ProteSys

Estudiante:

Juan Sebastian Galeano Gonzalez

Asignatura:

Patrones de Diseño de Software

Docente:

Fabrizio Bolaño Lopez

Pontificia Universidad Javeriana

Facultad de Ingeniería

Ingeniería de Sistemas

Bogotá

1. **Introducción**

El presente documento desarrolla el diseño del sistema de seguridad "proteSys", el cual tiene como objetivo brindar protección y seguridad a hogares y sus ocupantes mediante una aplicación móvil y una plataforma web.

Los usuarios podrán registrar su domicilio y a las personas que forman parte de su grupo familiar, y monitorear el comportamiento del hogar mediante sensores y cámaras de seguridad instaladas. Además, el sistema permitirá la comunicación entre los miembros del grupo familiar y la generación de alertas de seguridad, incluyendo una opción de alerta máxima que notificará a todos los usuarios registrados en el grupo familiar, a las autoridades correspondientes y a la empresa de seguridad contratada por el usuario.

El documento proporcionará una guía clara y completa para la implementación del sistema, incluyendo la definición de los componentes y módulos del sistema, la planificación del proyecto y las pruebas necesarias para asegurar su eficacia y confiabilidad.

2. **Requerimientos**.

2.1 **Seguridad:**

A continuación, se presentan los principales requerimientos de seguridad del sistema:

• Autenticación segura para los usuarios mediante contraseñas fuertes y autenticación de dos factores.

• Comunicación segura entre la aplicación móvil y la plataforma web utilizando protocolos de seguridad como HTTPS y SSL/TLS.

• Control de acceso basado en roles para limitar la información y las funcionalidades que pueden ser accedidas por cada usuario.

• Registro y auditoría de todas las actividades del usuario, incluyendo las alertas generadas y las acciones tomadas por los usuarios para garantizar la responsabilidad y la transparencia en el uso del sistema.

• Implementación de políticas de contraseñas seguras para garantizar que los usuarios elijan contraseñas fuertes y cambien regularmente sus contraseñas.

• Utilización de técnicas de cifrado para proteger la comunicación entre los dispositivos del usuario y el servidor del sistema de seguridad.

• Implementación de medidas de seguridad para prevenir la fuga de información confidencial, como la utilización de controles de acceso y encriptación de datos.

• Capacitación regular de los usuarios sobre las mejores prácticas de seguridad para prevenir la exposición de información confidencial.

2.2 **Requisitos Funcionales:**

- ProteSys debe permitir el registro de nuevos usuarios y almacenar su información de forma segura.
- Los usuarios de ProteSys deben tener la capacidad de iniciar sesión en la plataforma utilizando sus credenciales de usuario.
- ProteSys debe permitir a los usuarios cambiar su información de perfil, como la dirección de correo electrónico y la contraseña.
- Los usuarios deben tener la opción de recuperar su contraseña si la han olvidado.
- La plataforma debe permitir a los usuarios configurar sus preferencias de notificación y alertas.
- ProteSys debe permitir a los usuarios ver la información de los dispositivos de seguridad asociados a su cuenta.
- La plataforma debe permitir a los usuarios agregar y eliminar dispositivos de seguridad a su cuenta.
- ProteSys debe proporcionar a los usuarios una vista en tiempo real de las condiciones de seguridad de sus dispositivos.
- Los usuarios deben poder ver el historial de eventos de cada dispositivo de seguridad asociado a su cuenta.
- ProteSys debe permitir a los usuarios recibir alertas en tiempo real en su dispositivo móvil cuando se detecte una actividad sospechosa en su hogar o negocio.
- La plataforma debe permitir a los usuarios configurar y personalizar los informes de seguridad y análisis para sus dispositivos.

- Los usuarios deben tener la opción de contactar al soporte técnico de ProteSys a través de la aplicación móvil en caso de problemas o preguntas.

- La plataforma debe permitir a los usuarios realizar copias de seguridad de sus datos y configuraciones de seguridad en caso de pérdida de datos.

2.3 **Requisitos No Funcionales:**

- Disponibilidad: ProteSys debe estar disponible en todo momento, con un tiempo de inactividad mínimo para asegurar que los usuarios puedan acceder a su información y dispositivos de seguridad en todo momento.

- Fiabilidad: El sistema debe ser confiable y garantizar que los dispositivos de seguridad estén siempre en funcionamiento y respondan a las alertas de seguridad.

- Usabilidad: La interfaz de usuario de la aplicación móvil y la plataforma web de ProteSys deben ser intuitivas y fáciles de usar para garantizar que los usuarios puedan interactuar con el sistema sin problemas.

- Rendimiento: El sistema debe ser rápido y eficiente en su respuesta a las solicitudes de los usuarios y en el procesamiento de datos.

- Mantenibilidad: ProteSys debe ser fácil de mantener y actualizar, con una documentación clara y completa para permitir a los desarrolladores y al personal de soporte técnico realizar cambios y mejoras en el sistema.

- Integración: El sistema debe ser capaz de integrarse con otros sistemas y dispositivos de seguridad existentes para mejorar su funcionalidad y facilitar la interoperabilidad.

- Estabilidad: El sistema debe ser estable y evitar errores y fallos que puedan afectar negativamente a los usuarios.

- Seguridad de datos: ProteSys debe garantizar la protección y privacidad de los datos de los usuarios, cumpliendo con las leyes y regulaciones de protección de datos aplicables.

- Trazabilidad: ProteSys debe ser capaz de rastrear y registrar todas las acciones realizadas por los usuarios y el sistema, para permitir una fácil auditoría y solución de problemas.

3. Diseño del Sistema:

3.1 Casos de Uso:

1.

Nombre:	Agregar nuevo usuario
Actores:	Administrador del sistema
Objetivo	Añadir un nuevo usuario al sistema para que pueda acceder y utilizar las funcionalidades del sistema.
Precondiciones:	El administrador del sistema tiene credenciales de acceso válidas y autorización para añadir
Poscondiciones:	El nuevo usuario se agrega al sistema y se le asigna un conjunto de permisos correspondiente a su rol en el sistema.
Flujo de eventos:	1. El administrador inicia sesión en el sistema y accede a la sección de gestión de usuarios. 2. El administrador selecciona la opción de agregar nuevo usuario. 3. El sistema muestra un formulario para ingresar los datos del nuevo usuario, incluyendo nombre de usuario, correo electrónico y contraseña. 4. El administrador ingresa los datos del nuevo usuario y especifica el rol que tendrá en el sistema. 5. El sistema valida la información ingresada y agrega al nuevo usuario al sistema. 6. El sistema muestra una confirmación de que el nuevo usuario se agregó correctamente.
Situaciones excepcionales:	o Si el administrador ingresa datos incompletos o inválidos, el sistema muestra un mensaje de error y solicita que se corrijan los datos. o Si el correo electrónico ya se encuentra registrado en el sistema, el sistema muestra

	un mensaje de error indicando que ya existe un usuario con ese correo electrónico.

2.

Nombre:	Modificar información del usuario
Actores:	Usuario del sistema, Administrador del sistema
Objetivo	Permitir al usuario o al administrador del sistema modificar la información de un usuario registrado en el sistema.
Precondiciones:	El usuario o el administrador del sistema tienen credenciales de acceso válidas y autorización para modificar la información de usuarios.
Poscondiciones:	La información del usuario se actualiza en el sistema.
Flujo de eventos:	1. El usuario o administrador inicia sesión en el sistema y accede a la sección de gestión de usuarios. 2. El usuario o administrador busca y selecciona el usuario cuya información desea modificar. 3. El sistema muestra la información actual del usuario, incluyendo nombre, correo electrónico y otros detalles del perfil. 4. El usuario o administrador modifica los campos de información que desea actualizar. 5. El sistema valida la información ingresada y actualiza los datos del usuario en el sistema. 6. El sistema muestra una confirmación de que la información del usuario se actualizó correctamente.
Situaciones excepcionales:	o Si el usuario o administrador intenta modificar datos inválidos o incompletos, el sistema muestra un mensaje de error y solicita que se corrijan los datos. o Si el usuario o administrador no tiene autorización para modificar la información de un usuario específico, el sistema muestra

	un mensaje de error indicando que no se puede realizar la acción solicitada.

3.

Nombre:	Gestionar permisos de usuario
Actores:	Administrador del sistema
Objetivo	Asignar o revocar permisos a un usuario en el sistema.
Precondiciones:	El administrador del sistema ha iniciado sesión y tiene autorización para modificar los permisos de los usuarios.
Poscondiciones:	Los permisos del usuario se han actualizado en el sistema.
Flujo de eventos:	1. El administrador inicia sesión en el sistema y accede a la sección de gestión de usuarios. 2. El administrador busca el usuario al que desea asignar o revocar permisos. 3. El sistema muestra la información del usuario, incluyendo sus permisos actuales. 4. El administrador selecciona la opción de modificar permisos del usuario. 5. El sistema muestra una lista de los permisos disponibles y su estado actual para el usuario seleccionado. 6. El administrador selecciona los permisos que desea asignar o revocar y guarda los cambios. 7. El sistema actualiza los permisos del usuario y muestra una confirmación de que se realizaron los cambios correctamente.
Situaciones excepcionales:	o Si el administrador intenta asignar un permiso que ya tiene el usuario, el sistema muestra un mensaje indicando que el permiso ya está asignado. o Si el administrador intenta revocar un permiso que el usuario no tiene, el sistema muestra un mensaje indicando que el permiso no se puede revocar porque el usuario no lo tiene asignado. o Si el administrador ingresa datos incorrectos o incompletos, el sistema

	muestra un mensaje de error y solicita que se corrijan los datos.

4.

Nombre:	Eliminar usuario del sistema.
Actores:	Administrador del sistema
Objetivo	Eliminar un usuario existente del sistema.
Precondiciones:	o El administrador del sistema tiene credenciales de acceso válidas y autorización para eliminar usuarios. o El usuario que se desea eliminar existe en el sistema.
Poscondiciones:	El usuario seleccionado es eliminado del sistema, y todos sus datos y configuraciones asociadas son eliminados.
Flujo de eventos:	1. El administrador inicia sesión en el sistema y accede a la sección de gestión de usuarios. 2. El administrador selecciona el usuario que desea eliminar. 3. El sistema muestra una ventana de confirmación para verificar que el administrador desea eliminar al usuario. 4. El administrador confirma que desea eliminar al usuario. 5. El sistema elimina al usuario del sistema y todas sus configuraciones asociadas. 6. El sistema muestra una confirmación de que el usuario se eliminó correctamente.
Situaciones excepcionales:	o Si el administrador no tiene autorización para eliminar usuarios, el sistema muestra un mensaje de error y no permite la eliminación. o Si el usuario seleccionado no existe en el sistema, el sistema muestra un mensaje de error indicando que el usuario no existe.

5.

Nombre:	Notificar emergencia.
Actores:	Usuario del sistema
Objetivo	Notificar una emergencia a las autoridades y/o contactos de emergencia registrados en el sistema.
Precondiciones:	o El usuario del sistema tiene una cuenta activa. o El dispositivo móvil con la aplicación está conectado a internet.
Poscondiciones:	Se envía una notificación de emergencia a las autoridades y/o contactos de emergencia registrados en el sistema.
Flujo de eventos:	1. El usuario del sistema abre la aplicación del sistema en su dispositivo móvil. 2. El usuario del sistema selecciona la opción "Notificar emergencia". 3. El sistema muestra un formulario para ingresar los detalles de la emergencia, incluyendo la descripción y ubicación. 4. El usuario del sistema ingresa los detalles de la emergencia. 5. El sistema valida la información ingresada y muestra una confirmación de que se envió la notificación. 6. El sistema envía una notificación de emergencia a las autoridades y/o contactos de emergencia registrados en el sistema.
Situaciones excepcionales:	o Si el dispositivo móvil del usuario no está conectado a internet, el sistema muestra un mensaje de error indicando que no se puede enviar la notificación. o Si el usuario no ha ingresado la información necesaria para la notificación de emergencia, el sistema muestra un mensaje de error y solicita que se complete la información requerida. o Si la notificación no se pudo enviar, el sistema muestra un mensaje de error y ofrece la opción de volver a intentar el envío de la notificación.
Includes	o Incluir envío de imagen o video de la emergencia para proveer más información a

	las autoridades y/o contactos de emergencia. o Incluir opción de cancelar la notificación de emergencia después de ser enviada.
Extends	o Extender para permitir al usuario especificar el tipo de emergencia (incendio, asalto, accidente, etc.). o Extender para permitir al usuario especificar la gravedad de la emergencia (leve, moderada, grave). o Extender para incluir la opción de llamar directamente a servicios de emergencia desde la aplicación.

6.

Nombre:	Consultar historial de alertas.
Actores:	Usuario del sistema.
Objetivo	Consultar el historial de alertas generadas en el sistema en un periodo de tiempo específico.
Precondiciones:	El usuario del sistema tiene acceso válido y autorización para consultar el historial de alertas.
Poscondiciones:	El usuario visualiza la lista de alertas generadas en el periodo de tiempo especificado.
Flujo de eventos:	1. El usuario inicia sesión en el sistema. 2. El usuario navega hasta la sección de "Historial de alertas". 3. El usuario especifica un rango de tiempo para el cual desea visualizar las alertas generadas. 4. El sistema muestra la lista de alertas generadas en el rango de tiempo especificado. 5. El usuario puede hacer clic en una alerta específica para ver más detalles, como la fecha y hora de la alerta, el dispositivo que la generó y la descripción de la alerta.
Situaciones excepcionales:	o Si el usuario no tiene acceso válido o autorización para consultar el historial de alertas, el sistema muestra un mensaje de error indicando que no tiene los permisos necesarios.

	○ Si no hay alertas generadas en el rango de tiempo especificado, el sistema muestra un mensaje indicando que no hay alertas disponibles en ese período.

7.

Nombre:	Crear grupo familiar.
Actores:	Administrador del sistema
Objetivo	Crear un nuevo grupo familiar en el sistema.
Precondiciones:	○ El administrador del sistema ha iniciado sesión en el sistema. ○ El administrador tiene el permiso de crear grupos familiares.
Poscondiciones:	El nuevo grupo familiar se crea en el sistema y se asigna al administrador como propietario del grupo.
Flujo de eventos:	1. El administrador inicia sesión en el sistema y accede a la sección de administración de grupos familiares. 2. El administrador selecciona la opción de crear un nuevo grupo familiar. 3. El sistema muestra un formulario para ingresar los datos del nuevo grupo, incluyendo el nombre del grupo y los miembros que lo conformarán. 4. El administrador ingresa los datos del nuevo grupo y los miembros que lo conformarán. 5. El sistema valida la información ingresada y crea el nuevo grupo familiar. 6. El sistema muestra una confirmación de que el nuevo grupo familiar se creó correctamente.
Situaciones excepcionales:	○ Si el administrador ingresa datos incompletos o inválidos, el sistema muestra un mensaje de error y solicita que se corrijan los datos. ○ Si el administrador no tiene permiso para crear grupos familiares, el sistema muestra un mensaje indicando que no tiene autorización para realizar esta acción.

8.

Nombre:	Modificar grupo familiar.
Actores:	Administrador del sistema
Objetivo	Modificar la información de un grupo familiar existente.
Precondiciones:	El administrador del sistema ha iniciado sesión y tiene permisos para modificar grupos familiares.
Poscondiciones:	El grupo familiar ha sido modificado con éxito en el sistema.
Flujo de eventos:	1. El administrador del sistema inicia sesión y accede a la sección de administración de grupos familiares. 2. El administrador selecciona el grupo familiar que desea modificar. 3. El sistema muestra los detalles del grupo familiar, incluyendo su nombre, lista de miembros y dispositivos asociados. 4. El administrador realiza los cambios necesarios en la información del grupo, como cambiar su nombre o agregar o eliminar miembros o dispositivos. 5. El sistema valida la información ingresada por el administrador y actualiza el grupo familiar en la base de datos. 6. El sistema muestra una confirmación de que el grupo familiar ha sido modificado con éxito.
Situaciones excepcionales:	o Si el administrador intenta modificar un grupo familiar que no existe, el sistema muestra un mensaje de error y no realiza ninguna acción. o Si el administrador intenta agregar un miembro que ya pertenece a otro grupo familiar, el sistema muestra un mensaje de error y no realiza la acción.

9.

Nombre:	Agregar usuario a grupo familiar.

Actores:	○ Administrador del grupo familiar. ○ Usuario para agregar.
Objetivo	Agregar un usuario a un grupo familiar existente.
Precondiciones:	○ El administrador del grupo familiar tiene credenciales de acceso válidas y autorización para agregar usuarios al grupo. ○ El usuario para agregar no está actualmente en otro grupo familiar.
Poscondiciones:	El usuario se agrega al grupo familiar y se le otorga el acceso correspondiente a las funciones del grupo.
Flujo de eventos:	1. El administrador del grupo familiar inicia sesión en el sistema y accede a la sección de gestión de miembros del grupo familiar. 2. El administrador selecciona la opción de agregar un nuevo miembro al grupo. 3. El administrador ingresa los datos del nuevo usuario y especifica el rol que tendrá en el grupo. 4. El sistema verifica que el usuario no esté actualmente en otro grupo familiar. 5. Si el usuario está en otro grupo familiar, el sistema muestra un mensaje de error y no se agrega al grupo. 6. Si el usuario no está en otro grupo familiar, el sistema agrega al usuario al grupo y le otorga los permisos correspondientes. 7. El sistema muestra una confirmación de que el usuario se agregó correctamente.
Situaciones excepcionales:	○ Si el administrador ingresa datos incompletos o inválidos, el sistema muestra un mensaje de error y solicita que se corrijan los datos. ○ Si el usuario a agregar ya está en otro grupo familiar, el sistema muestra un mensaje de error indicando que el usuario ya está en otro grupo familiar y no se agrega al grupo.

10.

Nombre:	Consultar información del grupo familiar.
Actores:	Usuario con rol de miembro del grupo familiar.
Objetivo	Ver la información del grupo familiar al que pertenece el usuario.
Precondiciones:	El usuario ha iniciado sesión y es miembro de un grupo familiar.
Poscondiciones:	El usuario puede ver la información del grupo familiar.
Flujo de eventos:	1. El usuario inicia sesión en el sistema. 2. El usuario accede a la sección de información de su grupo familiar. 3. El sistema muestra la información del grupo familiar, que incluye el nombre del grupo, la lista de miembros, y la información de contacto del administrador del grupo. 4. El usuario puede ver y revisar la información del grupo.
Situaciones excepcionales:	o Si el usuario no es miembro de un grupo familiar, el sistema muestra un mensaje de error indicando que el usuario no pertenece a ningún grupo familiar. o Si no se puede acceder a la información del grupo familiar por problemas técnicos o de conectividad, el sistema muestra un mensaje de error y sugiere al usuario intentarlo de nuevo más tarde.

11.

Nombre:	Monitorear cámaras de seguridad.
Actores:	Usuario con permiso para ver cámaras de seguridad.
Objetivo	Monitorear las cámaras de seguridad para detectar posibles riesgos y alertar a las autoridades competentes en caso de una situación de emergencia.

Precondiciones:	○ El usuario debe tener acceso autorizado al sistema de monitoreo de cámaras de seguridad. ○ Las cámaras de seguridad deben estar instaladas y configuradas en el sistema.
Poscondiciones:	El usuario ha visualizado y monitoreado las cámaras de seguridad en busca de situaciones de riesgo.
Flujo de eventos:	1. El usuario inicia sesión en el sistema de monitoreo de cámaras de seguridad. 2. El usuario selecciona la opción de "Monitorear cámaras de seguridad". 3. El sistema muestra una lista de cámaras de seguridad disponibles para monitorear. 4. El usuario selecciona una o varias cámaras de seguridad para monitorear. 5. El sistema muestra la vista en tiempo real de las cámaras seleccionadas. 6. El usuario monitorea las cámaras y busca situaciones de riesgo. 7. Si el usuario detecta una situación de riesgo, toma las medidas necesarias para alertar a las autoridades competentes.
Situaciones excepcionales:	○ Si el usuario no tiene acceso autorizado al sistema de monitoreo de cámaras de seguridad, el sistema le muestra un mensaje de error y no le permite continuar. ○ Si las cámaras de seguridad no están instaladas o configuradas en el sistema, el sistema le muestra al usuario un mensaje de error indicando que no hay cámaras disponibles para monitorear.

12.

Nombre:	Chatear con grupo familiar.
Actores:	Usuario con rol de miembro del grupo familiar.
Objetivo	Permitir la comunicación entre los miembros del grupo familiar a través de un chat.

Precondiciones:	El usuario tiene una cuenta de proteSys y ha iniciado sesión. Además, el usuario es parte de un grupo familiar en el sistema.
Poscondiciones:	El usuario ha enviado y/o recibido mensajes en el chat del grupo familiar.
Flujo de eventos:	1. El usuario inicia sesión en su cuenta de proteSys y accede a la sección de grupo familiar. 2. El usuario selecciona la opción de chat con grupo familiar. 3. El sistema muestra una lista de los miembros del grupo familiar conectados al chat. 4. El usuario selecciona al miembro del grupo familiar con el que desea comunicarse. 5. El sistema muestra una interfaz de chat en la que el usuario puede enviar y recibir mensajes de texto. 6. El usuario escribe un mensaje y lo envía al miembro del grupo familiar seleccionado. 7. El sistema envía el mensaje al miembro del grupo familiar y muestra una confirmación de que el mensaje se ha enviado correctamente. 8. El usuario recibe mensajes entrantes del miembro del grupo familiar seleccionado y puede leerlos y responder.
Situaciones excepcionales:	o Si el usuario intenta enviar un mensaje sin contenido, el sistema muestra un mensaje de error y solicita que se escriba un mensaje válido.

13.

Nombre:	Monitorear sensores
Actores:	Usuario con rol de miembro del grupo familiar.
Objetivo	Verificar el estado actual de los sensores en tiempo real y recibir alertas en caso de detectar alguna anomalía.

Precondiciones:	El usuario ha iniciado sesión en el sistema y tiene acceso autorizado a los sensores que desea monitorear.
Poscondiciones:	El usuario ha visualizado la información actualizada de los sensores y recibido alertas en caso de detectar alguna anomalía.
Flujo de eventos:	1. El usuario accede a la sección de monitoreo de sensores en el sistema. 2. El sistema muestra una lista de los sensores disponibles para monitorear. 3. El usuario selecciona uno o varios sensores para visualizar su estado actual. 4. El sistema muestra la información actualizada de los sensores seleccionados. 5. Si el sensor detecta alguna anomalía, el sistema envía una alerta al usuario indicando el tipo de anomalía detectada y su ubicación.
Situaciones excepcionales:	o Si el usuario no tiene acceso autorizado a los sensores que desea monitorear, el sistema muestra un mensaje de error y no permite el acceso a la información. o Si hay algún problema técnico con el sensor, el sistema muestra un mensaje de error indicando que el sensor no se puede monitorear en ese momento.

14.

Nombre:	Generar alarma de máxima prioridad.
Actores:	Sistema de seguridad.
Objetivo	Generar una alarma de máxima prioridad cuando se detecte una situación de peligro inminente.
Precondiciones:	o Los sensores y cámaras están instalados y funcionando correctamente. o Los valores límite para las alertas de máxima prioridad están configurados en el sistema.
Poscondiciones:	o Se genera una alerta de máxima prioridad en el sistema.

	○ Se notifica a los usuarios correspondientes para que tomen medidas de seguridad.
Flujo de eventos:	1. El sistema de seguridad monitorea constantemente los sensores y cámaras instalados. 2. Si alguno de los sensores detecta una situación de peligro inminente, el sistema genera una alerta de máxima prioridad. 3. El sistema notifica inmediatamente a los usuarios correspondientes, proporcionando detalles sobre la situación detectada y las medidas de seguridad recomendadas. 4. El sistema continúa monitoreando la situación hasta que se confirme que se ha resuelto o que ya no representa una amenaza inminente.
Situaciones excepcionales:	○ Si el sistema no puede enviar la notificación a los usuarios correspondientes, se genera una alerta de máxima prioridad en la consola del administrador del sistema para que se tomen las medidas necesarias. ○ Si se detecta un falso positivo, los usuarios pueden confirmar la situación a través del sistema para cancelar la alerta de máxima prioridad.

15.

Nombre:	Solicitar ayuda a autoridades o algún servicio de emergencias.
Actores:	Usuario con rol de miembro del grupo familiar.
Objetivo	Permitir al usuario solicitar ayuda a autoridades o algún servicio de emergencias en caso de emergencia.
Precondiciones:	○ El usuario debe tener acceso al sistema. ○ El usuario debe encontrarse en una situación de emergencia.
Poscondiciones:	Se notifica a las autoridades o al servicio de emergencias correspondiente acerca de la situación de emergencia.

Flujo de eventos:	1. El usuario accede al sistema. 2. El usuario identifica una situación de emergencia y selecciona la opción de solicitar ayuda a autoridades o algún servicio de emergencias. 3. El sistema solicita la información necesaria para identificar la ubicación del usuario y la naturaleza de la emergencia. 4. El usuario ingresa la información solicitada. 5. El sistema valida la información ingresada y la envía a las autoridades o al servicio de emergencias correspondiente. 6. El sistema muestra un mensaje de confirmación de que la solicitud de ayuda ha sido enviada.
Situaciones excepcionales:	o Si el usuario no tiene acceso al sistema, se muestra un mensaje de error indicando que no se puede solicitar ayuda. o Si el usuario no se encuentra en una situación de emergencia, se muestra un mensaje de error indicando que no se puede solicitar ayuda. o Si la información ingresada por el usuario es incorrecta o incompleta, se muestra un mensaje de error y se solicita que se corrija la información.

3.2 **Historias de Usuario:**

- Como usuario, quiero poder agregar nuevos usuarios al sistema para que mi familia y yo podamos acceder al sistema de seguridad.

- Como usuario, quiero poder consultar el historial de alertas para ver las alertas previas y tomar decisiones basadas en esta información.

- Como usuario, quiero poder crear un grupo familiar para que mi familia y yo podamos compartir información y controlar el sistema de seguridad.

- Como administrador, quiero poder modificar la información de un grupo familiar existente para mantener actualizada la información de los miembros del grupo.

- Como administrador, quiero poder agregar nuevos miembros a un grupo familiar existente para permitir que más personas accedan al sistema de seguridad.

- Como usuario, quiero poder consultar la información del grupo familiar para conocer los miembros y los dispositivos de seguridad asociados a cada uno de ellos.

- Como usuario, quiero poder monitorear las cámaras de seguridad para saber lo que está sucediendo en tiempo real.

- Como usuario, quiero poder chatear con los miembros de mi grupo familiar para coordinar acciones en caso de emergencia.

- Como usuario, quiero poder monitorear los sensores de seguridad para detectar cualquier actividad sospechosa.

- Como usuario, quiero poder generar una alarma de máxima prioridad si detecto una situación de emergencia para alertar a las autoridades o a mi grupo familiar.

- Como usuario, quiero poder recibir notificaciones en tiempo real en caso de que se detecte una situación de emergencia para poder tomar medidas preventivas.

- Como administrador, quiero poder eliminar a un miembro de un grupo familiar existente para garantizar la seguridad del grupo.

- Como usuario, quiero poder solicitar ayuda a las autoridades o a algún servicio de emergencia en caso de una situación crítica.

- Como administrador, quiero poder asignar diferentes niveles de acceso a los miembros de un grupo familiar para garantizar la seguridad de la información.

- Como usuario, quiero poder consultar las instrucciones de seguridad para saber cómo actuar en caso de una emergencia.

3.3 **Patrones de Diseño implementados:**

- Factory Method: Este patrón se utilizó en la implementación del sistema de notificaciones. Mediante este se pueden crear distintos tipos de notificaciones según el contexto del caso de uso en el que se encuentre.

- Observer: Este patrón se utilizó en la implementación del sistema de notificaciones. Mediante este el usuario se suscribe al sistema de notificaciones de manera que cuando se crea una notificación, este es notificado y por tanto actualiza su listado de notificaciones.

- Adapter: Este patrón se intento utilizar en la implementación de los distintos tipos de sensores y cámaras de seguridad. Desafortunadamente, no se completó su desarrollo.

- Command: Este patrón se utilizó para la implementación del botón de pánico, mediante el cual se notifica a la empresa de seguridad. Se completó su implementación en el servidor, pero no esta implementada la funcionalidad en el cliente Angular.

- Singleton: Este patrón se utilizó en la implementación de la lógica relacionada con la empresa de seguridad. Encierra la comunicación con autoridades competentes y la empresa de seguridad asociada mediante una interfaz.

- Facade: Este patrón se utilizó para la integración de los distintos sistemas de comunicación con la empresa de seguridad.

4. **Arquitectura del Sistema:**

Clases:

1. Usuario: representa a un usuario del sistema proteSys.
   Atributos:
   - id (long): identificador único del usuario.
   - cedula (long): cédula del usuario.
   - nombre (str): nombre del usuario.
   - correo_electronico (str): correo electrónico del usuario.
   - telefono (str): número de teléfono del usuario.
   - contraseña (str): contraseña del usuario.
   - rol (str): rol del usuario en el sistema (administrador, miembro del grupo familiar, etc.).

2. Grupo: representa a un grupo familiar en el sistema proteSys.
   Atributos:
   - id (int): identificador único del grupo familiar.
   - nombre (str): nombre del grupo familiar.
   - direccion (str): dirección de la casa asociada al grupo familiar.
   - administrador (Usuario): usuario que es administrador del grupo familiar.

3. Piso: representa a un piso de una casa en el sistema proteSys.
   Atributos:
   - id (int): identificador único del piso.
   - numero (int): número del piso en la casa.
   - descripcion (str): descripción del piso.

4. Casa: representa a una casa en el sistema proteSys.
   Atributos:
   - id (int): identificador único de la casa.
   - direccion (str): dirección de la casa.
   - pisos (List[Piso]): lista de los pisos de la casa.

5. EmpresaSeguridad: representa a una empresa de seguridad asociada al sistema proteSys.
   Atributos:
   - id (int): identificador único de la empresa de seguridad.
   - nombre (str): nombre de la empresa de seguridad.
   - correo_electronico (str): correo electrónico de la empresa de seguridad.
   - telefono (str): número de teléfono de la empresa de seguridad.

6. Notificacion: representa una notificación generada por el sistema proteSys.
   Atributos:
   - id (int): identificador único de la notificación.
   - mensaje (str): mensaje de la notificación.
   - fecha (datetime): fecha y hora de la notificación.

7. Camara: representa una cámara de seguridad en el sistema proteSys.
   Atributos:
   - id (int): identificador único de la cámara de seguridad.
   - ubicacion (str): ubicación de la cámara de seguridad.
   - piso (Piso): piso al que pertenece la cámara de seguridad.

8. Sensor: representa un sensor de seguridad en el sistema proteSys.
   Atributos:
   - id (int): identificador único del sensor de seguridad.
   - ubicacion (str): ubicación del sensor de seguridad.
   - tipo (str): tipo de sensor de seguridad (humo, gas, movimiento, etc.).
   - piso (Piso): Piso al que pertenece el sensor.