usabilidad o seguridad. Son deseables para el MVP, pero el sistema podría operar con limitaciones sin ellas inicialmente.
- Baja (Deseable, Futuras Mejoras): Funcionalidades que añaden comodidad, optimización o características avanzadas. Pueden ser implementadas en fases posteriores del desarrollo.

1. Proceso de Negocio: Monitoreo y Detección de Intrusión

Este es el corazón del sistema de alarma.

- RF1.1. Gestión de Sensores: Permite agregar y configurar sensores.
  - Clasificación: Funcional.
  - Prioridad: Alta.
- RF1.2. Activación/Desactivación del Sistema: Permite armar y desarmar la alarma.
  - Clasificación: Funcional.
  - Prioridad: Alta.
- RF1.3. Detección de Eventos: El sistema debe detectar las activaciones de los sensores.
  - Clasificación: Funcional.
  - Prioridad: Alta.
- RF1.4. Configuración de Zonas de Monitoreo: Permite definir áreas específicas para los sensores.
  - Clasificación: Funcional.
  - Prioridad: Media.
- RF1.5. Ajuste de Sensibilidad: Permite configurar la sensibilidad de los sensores.
  - Clasificación: Funcional.
  - Prioridad: Media.
- RF1.6. Estado del Sistema en Tiempo Real: Muestra el estado actual de la alarma y los sensores. ○ Clasificación: Funcional. ○ Prioridad: Alta.

2. Proceso de Negocio: Alertas y Notificaciones en Tiempo Real

La comunicación es clave para un sistema de alarma.

- RF2.1. Envío de Notificaciones a Telegram: Notificaciones instantáneas y detalladas a Telegram. ○ Clasificación: Funcional. ○ Prioridad: Alta.
- RF2.2. Personalización de Mensajes de Alerta: Permite adaptar el contenido de las alertas.
    - Clasificación: Funcional.
    - Prioridad: Media.
- RF2.3. Envío de Medios (Opcional): Adjunta imágenes/videos a las notificaciones.
    - Clasificación: Funcional.
    - Prioridad: Baja (Requiere integración de cámara, que no es un requisito base para la alarma).
- RF2.4. Comandos Remotos por Telegram: Permite controlar la alarma desde Telegram.
    - Clasificación: Funcional.
    - Prioridad: Alta.
- RF2.5. Gestión de Destinatarios de Alertas: Permite añadir/eliminar quién recibe las alertas.
    - Clasificación: Funcional.
    - Prioridad: Alta.
- RF2.6. Historial de Notificaciones Enviadas: Mantiene un registro de las alertas enviadas.
    - Clasificación: Funcional. ○ Prioridad: Media.

3. Proceso de Negocio: Acceso con Reconocimiento Facial

El componente de seguridad y acceso avanzado del sistema.

- RF3.1. Registro de Rostros de Usuarios: Permite registrar los patrones faciales de usuarios autorizados. ○ Clasificación: Funcional.
    - Prioridad: Alta.
- RF3.2. Verificación de Identidad Facial: El sistema debe verificar la identidad del rostro capturado. ○ Clasificación: Funcional.
    - Prioridad: Alta.
- RF3.3. Concesión de Acceso Automático: Abre el dispositivo de acceso o desarma la alarma si la verificación es exitosa.
    - Clasificación: Funcional.
    - Prioridad: Alta.
- RF3.4. Registro de Intentos de Acceso: Guarda un log de todos los intentos de acceso.
    - Clasificación: Funcional.
    - Prioridad: Media.
- RF3.5. Notificaciones de Acceso (Exitoso/Fallido): Envía alertas a Telegram sobre los intentos de acceso. ○ Clasificación: Funcional.
    - Prioridad: Alta.
- RF3.6. Gestión de Perfiles Faciales: Permite actualizar o eliminar los patrones faciales.
    - Clasificación: Funcional.
    - Prioridad: Media.
- RF3.7. Detección de Vidas (Anti-spoofing): Evita la suplantación de identidad con fotos/videos.
    - Clasificación: Funcional.

- Prioridad: Baja (Importante para seguridad avanzada, pero puede ser una mejora futura para el MVP).

4. Proceso de Negocio: Gestión de Usuarios y Permisos

Fundamental para la administración y control del sistema.

- RF4.1. Creación y Edición de Perfiles de Usuario: Permite gestionar los usuarios del sistema. ○ Clasificación: Funcional.
  - Prioridad: Alta.
- RF4.2. Asignación de Roles y Permisos: Define lo que cada tipo de usuario puede hacer.
  - Clasificación: Funcional.
  - Prioridad: Alta.
- RF4.3. Programación de Acceso por Usuario: Permite establecer horarios de acceso para usuarios. ○ Clasificación: Funcional.
  - Prioridad: Media.
- RF4.4. Revocación de Acceso: Permite eliminar rápidamente el acceso de un usuario.
  - Clasificación: Funcional. ○ Prioridad: Alta.

5. Proceso de Negocio: Historial y Registro de Eventos

Necesario para auditoría y seguimiento.

- RF5.1. Registro Detallado de Eventos: Guarda un registro de todas las actividades importantes. ○ Clasificación: Funcional.
  - Prioridad: Alta.
- RF5.2. Consulta del Historial de Eventos: Permite a los usuarios ver el log de actividades.
  - Clasificación: Funcional.
  - Prioridad: Alta.
- RF5.3. Filtrado y Búsqueda de Eventos: Permite encontrar eventos específicos en el historial.
  - Clasificación: Funcional.
  - Prioridad: Media.
- RF5.4. Exportación de Registros: Permite descargar el historial para auditorías.
  - Clasificación: Funcional. ○ Prioridad: Baja.

Utilizar la plantilla VOLERE o cualquier otra plantilla para documentar los requisitos más importantes.

dentificador del Requisito:	Tipo de Requisito:	Caso de Uso/Evento:
RF1.2	Funcional	Armar Sistema, Desarmar Sistema, Control Remoto

Descripción:

El sistema debe permitir a los usuarios armar (activar) y desarmar (desactivar) la alarma de seguridad de forma remota. Esto se realizará a través de la aplicación móvil dedicada y

también mediante el envío de comandos específicos a un chat de Telegram asociado. Tras la ejecución, el sistema debe enviar una confirmación del cambio de estado al usuario.

Justificación del requisito:

Es fundamental para el control y la gestión remota de la seguridad del espacio. Permite al usuario interactuar con el sistema sin estar físicamente presente, lo cual es crucial para la conveniencia y la respuesta rápida.

Fuente (que interesado lo propone):	Unidad en la que se origina:
Propietarios de Viviendas, Propietarios de Negocios, Administradores.	Usuarios Finales, Seguridad del Hogar/Negocio

Criterios de validación:

- El usuario puede armar el sistema enviando el comando /armar a Telegram y recibe confirmación en <5s.
- El usuario puede desarmar el sistema desde la app móvil y el estado se actualiza en <2s. - El sistema rechaza y notifica intentos de desarmado por usuarios no autorizados.

Grado de satisfacción del interesado:	Grado de insatisfacción del interesado:
Muy Alta (control total y remoto).	Baja (si la funcionalidad no es fiable o lenta).
Dependencias (qué requisitos depende de este):	Conflictos (qué requisitos son incompatibles o

	inconsistentes con este):
- RF1.6 (Estado del Sistema en Tiempo Real) - RF2.4 (Comandos Remotos por Telegram)	N/A
dentificador del Requisito:	Tipo de Requisito: Caso de Uso/Evento:
Documentos de soporte:	Histórico de cambios:
Especificación de Interfaz de Telegram API, Diseño de Interfaz de Usuario de Aplicación Móvil.	1.0 (2025-07-02): Creación inicial.
Proyecto:	Analista:
Sistema de Alerta de Telegram con Acceso Facial	[Tu Nombre]

Exportar a Hojas de cálculo

---

2. Requisito Clave: RF2.1 - Envío de Notificaciones a Telegram

Identificador del Requisito:	Tipo de Requisito:	Caso de Uso/Evento:
RF2.1	Funcional	Alerta de Intrusion, Notificación de Evento de Seguridad

Descripción:

El sistema debe enviar notificaciones instantáneas, claras y detalladas a un chat o grupo de Telegram preconfigurado cuando se detecte un evento de seguridad. Las notificaciones deben incluir la hora del evento, el tipo de evento y la ubicación o sensor específico que lo activó.

Justificación del requisito:

Es el pilar de la funcionalidad de alerta del sistema. Proporciona a los usuarios información crucial en tiempo real,

permitiéndoles tomar decisiones informadas y rápidas ante cualquier incidencia de seguridad.

Fuente (que interesado lo propone):	Unidad en la que se origina:

Usuarios Finales, Usuarios Directos (Propietarios), Expertos en Operaciones de Seguridad.

Seguridad

Criterios de validación:

- Una vez detectado el evento, la notificación aparece en Telegram en <3s.
- La notificación incluye tipo de evento, hora y sensor/zona.
- Las notificaciones se envían solo a los destinatarios configurados.

Identificador del Requisito:	Tipo de Requisito:	Caso de Uso/Evento:
Grado de satisfacción del interesado:	Grado de insatisfacción del interesado:	
Muy Alta (información en tiempo real).	Alta (si las notificaciones se retrasan o no llegan).	
Dependencias (qué requisitos depende de este):	Conflictos (qué requisitos son incompatibles o inconsistentes con este):	
- RF1.3 (Detección de Eventos) - RF3.5 (Notificaciones de Acceso)	N/A	
Documentos de soporte:	Histórico de cambios:	
Especificación de Interfaz de Telegram API, Diagrama de Flujo de Eventos de Alarma.	1.0 (2025-07-02): Creación inicial.	
Proyecto:	Analista:	
Sistema de Alerta de Telegram con Acceso Facial	[Tu Nombre]	

Exportar a Hojas de cálculo

---

3. Requisito Clave: RF3.2 - Verificación de Identidad Facial

Identificador del Requisito:	Tipo de Requisito:	Caso de Uso/Evento:
RF3.2	Funcional	Acceso a Zona Restringida, Verificación de Ingreso

Descripción:

En el punto de acceso, el sistema debe capturar una imagen del rostro del individuo y compararla en tiempo real con la base de datos de patrones faciales de usuarios autorizados. El sistema debe determinar una coincidencia con un umbral de confianza predefinido para verificar la identidad.

Justificación del requisito:

Es la columna vertebral del sistema de control de acceso biométrico. Proporciona una capa de seguridad robusta y un

Identificador del Requisito:	método de acceso conveniente y sin contacto, mejorando la eficiencia y reduciendo la necesidad de llaves físicas.
Tipo de Requisito:	Caso de Uso/Evento:
Fuente (que interesado lo propone):	Unidad en la que se origina:
Gerencia de Seguridad, Propietarios (conveniencia y seguridad).	Seguridad, I+D (Investigación y Desarrollo)
Criterios de validación: - Identifica correctamente a usuarios autorizados con una tasa de éxito del >95% en condiciones normales. - Tiempo de verificación facial no excede 2 segundos. - No concede acceso a individuos no registrados.	
Grado de satisfacción del interesado:	Grado de insatisfacción del interesado:
Muy Alta (seguridad y comodidad).	Alta (si hay falsos negativos/positivos, o es lento). Conflictos (qué requisitos son incompatibles o inconsistentes con este):
Dependencias (qué requisitos depende de este): - RF3.1 (Registro de Rostros de Usuarios) - RF3.3 (Concesión de Acceso Automático) - RNF-PRECISION (Precisión de Reconocimiento Facial)	N/A
Documentos de soporte:	Histórico de cambios:
Especificaciones de Módulo de Reconocimiento Facial, Políticas de Privacidad de Datos Biométricos.	1.0 (2025-07-02): Creación inicial.
Proyecto:	Analista:
Sistema de Alerta de Telegram con Acceso Facial	[Tu Nombre]

Identificador del Requisito:

Exportar a Hojas de cálculo

---

4. Requisito Clave: RF5.1 - Registro Detallado de Eventos

Identificador del Requisito:	Tipo de Requisito:	Caso de Uso/Evento:
RF5.1	Funcional	Auditoría de Seguridad, Registro de Actividad del Sistema

Descripción:

El sistema debe registrar de forma persistente, inmutable y detallada todos los eventos significativos (activaciones de sensores, cambios de estado, intentos de acceso exitosos/fallidos-, notificaciones enviadas). Cada registro debe incluir una marca de tiempo precisa y detalles relevantes.

Justificación del requisito:

Es esencial para la auditoría de seguridad, la resolución de problemas y el análisis forense post-incidente. Proporciona un rastro de auditoría completo y mantiene la trazabilidad de la seguridad.

Fuente (que interesado lo propone):	Unidad en la que se origina:
Administradores del Sistema, Expertos en Seguridad, Requisitos de Auditoría.	Operaciones de Seguridad, Cumplimiento Normativo

Criterios de validación:

- Todos los eventos críticos se registran automáticamente y con precisión.
- Cada registro incluye fecha, hora, tipo de evento y detalles.
- El historial de eventos es accesible y se mantiene por al menos 30 días.
- La integridad de los registros es inalterable por usuarios no autorizados.

Identificador del Requisito:	
Grado de satisfacción del interesado:	Grado de insatisfacción del interesado:
Muy Alta (trazabilidad completa).	Alta (si los registros se pierden o son incompletos).
Dependencias (qué requisitos depende de este):	Conflictos (qué requisitos son incompatibles o inconsistentes con este):
- RF1.3 (Detección de Eventos) - RF3.4 (Registro de Intentos de Acceso) - RF5.2 (Consulta del Historial de Eventos)	N/A
Documentos de soporte:	Histórico de cambios:
Políticas de Retención de Datos, Normas de Auditoría de Seguridad.	1.0 (2025-07-02):
	Creación inicial.
Proyecto:	Analista:
Sistema de Alerta de Telegram con Acceso Facial	[Tu Nombre]

Usuario Github:

Celenia-Leo (Puntos trabajo 8-10)
Hectuneti (Puntos trabajo 2da parte entregable 1-3)
Mujicaa459 (Puntos trabajo 5-7)
Revan2404 (Puntos trabajo 2da parte entregable 4-6)
Dakota18 (Puntos trabajo 1-4)

Link Github:
https://github.com/dakota18/RequisitoSistemas.git