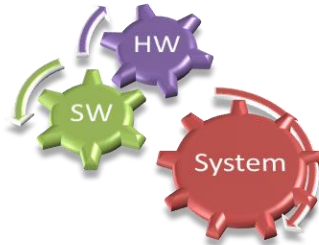


Smart Embedded Systems

Departamento de sistemas empotrados



Sistema de Seguridad para Hogares SSH-101

Requerimientos de Software

Borrador 9

04/20/2025

Historial de revisiones

Versión #	Autor	Notas del documento	Fecha
Borrador 1	Victor Sánchez Juan Pablo Ureña	Corrección y definición de: <ul style="list-style-type: none"> - Perspectiva del producto - Funciones del Producto 	2025-02-12
Borrador 2	Victor Sánchez Juan Pablo Ureña	Creacion de tabla para la Asignacion de requerimientos	2025-02-15
Borrador 2	V. Sánchez J. Ureña	Corrección y definición de: <ul style="list-style-type: none"> - Abreviaturas - Requisitos ambientales - Requisitos de interacción Hardware-Software 	2025-02-16
Borrador 3	V. Sánchez J. Ureña	Definición de requerimientos relacionados con la "Operación del software" (requerimientos de sistema): <ul style="list-style-type: none"> - Funciones - Requerimientos de usabilidad - Requerimientos de rendimiento - Restricciones de diseño - Estándares y regulaciones aplicables - Requerimientos funcionales 	2025-02-19
Borrador 4	V. Sánchez J. Ureña	Definición de requerimientos relacionados con la "Operación del software": <ul style="list-style-type: none"> - Activación de la alarma - Activación de la alerta de pánico - Activación de la alerta de incendio 	2025-02-22
Borrador 5	V. Sánchez J. Ureña	Definición de los requerimientos de sistema relacionados a funciones generales, así como atributos del sistema en general.	2025-02-23
Borrador 6	V. Sánchez J. Ureña	Creacion de la Matriz de Trazabilidad y correcciones a nivel de formato del documento	2025-02-25
Borrador 7	V. Sánchez J. Ureña	<ol style="list-style-type: none"> 1. Corrección ID requerimientos asociados a sección 4 del documento para mantener consistencia. 2. SW-ID-106. Nota agregada para indicar que no es un requerimiento funcional, sino para indicar característica necesaria por el sistema. 3. Sección 3 del documento fue actualizada. 4. Sección 6 modificada para incluir en forma especifica el público meta. 5. SW-ID-75. Nota fue incluida para indicar relevancia del contador. 6. SW-ID-80. Requerimiento fue modificado para indicar que el 	2025-03-19

		<p>requerimiento al que hace referencia solo indica formato y no el estado del mensaje</p> <p>7. SW-ID-83. Requerimiento fue modificado para indicar que el requerimiento al que hace referencia solo indica formato y no el estado del mensaje</p> <p>8. SW-ID-86. Requerimiento fue modificado para indicar que el requerimiento al que hace referencia solo indica formato y no el estado del mensaje</p> <p>9. SW-ID-93 y SW-ID-94 fueron modificados para brindar coherencia a la estructura del sistema.</p> <p>10. Sección 5 Arquitectura del sistema. Sección incluida para especificar la arquitectura del sistema, incluyendo diagramas de bloques funcionales, diagramas de flujo, diagramas de estado y demás información relevante.</p>	
Borrador 8	V. Sánchez J. Ureña	<p>1. Ajustando matriz de trazabilidad con las funciones implementadas para los requerimientos de bajo nivel.</p> <p>2. Eliminando requerimientos redundantes.</p> <p>3. Ajustando detalles generales del documento.</p>	2025-04-06
Borrador 9	V. Sánchez J. Ureña	<p>1. Actualizando requerimientos relacionados con la funcionalidad de la fuente de alimentación para corregir contradicciones.</p> <p>2. Adición de matriz de trazabilidad de requerimientos de software hacia casos de prueba.</p>	2025-04-20

Tabla de contenidos

1	Introducción.....	6
1.1	Propósito y alcance	6
1.2	Referencias.....	6
1.3	Abreviaturas	6
1.4	Definiciones	6
2	Descripción general	6
3	Alcance	7
4	Perspectiva del producto	8
4.1	Interfaces.....	8
4.1.1	Interfaces de sistema	8
4.1.2	Interfaces de usuario	8
4.1.3	Interfaces de hardware	9
4.1.4	Interfaces de software	9
4.2	Interfaces de comunicación	10
4.3	Restricciones de memoria	10
4.4	Modos de operación	10
4.5	Requerimientos de localización	10
5	Arquitectura de Software.....	11
5.1	Módulo de Control.....	12
5.1.1	Diagrama de estados Modo Armado (0 y 1).....	13
5.1.2	Diagrama de estados Modo Desarmado.....	14
5.1.3	Diagrama de flujo Ahorro de Batería	14
5.1.4	Diagrama de flujo del modo administrador	16
5.2	Interfaz principal.....	18
5.3	Módulo de Auto Prueba	20
6	Funciones del producto	20
7	Características del usuario	20
8	Limitaciones	21
9	Suposiciones y dependencias.....	21
10	Asignación de requerimientos	22
11	Interfaces externos	23
12	Requerimientos.....	24
12.1	Funciones.....	24
12.2	Requerimientos de <i>usabilidad</i>	26
12.3	Requerimientos de rendimiento.....	27
12.4	Restricciones de diseño	27

12.5	Estándares y regulaciones aplicables	28
12.6	Requerimientos funcionales	28
12.6.1	Modo 0.....	28
12.6.2	Modo 1.....	29
12.6.3	Modo Desarmado.....	30
12.6.4	Modo Ahorro.....	30
12.7	Atributos de sistema.....	31
12.7.1	Requerimientos de confiabilidad.....	31
12.7.2	Requerimientos de seguridad.....	31
12.7.3	Requerimientos de mantenibilidad.....	31
12.7.4	Requerimientos de portabilidad	32
12.7.5	Otros requerimientos.....	32
13	Verificación.....	iError! Marcador no definido.
14	Información de soporte	iError! Marcador no definido.
Apéndice 1.	Matriz de Trazabilidad	33

1 Introducción

1.1 Propósito y alcance

El propósito de este documento es proveer la especificación de los requerimientos de *software* para el sistema de alarma SSH-101. El sistema de alarma para hogares SSH-101 constituye el modelo más básico de sistemas de seguridad de la compañía *Smart Embedded Systems*. Es una solución de bajo costo para necesidades de seguridad con un máximo de 16 sensores.

1.2 Referencias

- ISO/IEC/IEEE 29148 - Systems and software engineering —Life cycle processes — Requirements engineering

1.3 Abreviaturas

SSH: Sistema de Seguridad para Hogares

LCD: Indicador de cristal líquido

LED: Diodo emisor de luz

DC: Corriente Directa

GSM: Sistema Global para las Comunicaciones Móviles

1.4 Definiciones

Caso de prueba: Documentación que especifica las entradas, resultados esperados, y un conjunto de condiciones de ejecución para un elemento de prueba [IEEE Std 1012-1998].

LCD: Indicador de cristal líquido o *Liquid Crystal Display*.

LED: Diodo emisor de luz o *Light Emitting Diode*.

Nivel de integridad: Una indicación de un rango de valores de una propiedad de un elemento necesario para mantener los riesgos del sistema dentro de límites aceptables. Para elementos que realizan funciones de mitigación, la propiedad es la confiabilidad con la cual el elemento debe realizar la función de mitigación. Para elementos cuya falla puede conducir a una amenaza, la propiedad es el límite en la frecuencia de esa falla [ISO/IEC 15026].

Procedimiento de Prueba: Documentación que especifica una secuencia de acciones para ejecutar una prueba [IEEE Std 1012-1998].

Revisión técnica: Evaluación sistemática de un producto de software por un equipo calificado que examina la conformidad del mismo con respecto a su uso programado y sus especificaciones. [IEEE Std 1012-1998].

2 Descripción general

El sistema de seguridad SSH-101 consta de 4 componentes:

- Sistema de control con respaldo de batería
- Sensores
- Tablero
- Sirena

El diagrama de la Figura 1 muestra la forma en que se interconectan dichos componentes:

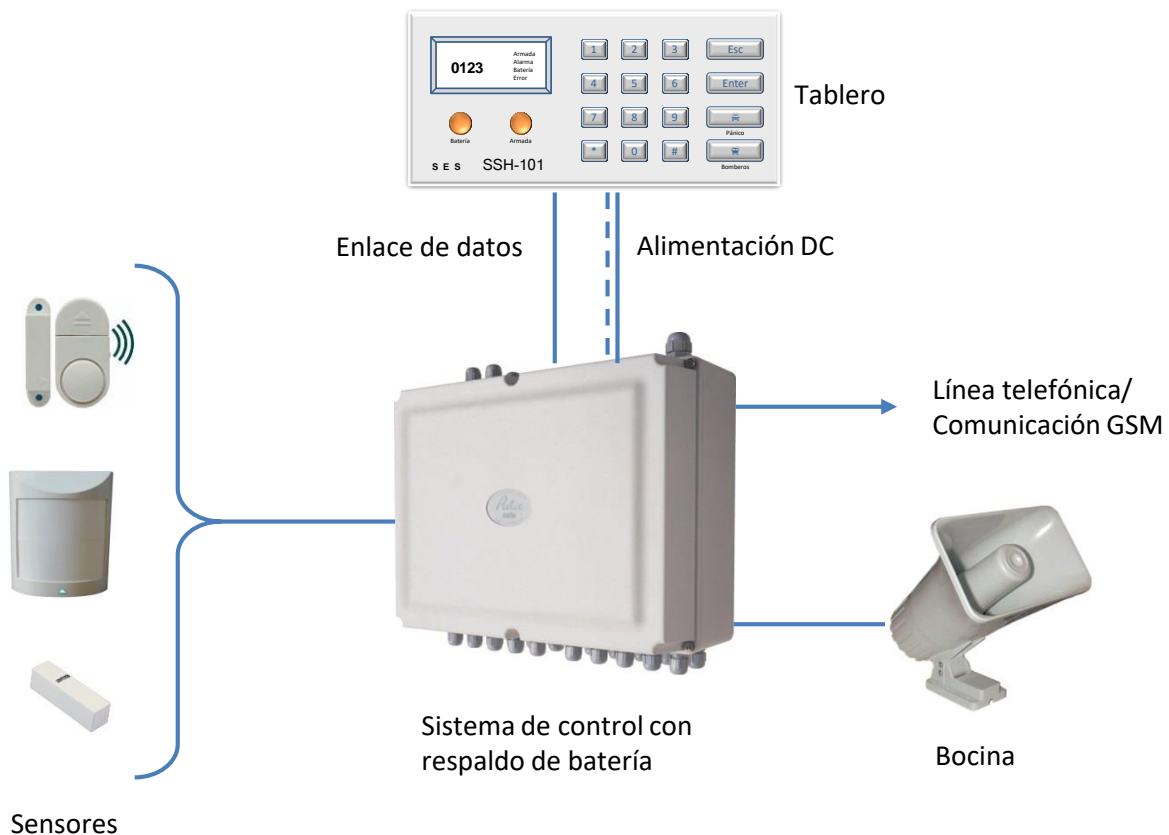


Figura 1. Componentes del sistema SSH-101

3 Alcance

El Sistema de Seguridad para Hogares constará con los siguientes elementos:

- Sistema de Control con respaldo de batería
- Tablero principal
- Bocina
- Sensores

Además de puertos para conectar interfaces de comunicación tales como:

- Línea telefónica/comunicación GSM
- Líneas de alimentación AC/DC
- Líneas de comunicación de datos para Sistema Control-Sensores y Sistema Control-Tablero

De modo que se cuenta con un sistema capaz de monitorear el hogar aún cuando no hay suministro por parte de la red de alimentación principal.

Mediante la conexión con sensores y bocina, el Sistema de Seguridad para Hogares brinda protección a aquellos espacios críticos identificados por el usuario, con el respaldo de una bocina para mantener alerta al usuario en aquellas situaciones que sean pertinentes (detección por parte de alguno de los sensores, falla del sistema, entre otros)

Adicionalmente, cuenta con utilidades para tener una línea de contacto directa con el cuerpo de bomberos y la agencia de seguridad de preferencia en caso de alguna situación crítica.

4 Perspectiva del producto

El Sistema de Alarmas para el Hogar (SSH) es un sistema de seguridad diseñado para monitorear eventos de intrusión, emergencia y fallas en un área protegida (Hogar). Su propósito es detectar condiciones anormales y, en caso de hacerlo, notificar a los usuarios y a un centro de supervisión de una agencia de seguridad definida por el usuario en tiempo real.

El sistema opera mediante una serie de sensores (tipo contacto, movimiento e impacto) que envían señales de activación al módulo de control principal (hasta 16 sensores). Este módulo procesa los eventos y responde de acuerdo con la configuración establecida, activando alertas visuales (Teclado de Control), sonoras (Bocina) o enviando notificaciones remotas (Llamada a centro de atención de la agencia de seguridad).

El Sistema de Alarmas puede operar de manera independiente o integrarse con otros sistemas de seguridad. Su funcionalidad principal se basa en la interacción con los siguientes sistemas:

- Sensores físicos (contacto magnético, movimiento, vibración): detección de eventos.
- Teclado de Control: configuración, operación del sistema e interacción con el usuario en general.
- Pantalla LCD y LEDs indicadores: mostrar el estado del sistema.
- Bocina: alertas audibles.
- Interfaz protocolo GSM: Llamadas a Centro de Supervisión.
- Fuente de alimentación principal y batería de respaldo: garantizar operación continua.

Para su correcto funcionamiento, el sistema requiere de conexión a la red eléctrica, así como conectar el sistema al puerto GSM, instalar aquellos sensores compatibles con el sistema (hasta un máximo de 16 sensores).

4.1 Interfaces

4.1.1 Interfaces de sistema

- | | |
|--------------------|---|
| [SW-ID-100] | El sistema de control debe comunicarse con los sensores instalados y el Tablero mediante el protocolo de comunicación SPI. |
| [SW-ID-101] | Los LEDs del Tablero deben recibir comandos de activación y desactivación a través de señales discretas (GPIO). |
| [SW-ID-102] | La bocina debe recibir comandos de activación y desactivación a través de señales discretas (GPIO). |
| [SW-ID-103] | El sistema de control debe comunicarse con el centro de supervisión de la agencia de seguridad mediante el protocolo de comunicación GSM. |

4.1.2 Interfaces de usuario

- | | |
|--------------------|--|
| [SW-ID-104] | El Tablero debe contar con una pantalla LCD que muestre el Modo de Operación del Sistema, configuración del sistema de alarmas, mensajes de error y batería. |
| [SW-ID-105] | El Tablero debe contar con un teclado numérico e incluir teclas especiales para funciones de configuración y emergencias. |

Nota: Los siguientes son los caracteres especiales que deben incluirse en el Tablero:

- *
- #
- Esc
- Pánico
- Bomberos

[SW-ID-106] El sistema debe contar con dos LEDs en el Teclado que proporcionen información visual al usuario sobre la Batería y el estado de la alarma.

Nota: No es un requerimiento funcional. Establece una característica con la que debe contar el SSH. Otros requerimientos cubrirán el funcionamiento de los dos LEDs que se indican en este requerimiento

[SW-ID-107] El sistema debe emitir una señal sonora a través de la bocina para indicar los cambios de Modo de Operación del sistema de alarmas.

4.1.3 Interfaces de hardware

[SW-ID-108] El sistema de control debe ser compatible con sensores de tipo apertura de puertas y ventanas, movimiento e impacto.

[SW-ID-109] Los sensores deben conectarse mediante interfaces cableadas con el sistema de control.

[SW-ID-110] El sistema de control debe tener un máximo de 16 puertos de entrada para conexiones alámbricas con sensores.

[SW-ID-111] El sistema de control debe tener un máximo de un puerto para la conexión alámbrica con la bocina.

[SW-ID-112] El sistema de control debe contar con un puerto dedicado para la interfaz de comunicación de tipo GSM.

[SW-ID-113] El sistema de control debe tener un puerto de salida de alimentación DC para alimentación a periféricos conectados.

[SW-ID-114] El sistema de control debe contar con un puerto para la comunicación con el Tablero de control.

[SW-ID-115] El sistema de control debe contar con una batería de respaldo que garantice el funcionamiento del sistema de alarmas en caso de cortes del suministro principal de energía.

[SW-ID-116] El sistema de control debe contar con un puerto de alimentación principal que permita su operación con suministro eléctrico.

4.1.4 Interfaces de software

[SW-ID-117] El sistema de control debe comunicarse con el Tablero de control mediante un protocolo de comunicación SPI que consta de:

- 1 bit de inicio de comunicación.
- Formato de tramas de 8 bits.
- 1 bit de finalización de comunicación.
- El tiempo de respuesta máxima entre comandos es de 100ms +/-5%.

[SW-ID-118] El sistema de control debe interpretar la información enviada por los sensores donde:

- Bit Alerta en estado alto representa Sensor Activo

- Bit Alerta en estado bajo representa Sensor Inactivo.

[SW-ID-119] El sistema debe ser capaz de enviar mensajes de alerta al centro de supervisión de la agencia de seguridad en caso de eventos críticos.

[SW-ID-120] El software del Tablero de Control debe procesar entradas del usuario, producir salidas y mostrar información sobre el estado del sistema.

4.2 Interfaces de comunicación

[SW-ID-121] El sistema de control debe comunicarse con los sensores instalados mediante protocolos de comunicación SPI.

[SW-ID-122] El sistema de control debe comunicarse con los LEDs y bocina mediante señales discretas (GPIO).

[SW-ID-123] El sistema de control debe comunicarse con el Tablero de Control mediante el protocolo de comunicación SPI.

[SW-ID-124] El sistema debe monitorear el estado de la batería de respaldo y comunicar al Tablero de Control cualquier fallo o necesidad de carga.

[SW-ID-125] El sistema de control debe comunicarse con el centro de supervisión de la agencia de seguridad mediante el protocolo de comunicación GSM

4.3 Restricciones de memoria

[SW-ID-126] El software debe ocupar un máximo de 50% de la memoria RAM instalada en el Tablero de Control.

4.4 Modos de operación

[SW-ID-127] El sistema debe contar con los siguientes modos de operación:

- Modo 0
- Modo 1
- Desarmado
- Admin
- Ahorro

[SW-ID-128] Cuando se presente una falla en la fuente de alimentación principal, el sistema se debe mover al Modo de Operación Ahorro

[SW-ID-129] Cuando el usuario accione en el Tablero de control los comandos de ingreso a Modo 0, el sistema se debe mover al Modo de Operación Modo 0

[SW-ID-130] Cuando el usuario accione en el Tablero de control los comandos de ingreso a Modo 1, el sistema se debe mover al Modo de Operación Modo 1

[SW-ID-131] Cuando el usuario accione en el Tablero de control los comandos de ingreso a Modo Admin, el sistema se debe mover al Modo de Operación Admin

[SW-ID-132] Cuando el usuario accione en el Tablero de control los comandos de ingreso a Modo Desarmado, el sistema se debe mover al Modo de Operación Desarmado

4.5 Requerimientos de localización

[SW-ID-133] El sistema debe operar en condiciones ambientales donde la temperatura se encuentre dentro del rango de operación comprendido por 0 a 55 °C.

- [SW-ID-134]** El sistema debe operar en condiciones ambientales donde la presión se encuentre dentro del rango de operación comprendido por 80 a 110 kPa.
- [SW-ID-135]** El sistema debe operar en condiciones ambientales donde la humedad se encuentre dentro del rango de operación comprendido por 10% hasta 90% sin condensación.
- [SW-ID-136]** El sistema debe operar en condiciones eléctricas de alimentación igual a 110 VAC +/-10%.
- [SW-ID-137]** El sistema debe operar con un consumo máximo de corriente eléctrica definido como:
- 200mA +/-5% en Modo Reposo
 - 1 A +/-5% en Modo Armado (con la bocina activada)

5 Arquitectura de Software

El presente apartado describe la arquitectura del Sistema de Alarmas para Hogares, proporcionando una visión general de su estructura, los principales componentes y su interacción. La arquitectura ha sido diseñada para garantizar fiabilidad, modularidad y escalabilidad, permitiendo la integración de sensores, bocina, centro de control, panel principal y módulos de comunicación.

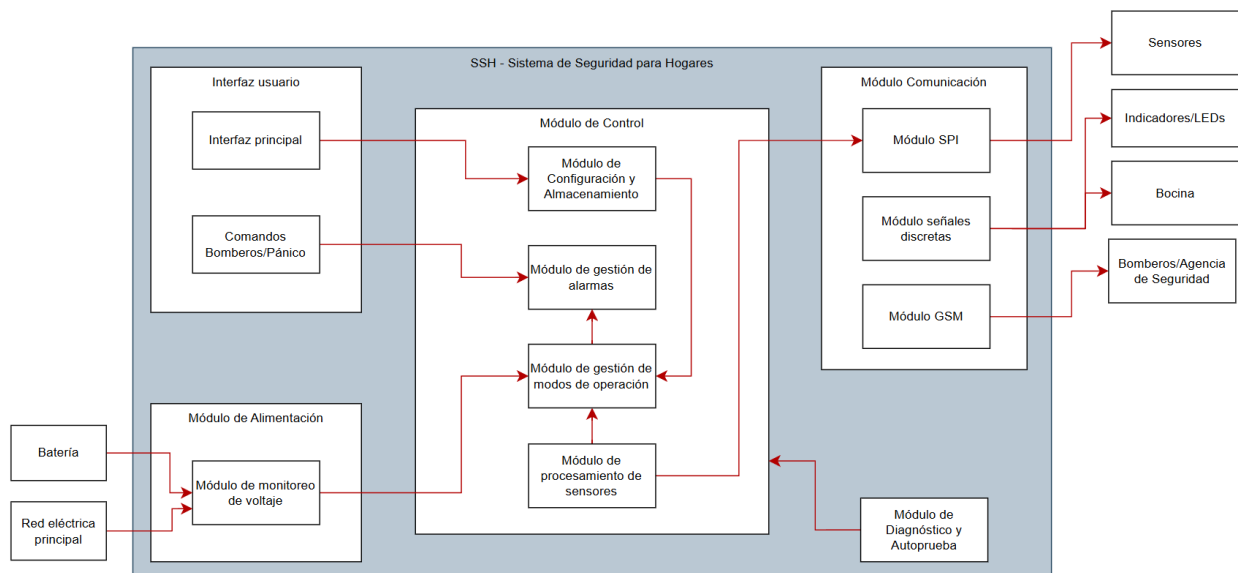


Figura 2. Diagrama de bloques funcionales

En el diagrama anterior se presentan los bloques funcionales del sistema, destacando los bloques principales:

- **Módulo de Control:** A través de este módulo se toman todas las decisiones del sistema. Se hace el procesamiento de datos desde la interfaz principales y elementos de hardware (como sensores, bocina, LEDs), así como la comunicación con demás agentes del sistema.
- **Interfaz de usuario:** Consta de la interfaz principal, la cual permite una interacción fluida entre el usuario y el sistema, de modo que comandos específicos puedan ser procesados

- **Modulo de Alimentación:** Encargado de proveer al sistema con la alimentación necesaria para su funcionamiento. Para garantizar esto cuenta con un sistema de alimentación principal y secundario (batería). Adicionalmente, un modulo que monitorea el nivel de la batería para garantizar que se encuentra en niveles aptos para la operación
- **Modulo de comunicación:** Modulo encargado de comunicar al sistema principal con los diferentes elementos de hardware (LEDs, indicadores, bocina, sensores, conexiones GSM).
- **Modulo de Diagnóstico y Auto prueba:** Este modulo permite realizar pruebas a nivel de sistema relacionados con fallas en la red de suministro eléctrico, así como fallas en sensores y llamados de auxilio. Este modo esta diseñado para realizar pruebas de funcionamiento y no necesariamente para el uso diario.

En las siguientes subsecciones se detallan los principales módulos del sistema, sus interacciones y los patrones de diseño utilizados para la implementación.

5.1 Módulo de Control

En el siguiente diagrama se presenta el flujo de funcionamiento del modulo de control en este de destacan los principales módulos de operación:

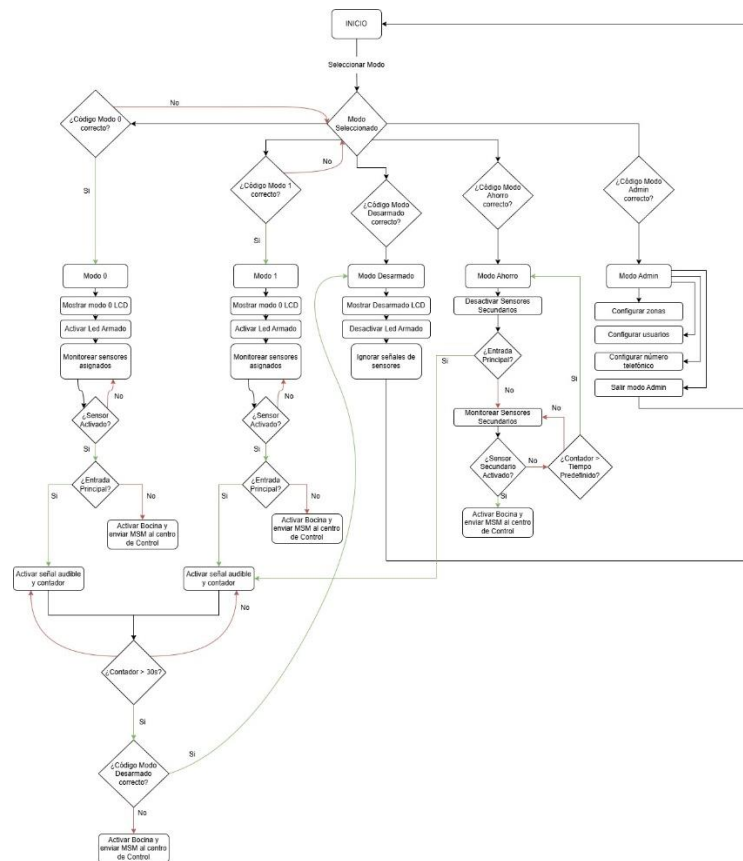


Figura 3 Diagrama de flujo de control

- **Modo Armado (0 y 1):** En estos modos, el sistema monitorea sensores asignados. Si un sensor detecta actividad, se verifica si es la entrada principal. Si es así, se activa una señal audible y se activa el contador para el ingreso del código de desarmado, si para el tiempo del contador supera los 30 segundos o el código es incorrecto se activa una bocina y se envía la alerta, de igual manera sucedería si el sensor no es la entrada principal. Cada modo tiene sensores asignados

independientes en el Modo 0 son todos los sensores y en el Modo 1 son algunos dependiendo de su configuración. Cada vez que se encuentra en el modo armado se activará un led en el panel para indicar este estado.

- **Modo Desarmado:** En este modo, el sistema ignora las señales de los sensores, permitiendo el acceso sin activar alarmas.
- **Modo Ahorro:** Se desactivan sensores secundarios y se monitorea solo la entrada principal. Si se detecta actividad en sensores secundarios, se evalúa un tiempo predefinido antes de activar una alerta. Este modo también permite realizar un desarmado siempre y cuando el sensor activado sea la entrada principal, el igual que el modo armado.
- **Modo Administrador:** Permite la configuración del sistema, como zonas de monitoreo, usuarios y números de contacto.

5.1.1 Diagrama de estados Modo Armado (0 y 1)

En los siguientes diagramas se representan los estados de funcionamiento del Modo 0 y el Modo 1 del sistema de alarma, ambos modos son similares su diferencia radica en los sensores a monitorear, de tal manera que para cada uno se destacan los siguientes estados:

- **Modo Init:** El sistema espera la secuencia de ingreso correcta para activar el Modo Armado. Esto es el código de activación de cada usuario para los diferentes modos provenientes de la interfaz del sistema.
- **Modo Operacional:** Una vez activado, el sistema habilita los sensores a monitorear, enciende el LED de "Armado" y muestra un mensaje en la interfaz principal.
- **Modo Falla:** Si se detecta una falla en los sensores mientras el sistema está en operación, se activa la bocina de alerta, se envía un mensaje SMS a la agencia de seguridad y se enciende el LED de "Alerta".

Para regresar al "Modo Operacional" la falla por la cual el sistema se movió hacia el estado "Modo Falla" debe estar inactiva. Adicionalmente, ningún otro sensor debe estar alarmado para poder realizar esta acción. Además, para poder salir del Modo Armado, ningún sensor debe estar alarmado, en caso contrario, el sistema continuará armado aunque la secuencia Desactivar "Modo 0" sea correcta.

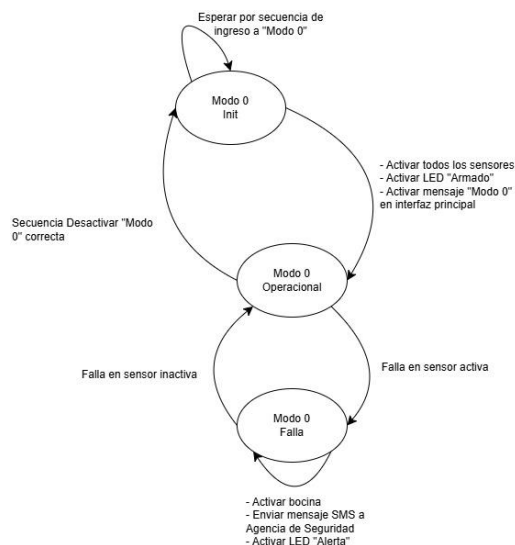


Figura 4 Diagrama de estados Modo 0

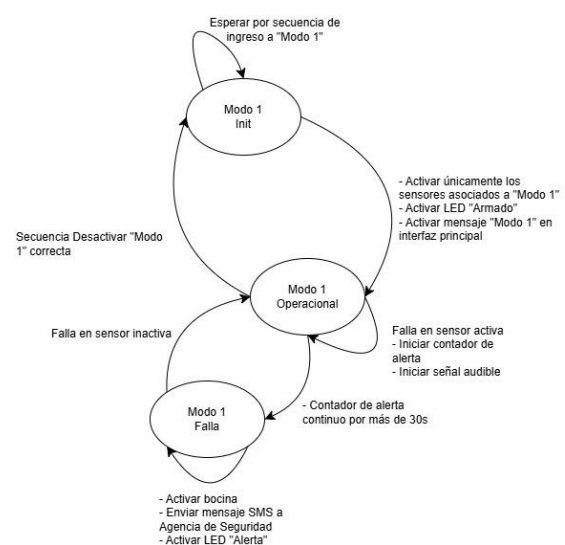


Figura 5 Diagrama de estados Modo 1

5.1.2 Diagrama de estados Modo Desarmado

El Modo Desarmado es un estado en el que el sistema de seguridad ignora las señales de los sensores, permitiendo el acceso libre sin activar alarmas. Este modo se activa cuando se ingresa un comando de desarmado (código) correcto proveniente de los modos 1 o 0. Al entrar en este modo, el sistema realiza las siguientes acciones:

- Desactiva el LED que indica el estado de "Armado", mostrando visualmente que el sistema no está monitoreando.
- Desactiva los indicadores de los modos de operación ("Modo 0" y "Modo 1"), ya que el sistema no está en ninguno de estos estados.
- Deja de escanear los sensores, lo que significa que no se monitorea ninguna actividad en los sensores asignados.

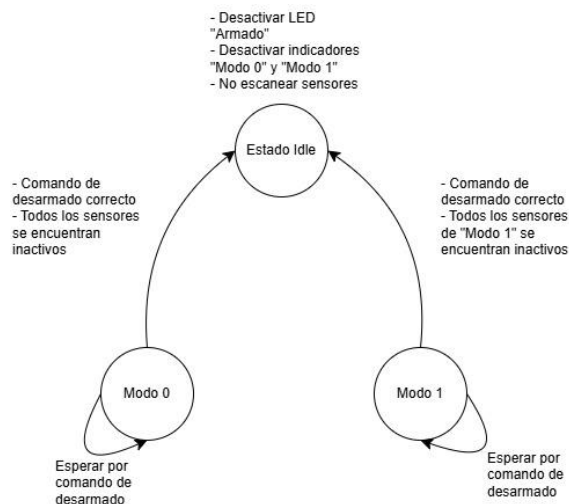


Figura 6 Diagrama de estados Modo Desarmado

5.1.3 Diagrama de flujo Ahorro de Batería

Este módulo tiene como objetivo principal mantener el sistema operativo en todo momento, utilizando dos fuentes de alimentación:

1. **Red eléctrica principal.**
2. **Batería.**

El sistema está diseñado para detectar fallas en cualquiera de las dos fuentes de energía y cambiar automáticamente a la fuente disponible, asegurando la continuidad del servicio. Para lograr esto, el sistema cuenta con un módulo de monitoreo de voltaje, que evalúa el nivel de carga de la batería en comparación con un voltaje límite previamente definido por el usuario.

En el diagrama se presentan los estados de la funcionalidad que tiene el sistema de alarma para realizar un ahorro eficiente de batería, donde se rescatan los principales estados:

- **Inicio:** El sistema comienza verificando si se ha definido un voltaje límite para la batería.
- **Definir Voltaje Límite:** Si no se ha definido un voltaje límite, el sistema procede a definir este valor.
- **Escanear Nivel de Batería:** El sistema escanea el nivel de voltaje de la batería.
- **Verificar Fuente de Alimentación:** El sistema verifica si la fuente de alimentación actual es la batería.
 - **Si es Batería:**
 - Compara el voltaje de la batería con el voltaje límite.
 - Si el voltaje de la batería es menor que el límite, cambia la fuente de alimentación a "Principal".
 - Desactiva el indicador de "Alarma" y el LED de "Batería".
 - **Si es Principal:**
 - Cambia la fuente de alimentación a "Batería".
 - Activa el indicador de "Alarma" y el LED de "Batería".

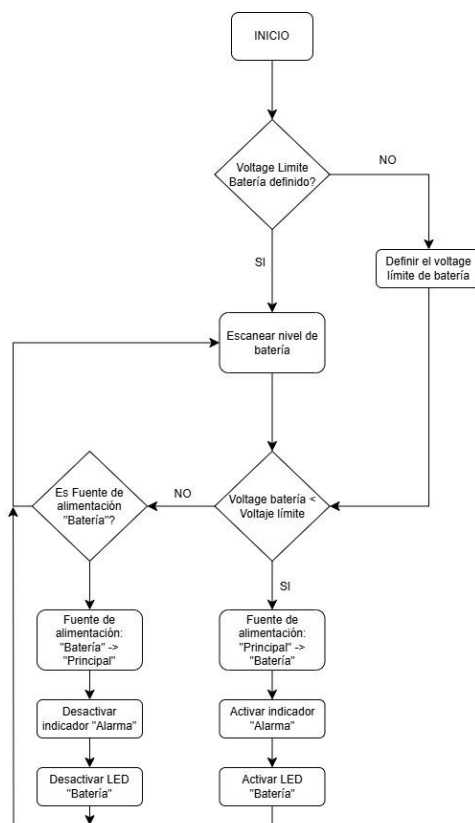


Figura 7 Diagrama de Flujo Ahorro de batería

5.1.3.1 Diagrama de estados Modo Ahorro

En el siguiente diagrama se representan los estados de funcionamiento del Modo Ahorro en el sistema de alarma, destacando los siguientes estados:

- **Modo Ahorro Init:** El sistema espera la secuencia de ingreso correcta para activar el Modo Ahorro. Esto es el código de activación de cada usuario proveniente de la interfaz del sistema.
- **Modo Ahorro Operacional:** En este estado, el sistema mantiene activos los sensores principales y desactiva los sensores secundarios si se supera un tiempo de inactividad definido por el usuario.
- **Modo Ahorro Limitado:** Si se detecta actividad en el sensor principal, los sensores secundarios vuelven a activarse. Si el sistema continúa inactivo por un tiempo mayor al definido por el usuario, se desactivan nuevamente los sensores secundarios.

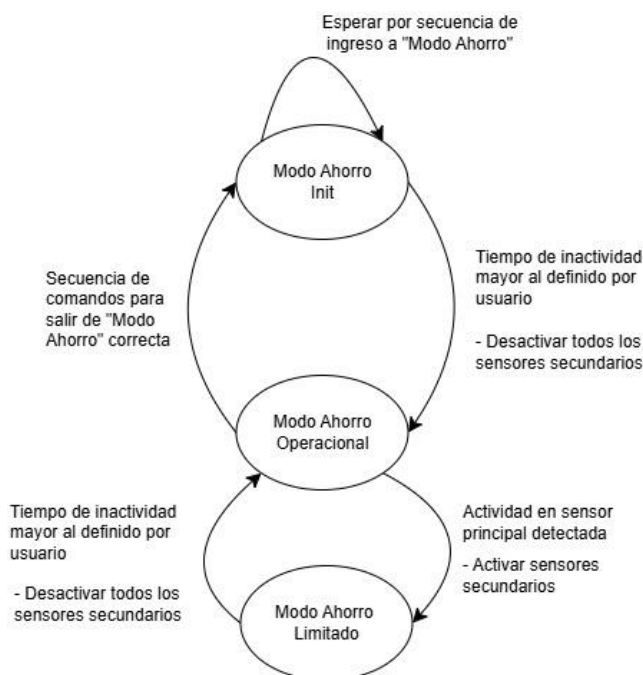


Figura 8 Diagrama de estados Modo Ahorro

5.1.4 Diagrama de flujo del modo administrador

En el diagrama de flujo del modo administrador se puede observar como este modo comienza con una verificación inicial, el sistema pregunta si la secuencia (código) ingresada por el usuario es correcta. Si no lo es, el sistema simplemente regresa al inicio y no permite el acceso. Sin embargo, si el código es correcto, el sistema entra en un estado de espera, listo para recibir la interacción del usuario y permitirle seleccionar una de las siguientes opciones:

- **Registro de usuario:** En esta opción, el sistema verifica si el número de usuario que se intenta registrar ya existe. Si el número está repetido, el sistema regresa al inicio. Si no está repetido, solicita una contraseña (que solo puede contener números). Si la contraseña cumple con los requisitos, el sistema guarda los datos del nuevo usuario, permitiéndole activar o desactivar los modos de operación en el futuro.
- **Registro de sensores:** El sistema primero verifica si ya hay 16 sensores registrados, que es el límite máximo. Si se alcanza este límite, el sistema regresa al inicio. Si aún hay espacio, el

sistema revisa si la entrada del sensor está activa. Si lo está, guarda los datos del nuevo sensor, permitiendo su uso en los modos de operación.

- **Modificar sensor:** El sistema verifica si el sensor que se desea modificar existe en la configuración actual. Si el sensor no existe, el sistema regresa al inicio. Si existe, permite realizar los cambios necesarios (como activar o desactivar el sensor) y guarda los datos actualizados.
- **Registro de número telefónico:** Esta opción permite configurar el número de teléfono al que se debe enviar un MSM en caso de una alerta. El sistema verifica si el número ingresado tiene un formato válido. Si no es válido, el sistema regresa al inicio. Si el formato es correcto, guarda el nuevo número para su uso en futuras notificaciones.
- **Salir del modo administrador:** Si el usuario selecciona esta opción, el sistema simplemente sale del modo administrador y regresa al inicio, listo para continuar con otras operaciones.

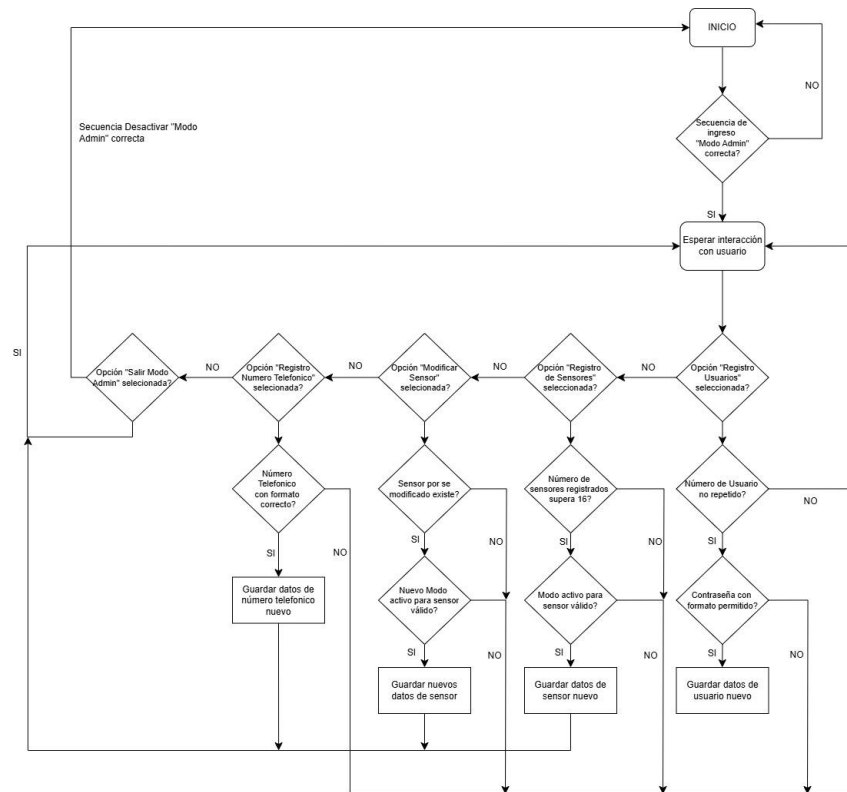


Figura 9 Diagrama de flujo del Modo Administrador

5.2 Interfaz principal

Para la interacción del Usuario con el Panel principal del SSH, se cuenta con la siguiente interfaz gráfica:

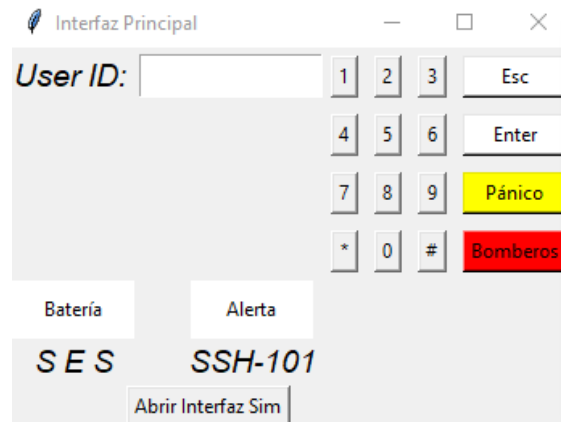


Figura 10 Interfaz principal Panel de Control

En donde se cuenta con:

- Botón "Esc": Permite al usuario limpiar el cuadro de texto (opciones de sistema)
- Botón "Enter": Permite al usuario continuar con el dialogo con el panel de control una vez que los caracteres deseados han sido digitados
- Botón "Pánico": Permite una opción rápida de acción cuando el usuario se encuentre en alguna situación no deseada, como entrada no deseada al hogar por un tercero, o cuando el usuario así lo desee. Comunicación directa con la Agencia de Seguridad.
- Botón "Bomberos": Permite una opción rápida de acción cuando el usuario se encuentre en alguna situación no deseada, como inicio de incendio o cuando así lo considere el usuario. Comunicación directa con el cuerpo de bomberos.
- Teclado alfanumérico: Permite al usuario interactuar con el cuadro de texto del panel, y de esta forma navegar entre las opciones disponibles
- LED "Batería": LED interacción SW-Usuario, indicando cuando existe una falla en el sistema a nivel de fuente de alimentación
- LED "Alerta": LED interacción SW-Usuario, indicando cuando existe alguna falla reportada por sensor, botón "Pánico" o "Bomberos"

Para el funcionamiento de la interfaz principal, se cuenta con el siguiente diagrama de flujo.

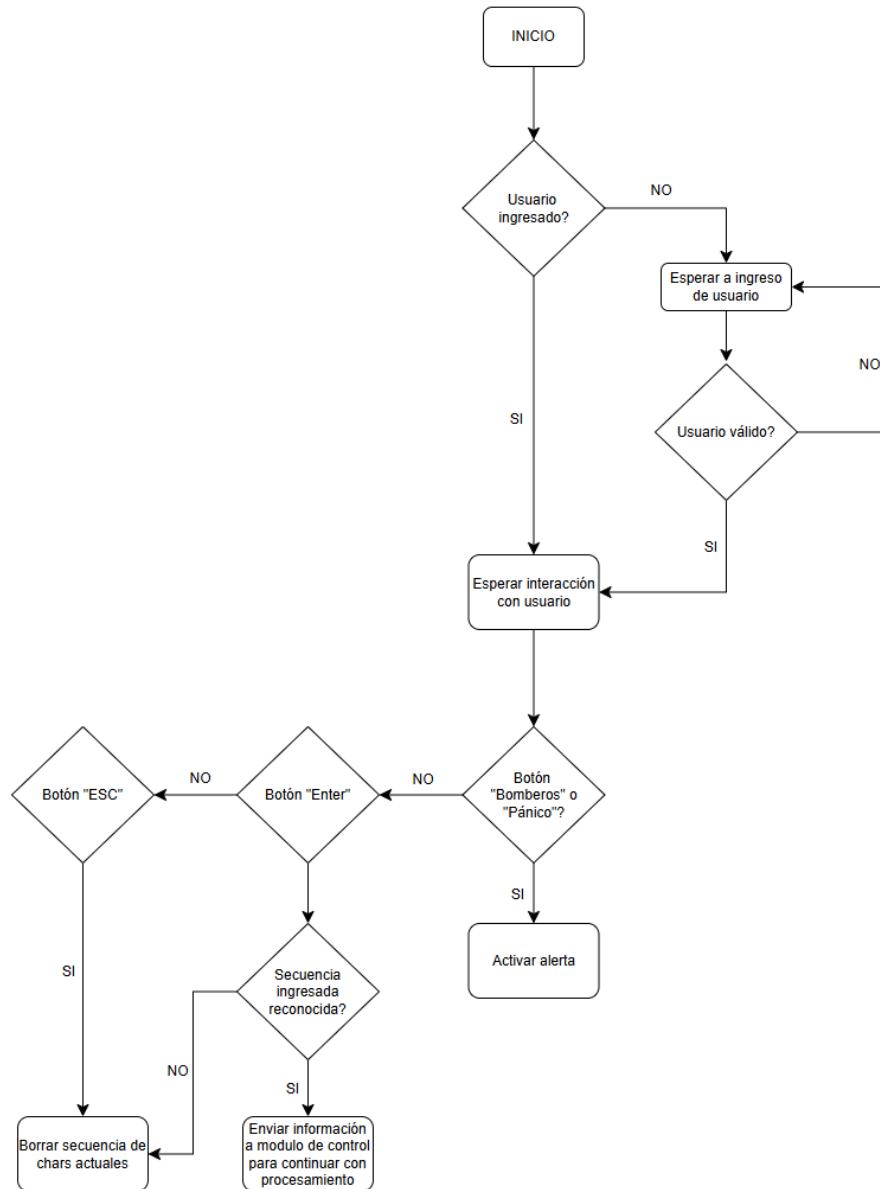


Figura 11 Diagrama de flujo interfaz principal

En el diagrama de flujo se resalta la necesidad de que exista un usuario válido para su operación, de otra forma los comandos no serán permitidos.

Adicionalmente, los botones especiales (bomberos y pánico) cuentan con una comunicación directa con el módulo de gestión de alarmas del modulo de control, de modo que, si alguna alarma se debe generar, se tenga la capacidad de iniciar los indicadores o alertas necesarias.

5.3 Módulo de Auto Prueba

Como parte del sistema de auto escaneo, se ofrece el botón “Abrir Interfaz Sim”:



Figure 12 Interfaz de simulación

Esta interfaz permite al usuario o técnico la interacción con el sistema, de modo que se pueda simular alguna falla en la red eléctrica de alimentación, así como una falla en el sensor o una respuesta positiva por parte del cuerpo de bomberos o de la agencia de seguridad.

6 Funciones del producto

El Sistema de Seguridad para Hogares proporciona seguridad a sus usuarios mediante la detección de eventos de intrusión y la activación de señales de alerta, así como la posibilidad de notificar al centro de ayuda de la agencia de seguridad de preferencia y a los bomberos según sea la necesidad.

En términos generales, las principales funciones del Sistema de Seguridad para Hogares constan de:

- Controlar los cambios entre Modos disponibles por el sistema.
- De esta forma, el sistema de Alarma se puede Armar o Desarmar, así como cambiar su forma de operación entre los distintos Modos disponibles.
- Monitorear el estatus de los sensores instalados en el sistema.
- Monitorear el nivel de la fuente de alimentación, de modo que se pueda alertar al usuario cuando existe algún evento referente con la fuente principal de alimentación o el sistema de respaldo mediante batería.
- Activar los distintos protocolos de alarmas dependiendo de la alerta activada
- Incendio, pánico, intrusión, entre otros.
- Permitir el almacenamiento de datos como:
 - Usuario
 - Sensores
 - Número telefónico del centro de supervisión de la agencia de seguridad

Adicionalmente de opciones para poder interactuar con el usuario por medio del Tablero de Control, brindando soluciones de control intuitivas y que facilitan el proceso de proteger el Hogar del usuario.

7 Características del usuario

El Sistema de Seguridad para Hogares tiene como público meta la población en general, siendo que debido a la versatilidad de este sistema se puede adaptar a distintas necesidades y escenarios.

1. Permite monitorear el hogar ante la ausencia de los inquilinos.

2. Permite monitorear personas adultas mayores en caso de complicaciones mediante el botón "Pánico".
3. Permite una interacción eficaz entre el usuario y el cuerpo de bomberos o el centro de atención de la agencia de seguridad ante situaciones apremiantes, tales como la intrusión al hogar o algún evento relacionado con incendios.

Adicionalmente, para el uso del sistema no se requiere de un nivel de conocimiento elevado en el mismo, ya que su diseño amigable con el usuario permite una ambientación rápida, haciendo que el funcionamiento del sistema sea transparente con el usuario meta.

Por lo anterior, el SSH no requiere conocimientos técnicos avanzados para su instalación. Sin embargo, se recomienda la asistencia por parte de técnicos capacitados en el área eléctrica para evitar inconvenientes.

Nota: Aclaración "Población en general". El SSH se encuentra enfocado en adultos jóvenes y mayores, siendo que su funcionamiento y control no se encuentra apto para el uso de niños.

8 Limitaciones

El Sistema de Seguridad para Hogares cuenta con una serie de limitaciones que se detalla a continuación:

1. El sistema debe operar en condiciones eléctricas de alimentación igual a 110 VAC +/-10%, en una configuración que opere a 60Hz.
2. El sistema debe operar con un consumo máximo de 1 A +/- 5% en su modo de mayor consumo.
3. La interfaz con el usuario se limita al Teclado del Centro de Control, siendo que la interacción entre el usuario y el sistema se limita al Teclado y su pantalla LCD, sin integrar soporte para pantallas táctiles o dispositivos móviles.
4. El software debe ocupar un máximo de 50% de la memoria RAM instalada en el Tablero de Control.
5. El sistema soporta un máximo de 16 sensores instalados, no existe posibilidad de un número mayor de sensores.
6. La comunicación entre sensores y el sistema de control será únicamente a través de interfaces cableadas, sin soporte para conexiones inalámbricas.
7. La comunicación remota (con fines exclusivos para comunicación con el cuerpo de bomberos o el centro de atención de la agencia de seguridad) será mediante el protocolo GSM, sin integración con Wi-Fi, Ethernet o protocolos similares.
8. Transmisión de datos se limita a mensajes SMS, sin transmisión de mensajes multimedia.

9 Suposiciones y dependencias

A continuación, se listan una serie de **suposiciones** para el funcionamiento correcto del Sistema de Seguridad para Hogares:

1. Se asume que la red eléctrica brindada por el usuario proporcionará un suministro estable de 110VAC +/-10% a 60Hz al sistema.
2. Se asume que los usuarios tienen conocimientos básicos en el uso de pantallas LCD y teclados alfanuméricos.
3. Se asume que las condiciones ambientales donde el sistema se encontrará instalado se apegan con los requerimientos ambientales del sistema, donde se establecen rangos operativos a nivel de humedad y temperatura para garantizar el correcto funcionamiento del sistema.
4. Se asume que el centro de atención de la agencia de seguridad está disponible para recibir alertas GSM en cualquier momento.

A continuación, se detallan una serie de **dependencias** que posee el SSH:

1. La disposición de los sensores en el Hogar dependerá del alcance del cableado disponible.
2. El correcto funcionamiento de supervisión de sensores por parte del centro de control dependerá que los sensores instalados correspondan estrictamente a la lista de sensores admitidos por el sistema.
3. El sistema depende de la disponibilidad de una red GSM funcional para la transmisión de alertas remotas.
4. El sistema depende de un suministro de emergencia por medio de baterías de respaldo en caso de falla del suministro, y que adicionalmente la batería se encuentre en buen estado.
5. El correcto funcionamiento de SSH dependerá de la instalación y configuración adecuada de los sensores según las especificaciones del fabricante.

10 Asignación de requerimientos

Componente	Requerimiento	Descripción
Centro de Control Validación de la lógica de comunicación entre el software y sensores, envío de datos y supervisión remota.	[SW-ID-100]	El sistema de control debe comunicarse con los sensores instalados y el Tablero mediante el protocolo de comunicación SPI.
	[SW-ID-103]	El sistema de control debe comunicarse con el centro de supervisión de la agencia de seguridad mediante el protocolo de comunicación GSM.
	[SW-ID-121]	El sistema de control debe comunicarse con los sensores instalados mediante protocolos de comunicación SPI.
	[SW-ID-125]	El sistema de control debe comunicarse con el centro de supervisión de la agencia de seguridad mediante el protocolo de comunicación GSM.
	[SW-4.3.4]	El sistema debe monitorear el estado de la batería de respaldo y comunicar al Tablero de Control cualquier fallo o necesidad de carga.
	[SW-ID-128]	Cuando se presente una falla en la fuente de alimentación principal, el sistema se debe mover al Modo de Operación Ahorro.
Interfaz de Usuario Software que maneja la pantalla, teclas y alertas en el sistema.	[SW-ID-104]	El Tablero debe contar con una pantalla LCD que muestre el Modo de Operación del Sistema, configuración del sistema de alarmas, mensajes de error y batería.
	[SW-ID-105]	El Tablero debe contar con un teclado numérico e incluir teclas especiales para funciones de configuración y emergencias.
	[SW-ID-106]	El sistema debe contar con dos LEDs en el Teclado que proporcionen información visual al usuario sobre la Batería y el estado de la alarma.
	[SW-ID-107]	El sistema debe emitir una señal sonora a través de la bocina para indicar los cambios de Modo de Operación del sistema de alarmas.
	[SW-ID-129]	Cuando el usuario accione en el Tablero de control los comandos de ingreso a Modo 0, el sistema se debe mover al Modo de Operación Modo 0.
	[SW-ID-130]	Cuando el usuario accione en el Tablero de control los comandos de ingreso a Modo 1, el sistema se debe mover al Modo de Operación Modo 1.
	[SW-ID-131]	Cuando el usuario accione en el Tablero de control los comandos de ingreso a Modo Admin, el sistema se debe mover al Modo de Operación Admin.
	[SW-ID-132]	Cuando el usuario accione en el Tablero de control los comandos de ingreso a Modo Desarmado, el sistema se debe mover al Modo de Operación Desarmado.
Manejo de Sensores Interpretación de señales de los sensores dentro del software.	[SW-ID-108]	El sistema de control debe ser compatible con sensores de tipo apertura de puertas y ventanas, movimiento e impacto.
	[SW-ID-109]	Los sensores deben conectarse mediante interfaces cableadas con el sistema de control.
	[SW-ID-110]	El sistema de control debe tener un máximo de 16 puertos de entrada para conexiones alámbricas con sensores.
	[SW-ID-122]	El sistema de control debe comunicarse con los LEDs y bocina mediante señales discretas (GPIO).
	[SW-ID-130]	Cuando el usuario accione en el Tablero de control los comandos de ingreso a Modo 1, el sistema se debe mover al Modo de Operación Modo 1.
Protocolos de Comunicación	[SW-ID-117]	El sistema de control debe comunicarse con el Tablero de control mediante un protocolo de comunicación SPI

Implementación de SPI, GPIO en el software.	[SW-ID-118]	El sistema de control debe interpretar la información enviada por los sensores donde: Bit Alerta en estado alto representa Sensor Activo. Bit Alerta en estado bajo representa Sensor Inactivo.
Interacción con Dispositivos Externos Software que maneja la conexión con otros dispositivos.	[SW-ID-111]	El sistema de control debe tener un máximo de un puerto para la conexión alámbrica con la bocina.
	[SW-ID-112]	El sistema de control debe contar con una puerto dedicado para la interfaz de comunicación de tipo GSM.
	[SW-ID-113]	El sistema de control debe tener un puerto de salida de alimentación DC para alimentación a periféricos conectados.
	[SW-ID-114]	El sistema de control debe contar con un puerto para la comunicación con el Tablero de control.
	[SW-ID-115]	El sistema de control debe contar con una batería de respaldo que garantice el funcionamiento del sistema de alarmas en caso de cortes del suministro principal de energía.
	[SW-ID-116]	El sistema de control debe contar con un puerto de alimentación principal que permita su operación con suministro eléctrico.
	[SW-ID-120]	El software del Tablero de Control debe procesar entradas del usuario, producir salidas y mostrar información sobre el estado del sistema.
	[SW-ID-124]	El sistema de control debe comunicarse con el Tablero de Control mediante el protocolo de comunicación SPI.
Procesamiento Tiempos de respuesta, condiciones y restricciones de memoria.	[SW-ID-116]	El sistema de control debe contar con un puerto de alimentación principal que permita su operación con suministro eléctrico.
	[SW-ID-126]	El software debe ocupar un máximo de 50% de la memoria RAM instalada en el Tablero de Control.
	[SW-ID-128]	Cuando se presente una falla en la fuente de alimentación principal, el sistema se debe mover al Modo de Operación Ahorro.
	[SW-ID-133]	El sistema debe operar en condiciones ambientales donde la temperatura se encuentre dentro del rango de operación comprendido por 0 a 55 °C.
	[SW-ID-134]	El sistema debe operar en condiciones ambientales donde la presión se encuentre dentro del rango de operación comprendido por 80 a 110 kPa.
	[SW-ID-135]	El sistema debe operar en condiciones ambientales donde la humedad se encuentre dentro del rango de operación comprendido por 10% hasta 90% sin condensación.
	[SW-ID-136]	El sistema debe operar en condiciones eléctricas de alimentación igual a 110 VAC +/-10%.
	[SW-ID-137]	El sistema debe operar con un consumo máximo de corriente eléctrica definido.
Alertas y Notificaciones Software para activar notificaciones, mensajes en pantalla y registros de eventos.	[SW-ID-119]	El sistema debe ser capaz de enviar mensajes de alerta al centro de supervisión de la agencia de seguridad en caso de eventos críticos.
	[SW-ID-130]	Cuando el usuario accione en el Tablero de control los comandos de ingreso a Modo 1, el sistema se debe mover al Modo de Operación Modo 1.

11 Interfaces externos

1. Interfaces de Sistema

El sistema deberá soportar interfaces de comunicación tipo SPI así como Señales Discretas (para comunicaciones internas entre los diversos componentes del sistema) y GSM (para comunicaciones con agentes externos al sistema) (SW-ID-100, SW-ID-101, SW-ID-102, SW-ID-103).

2. Interfaces de Usuario

El sistema deberá interactuar con el usuario mediante el Tablero de Control (SW-ID-104, SW-ID-105, SW-ID-106).

El sistema deberá contar con señales audibles para emitir alertas en caso de alguna emergencia (SW-ID-107).

3. Interfaces de Hardware

El sistema se conectará a sensores de apertura de puertas y ventanas, sensores de movimiento e impacto mediante conexiones cableadas (SW-ID-108, SW-ID-109, SW-ID-110).

La bocina se activará mediante una salida digital en un puerto GPIO (SW-ID-111).

La asistencia con el centro de atención de la agencia de seguridad se permitirá mediante una salida SMS en un puerto GSM (SW-ID-112).

El centro de control debe tener la capacidad de tener conectados dispositivos periféricos en puertos de alimentación DC dispuestos para dicho fin (SW-ID-113).

El sistema de control debe tener un puerto de comunicación dedicado a la comunicación con el Teclado de Control (SW-ID-114).

La alimentación principal será de 110 VAC, con una batería de respaldo incluida en el sistema de control (SW-ID-115, SW-ID-116).

4. Interfaces de Software

El Sistema de Control debe comunicarse con el Teclado de Control mediante una interfaz de comunicación SPI (SW-ID-117, SW-ID-120).

El sistema de Control interpretará las comunicaciones enviadas por los sensores mediante mensajes SPI (SW-ID-118, SW-ID-120).

El sistema de control deberá comunicarse con el centro de monitoreo de la agencia de seguridad utilizando el protocolo GSM (SW-ID-119, SW-ID-120).

El Tablero de Control deberá interactuar con el usuario, recibir entradas de datos y mostrar relación relevante al estado actual del SSH (SW-ID-120).

5. Interfaces de Comunicación

Las alertas remotas se enviarán a través de la red GSM utilizando mensajes de texto (SW-ID-125).

El Tablero de Control y el Teclado de Control se deberán comunicar mediante mensajes SPI (SW-ID-123, SW-ID-124).

Las alertas por parte de los sensores se enviarán a través de mensajes SPI (SW-ID-121).

Las alertas a los LEDs del Teclado del Control y la Bocina se transmitirán mediante puertos de entrada y salida GPIO (SW-ID-122).

12 Requerimientos

Durante esta sección, se presentarán los diversos requerimientos relacionados con la implementación del Sistema de Seguridad para Hogares.

12.1 Funciones

[SW-ID-1]

El software **debe** controlar mediante mensajes SPI los indicadores LCD en la pantalla del teclado: Modo 0, Modo 1, Batería y Error.

- [SW-ID-2]** El software **debe** controlar los indicadores LED "Armada" y "Batería" mediante los puertos asignados en la interfaz de comunicación GPIO.
- [SW-ID-5]** El software **debe** detectar que una alerta ha sido recibida por parte de un sensor si el sensor alertado envía una señal discreta de alarma (1).
- [SW-ID-6]** El software **debe** detectar que el sensor está desactivado (no alertado) si el sensor desactivado envía una señal discreta de NO alarma (0).
- [SW-ID-7]** El software **debe** activar la bocina mediante una señal GPIO en ALTO (1) en el puerto de comunicación asignado.
- [SW-ID-8]** El software **debe** desactivar la bocina mediante una señal GPIO en BAJO (0) en el puerto de comunicación asignado.
- [SW-ID-9]** El software **debe** activar el protocolo de alerta de incendio cuando se presione el botón "Incendio" del Teclado de Control.
- [SW-ID-10]** El software **debe** activar el protocolo de alerta de pánico cuando se presione el botón "Pánico" del Teclado de Control.
- [SW-ID-21]** El software **debe** contar únicamente con los siguientes modos de operación:
- Modo 0 (0)
 - Modo 1 (1)
 - Desarmado (2)
 - Admin (3)
 - Ahorro (4)
- [SW-ID-26]** El software **debe** almacenar todos los cambios de configuración en la memoria del sistema.
- [SW-ID-27]** El software **debe** guardar la siguiente información para cada sensor que forma parte del sistema de alarmas:
- Número de sensor
 - Zona
 - Estado (Activo o Inactivo)
- [SW-ID-29]** El software **debe** almacenar la información de asignación de zona de cada sensor en la memoria del sistema.
- [SW-ID-42]** El software **debe**:
- Interpretar la secuencia de comandos de Modo Admin.
 - Validar si la secuencia es correcta.
- [SW-ID-51]** El software **debe** mostrar un mensaje "Error" en la pantalla LCD si el usuario intenta registrar un nuevo usuario sin estar en Modo Admin.
- [SW-ID-52]** El software **debe** mostrar un mensaje "Error" si durante el proceso de guardar datos en memoria:
- Error en la escritura de datos en memoria ●
 - Error en la lectura de confirmación de datos.

Derivado: La escritura a memoria es un proceso necesario para el mantenimiento de datos, pero no se asocia directamente a un proceso en particular.

- [SW-ID-54]** Antes de guardar un número telefónico de la agencia de seguridad, el software **debe**:
- Validar que el sistema se encuentra en Modo Admin.
 - La opción seleccionada en Modo Admin es "Programación de número telefónico de la agencia de seguridad".
- [SW-ID-81]** Cuando se presione el botón "Incendio" del Teclado de Control, el software **debe**:
- Activar la bocina mediante una señal discreta de activación (1).
- [SW-ID-82]** Cuando se presione el botón "Incendio" del Teclado de Control, el software **debe** preparar un mensaje formato MSM con los siguientes datos:
- Modo del Sistema.
 - Usuario activo.
 - Palabra clave: "Incendio".
- [SW-ID-83]** Cuando se presione el botón "Incendio" del Teclado de Control, el software **debe** establecer comunicación con el centro de supervisión mediante el protocolo GSM y transmitir mensaje con el mismo formato establecido en el requerimiento anterior.
- [SW-ID-84]** Cuando se presione el botón "Pánico" del Teclado de Control, el software **debe**:
- Activar la bocina mediante una señal discreta de activación (1).
- [SW-ID-85]** Cuando se presione el botón "Pánico", el software **debe** preparar un mensaje formato MSM con los siguientes datos:
- Modo del Sistema.
 - Usuario activo.
 - Palabra clave: "Pánico".
- [SW-ID-86]** Cuando se presione el botón "Pánico" del Teclado de Control, el software **debe** establecer comunicación con el centro de supervisión mediante el protocolo GSM y transmitir mensaje con el mismo formato establecido en el requerimiento anterior.

12.2 Requerimientos de *usabilidad*

- [SW-ID-22]** En el Modo Admin, el software **debe** permitir al usuario ingresar y modificar el código de armado y desarmado.
- [SW-ID-23]** En el Modo Admin, el software **debe** permitir registrar nuevos usuarios con un código de acceso.
- [SW-ID-24]** En el Modo Admin, el software **debe** permitir registrar nuevos sensores y asignarlos a una zona.
- [SW-ID-25]** En el Modo Admin, el software **debe** permitir ingresar el número telefónico de la agencia de seguridad.
- [SW-ID-30]** El software **debe** permitir modificar la asignación de zona del sensor cuando se encuentra en Modo Admin.

- [SW-ID-38]** Durante el Modo Desarmado, el software **debe** permitir la interacción con el usuario para cambiar de modo de operación.
- [SW-ID-55]** El software **debe** detectar y validar la secuencia de comandos "Modo 0" ingresada por el usuario.
- [SW-ID-59]** El software **debe** detectar y validar la secuencia de comandos "Modo 1" ingresada por el usuario.
- [SW-ID-48]** El software **debe** asignar un número de usuario cuando se ingrese un usuario nuevo al sistema de alarmas.

12.3 Requerimientos de rendimiento

- [SW-ID-18]** El software debe monitorear el estado del voltaje de alimentación a una frecuencia de 1Hz+/-5%
- [SW-ID-69]** El software **debe** monitorear el estado de los sensores cuando el sistema está en Modo 0 a una frecuencia de 1Hz+/-5%.
- [SW-ID-73]** El software **debe** monitorear el estado de los sensores asignados únicamente a "Modo 1" cuando el sistema está en Modo 1 a una frecuencia de 0.5Hz.

12.4 Restricciones de diseño

- [SW-ID-13]** El software **debe** identificar cada sensor mediante un identificador único e incremental.
- Nota: No debe haber sensores con el mismo indicador (número de sensor). Es también aplicable a las Funciones del sistema
- [SW-ID-16]** El software **debe** ignorar señales provenientes de sensores no configurados o fuera del límite de 16 sensores.
- Nota: También aplicable como Requerimiento Funcional del Sistema
- [SW-ID-17]** El software debe generar una alerta si se detecta la conexión de más de 16 sensores mediante:
- Activación señal "Error" en panel LCD del Teclado de Control.
- Nota: También aplicable como Requerimiento Funcional del Sistema
- [SW-ID-28]** Como parte de la información guardada para cada sensor, el software **debe** aceptar Zonas iguales a 0 o 1, de otra forma rechazar la asignación de la zona de sensor.
- [SW-ID-31]** Cuando un sensor es asignado con un número de sensor igual a 0, el software **debe** asignarlo a la zona "Entrada Principal" (0).
- [SW-ID-32]** El software **debe** permitir asignar los sensores a las siguientes 2 zonas:
- Entrada Principal (0)
 - Interior Hogar (1)
- [SW-ID-39]** El software **debe** permitir configurar el tiempo de inactividad antes de activar el Modo Ahorro.

12.5 Estándares y regulaciones aplicables

- [SW-ID-49]** El software del sistema de alarma **debe** garantizar la compatibilidad y correcto funcionamiento con los dispositivos instalados bajo el estándar UL 1641, asegurando el cumplimiento de los requisitos de seguridad y operación del sistema.

12.6 Requerimientos funcionales

- [SW-ID-14]** El software **debe** procesar las señales de hasta 16 sensores y determinar si se ha producido un evento de alarma mediante las señales discretas recibidas por parte de los sensores en la interfaz GPIO.
- Nota: Es también aplicable a las Funciones del sistema.
- [SW-ID-15]** El software **debe** registrar el estado de cada sensor en memoria.
- Nota: Es también aplicable a las Funciones del sistema.
- [SW-ID-44]** Si el sistema se encuentra en:
- Modo 0 o
 - Modo 1
- Entonces el software **debe** verificar que todos los sensores estén desactivados antes de permitir la transición a Modo Admin.
- [SW-ID-45]** El software **debe** bloquear la transición a Modo Admin si las condiciones anteriores no se cumplen.

12.6.1 Modo 0

- [SW-ID-33]** Cuando el sistema se encuentra en Modo 0, el software **debe** monitorear el estado de todos los sensores instalados.
- [SW-ID-34]** Si cualquier sensor instalado detecta una condición de alarma en Modo 0, el software **debe** activar la bocina y enviar una señal de alerta.
- [SW-ID-56]** El software **debe** verificar que el sistema esté en Modo Desarmado antes de ejecutar la activación en Modo 0.
- [SW-ID-57]** El software **debe** actualizar el estado del sistema a "Modo 0" en el Teclado de Control mediante:
- Activación de LED "Armado"
 - Activación de mensaje "Modo 0" en la pantalla LCD.
- [SW-ID-58]** El software **debe** generar una señal de activación discreta para los sensores correspondientes al Modo 0.
- [SW-ID-70]** El software **debe** generar una señal de activación discreta (1) para la bocina cuando:
- Cualquier sensor es activado
 - El sistema se encuentra en Modo 0.
- [SW-ID-71]** El software **debe** preparar un mensaje formato MSM con los siguientes datos:
- Modo del Sistema.
 - Usuario activo.

- Sensor activo.

[SW-ID-72]

El software **debe** establecer una comunicación con el centro de supervisión mediante el protocolo GSM enviando el mensaje formateado en el requerimiento anterior.

12.6.2 Modo 1

[SW-ID-35]

Cuando el sistema se encuentra en Modo 1, el software **debe** monitorear únicamente los sensores asignados a la Zona 1.

[SW-ID-36]

Si cualquier sensor asignado a la Zona 1 detecta una condición de alarma en Modo 1, el software **debe** activar la bocina y enviar una señal de alerta.

[SW-ID-60]

El software **debe** verificar que el sistema esté en Modo Desarmado antes de ejecutar la activación en Modo 1.

[SW-ID-61]

El software **debe** actualizar el estado del sistema a "Modo 1" en el Teclado de Control mediante:

- Activación de LED "Armado"
- Activación de mensaje "Modo 1" en la pantalla LCD.

[SW-ID-62]

El software **debe** generar una señal de activación discreta para los sensores correspondientes al Modo 1.

[SW-ID-63]

El software **debe** generar una señal de desactivación discreta para los sensores no asignados al Modo 1.

[SW-ID-74]

Cuando el sistema se encuentra en "Modo 1", el software **debe** activar una señal audible mediante una señal discreta de activación (1) si:

- El sensor activado (alarmado) corresponde a "Entrada Principal".

[SW-ID-75]

Cuando el sistema se encuentra en "Modo 1", el software **debe** iniciar un contador si:

- El sensor activado (alarmado) corresponde a "Entrada Principal".

Nota: La función del contador será la de brindar una herramienta de conteo temporal al SW para determinar si la bocina debe ser accionada o no. Ver SW-ID-76.

[SW-ID-76]

El software **debe** generar una señal de activación discreta (1) para la bocina cuando:

- La señal audible haya sido emitida por 30 segundos o más (considerando una tolerancia de 5% del tiempo total).

[SW-ID-77]

El software **debe** desactivar la "señal audible" mediante una señal discreta de desactivación (0) si:

- La clave de desactivación es ingresada satisfactoriamente.

[SW-ID-78]

El software **debe** enviar una señal de desactivación discreta (0) para la bocina cuando:

- La señal audible está desactivada (0)

[SW-ID-79] El software **debe** preparar un mensaje formato MSM con los siguientes datos:

- Modo del Sistema.
- Usuario activo.
- Sensor activo.

[SW-ID-80] El software **debe** establecer comunicación con el centro de supervisión mediante el protocolo GSM y transmitir un mensaje con el formato establecido en el requerimiento anterior.

12.6.3 Modo Desarmado

[SW-ID-37] Cuando el sistema se encuentra en Modo Desarmado, el software **debe** ignorar las señales de los sensores.

[SW-ID-65] Mientras el sistema se encuentra en "Modo 0", el software debe mover su estado a "Desarmado" si:

- Comando "Desarmar" fue recibido exitosamente.
- Todos los sensores "Modo 0" están desactivados (no alarmados).

[SW-ID-66] Cuando el sistema mueve su estado de "Modo 0" a "Desarmado", el software debe actualizar el estado del sistema en el Teclado de Control mediante:

- Desactivación de LED "Armado"
- Activación de mensaje "Modo 0" en la pantalla LCD.

[SW-ID-67] Mientras el sistema se encuentra en "Modo 1", el software debe mover su estado a "Desarmado" si:

- Comando "Desarmar" fue recibido exitosamente.
- Todos los sensores "Modo 1" están desactivados (no alarmados).

[SW-ID-68] Cuando el sistema mueve su estado de "Modo 1" a "Desarmado", el software debe actualizar el estado del sistema en el Teclado de Control mediante:

- Desactivación de LED "Armado"
- Activación de mensaje "Modo 1" en la pantalla LCD.

12.6.4 Modo Ahorro

[SW-ID-40] Cuando el sistema se encuentra en Modo Ahorro, el software **debe** reactivar los sensores secundarios si se detecta actividad en el sensor "Entrada Principal".

[SW-ID-41] En el Modo Ahorro, el sistema **debe** desactivar los sensores secundarios cuando no se detecte actividad en un tiempo predefinido.

Nota: Sensores secundarios son todos aquellos sensores diferentes del sensor "Entrada Principal". El tiempo definido para apagar los sensores se define en el Modo Admin. Ver SYS-7.2.2 para más información.

12.7 Atributos de sistema

12.7.1 Requerimientos de confiabilidad

[SW-ID-93] El software **debe** implementar un mecanismo de watchdog para reiniciar el sistema en caso de falla inesperada del software.

Nota: El watchdog debe realizarse después de 50ms+/-5% de la detección de la falla.

[SW-ID-94] En caso de falla en la comunicación con el centro de supervisión, el software **debe** intentar reenviar la alerta hasta 3 veces, esperando 30 segundos entre intentos antes de generar una alerta de falla.

Nota: En caso de fallar por tercera vez, el mecanismo de watchdog reset puede resetear al software al detectar una falla.

[SW-ID-95] El software **debe** registrar en memoria eventos de fallas en sensores, comunicación y alimentación, con la siguiente información:

- Fecha y hora del fallo
- Tipo de fallo (sensor, alimentación, comunicación)
- Modo del sistema al momento del fallo

12.7.2 Requerimientos de seguridad

[SW-ID-43] El software **debe** validar si el sistema se encuentra en Modo Desarmado antes de cambiar a Modo Admin.

[SW-ID-46] En caso de bloqueo de transición hacia Modo Admin, el software **debe** mostrar un mensaje "Error" en la pantalla LCD.

[SW-ID-64] El software **debe** detectar y validar la secuencia de comandos "Desarmar" ingresada por el usuario.

12.7.3 Requerimientos de mantenibilidad

[SW-ID-89] El software **debe** permitir la actualización del firmware sin borrar los datos de configuración almacenados en memoria no volátil.

[SW-ID-90]

El software **debe** almacenar en memoria los eventos de activación de alarma con la siguiente información:

- Fecha y hora del evento
- Sensor activado
- Modo en el que se encontraba el sistema

[SW-ID-91] El software **debe** permitir el restablecimiento de todos los parámetros a valores predeterminados cuando el usuario seleccione la opción "Restaurar Fábrica" en Modo Admin.

[SW-ID-87] El software **debe** incluir una función para ejecutar una prueba de activación en cada sensor.

12.7.4 Requerimientos de portabilidad

- [SW-ID-88]** El software **debe** reconocer y gestionar los tres tipos de sensores (apertura de puertas y ventanas, movimiento e impacto), permitiendo su configuración y monitoreo.
- [SW-ID-92]** El software debe permitir la configuración de zonas o grupos de sensores de manera flexible, admitiendo la adición o eliminación de sensores sin requerir modificaciones en el código fuente.

12.7.5 Otros requerimientos

- [SW-ID-3]** Cuando la fuente de alimentación no se encuentra activa (fallo eléctrico, error en suministro principal, entre otros), el software **debe** actualizar el indicador de fuente de alimentación en la pantalla de "Principal" a "Batería".
- [SW-ID-4]** Cuando el nivel de voltaje de la batería es mayor o igual que un valor determinado, el software **debe** desactivar el LED de alarma de batería en el Teclado de Control mediante una señal GPIO en BAJO (0) en el puerto de comunicación asignado, de lo contrario la señal GPIO debe permanecer en ALTO (1).
- [SW-ID-11]** Cuando el nivel de voltaje de alimentación de la batería es mayor o igual que un valor determinado y la fuente de alimentación principal se encuentra disponible, el software debe cambiar la fuente de alimentación de "Batería" a "Principal".
- [SW-ID-12]** Cuando el nivel de voltaje de alimentación de la batería es menor que un valor determinado y la fuente de alimentación principal no se encuentra disponible, el software debe cambiar la fuente de alimentación de "Principal" a "Batería".
- [SW-ID-19]** Si el voltaje de alimentación cae por debajo del umbral determinado y la fuente de alimentación no se encuentra disponible, el software **debe**:
- Activar el indicador de alarma en la pantalla del teclado.
 - Encender el LED respectivo a la alarma "Batería"
- [SW-ID-20]** Si el voltaje de alimentación se encuentra por encima del umbral determinado y la fuente de alimentación principal se encuentra disponible, el software **debe**:
- Desactivar el indicador de alarma en la pantalla del teclado.
 - Apagar el LED respectivo a la alarma "Batería"

Apéndices

Apéndice 1. Matriz de Trazabilidad Requerimientos de Sistema – Requerimientos de Software

ID - Requerimiento de sistema	ID - Requerimiento de software
[SYS-6.3.1]	[SW-ID-1]
	[SW-ID-2]
	[SW-ID-3]
	[SW-ID-4]
[SYS-6.3.2]	[SW-ID-5]
	[SW-ID-6]
[SYS-6.3.3]	[SW-ID-7]
	[SW-ID-8]
[SYS-6.3.4]	[SW-ID-9]
	[SW-ID-10]
[SYS-6.3.5]	[SW-ID-11]
	[SW-ID-12]
[SYS-6.3.6]	[SW-ID-13]
	[SW-ID-14]
	[SW-ID-15]
	[SW-ID-16]
	[SW-ID-17]
[SYS-6.3.7]	[SW-ID-88]
[SYS-6.3.8]	[SW-ID-89]
[SYS-6.3.9]	[SW-ID-90]
[SYS-6.3.10]	[SW-ID-91]
[SYS-6.3.11]	[SW-ID-92]
[SYS-6.3.12]	[SW-ID-93]
[SYS-6.3.13]	[SW-ID-94]
[SYS-6.3.14]	[SW-ID-95]
[SYS-7.1.1]	[SW-ID-18]
	[SW-ID-19]

	[SW-ID-20]
[SYS-7.1.2]	[SW-ID-87]
[SYS-7.2.1]	[SW-ID-21]
[SYS-7.2.2]	[SW-ID-22]
	[SW-ID-23]
	[SW-ID-24]
	[SW-ID-25]
	[SW-ID-26]
[SYS-7.2.3]	[SW-ID-27]
	[SW-ID-28]
	[SW-ID-29]
[SYS-7.2.4]	[SW-ID-30]
	[SW-ID-31]
[SYS-7.2.5]	[SW-ID-32]
[SYS-7.2.6]	[SW-ID-33]
	[SW-ID-34]
[SYS-7.2.7]	[SW-ID-35]
	[SW-ID-36]
[SYS-7.2.8]	[SW-ID-37]
	[SW-ID-38]
[SYS-7.2.9]	[SW-ID-39]
	[SW-ID-40]
	[SW-ID-41]
[SYS-7.2.10]	[SW-ID-42]
	[SW-ID-43]
	[SW-ID-44]
	[SW-ID-45]
	[SW-ID-46]
[SYS-7.2.11]	[SW-ID-51]
[SYS-7.2.12]	[SW-ID-48]
[SYS-7.2.14]	[SW-ID-54]
[SYS-7.3.1]	[SW-ID-55]

	[SW-ID-56]
	[SW-ID-57]
	[SW-ID-58]
[SYS-7.3.2]	[SW-ID-59]
	[SW-ID-60]
	[SW-ID-61]
	[SW-ID-62]
	[SW-ID-63]
[SYS-7.3.3]	[SW-ID-64]
	[SW-ID-65]
	[SW-ID-66]
	[SW-ID-67]
	[SW-ID-68]
[SYS-7.4.1]	[SW-ID-69]
	[SW-ID-70]
	[SW-ID-71]
	[SW-ID-72]
[SYS-7.4.2]	[SW-ID-73]
	[SW-ID-74]
	[SW-ID-75]
[SYS-7.4.3]	[SW-ID-76]
	[SW-ID-79]
	[SW-ID-80]
[SYS-7.4.4]	[SW-ID-77]
	[SW-ID-78]
[SYS-7.4.5]	[SW-ID-81]
	[SW-ID-82]
	[SW-ID-83]
[SYS-7.4.6]	[SW-ID-84]
	[SW-ID-85]
	[SW-ID-86]
[SYS-6.2.1]	[SW-ID-49]

Apéndice 2. Matriz de Trazabilidad Requerimiento de Software – Funciones implementadas

ID - Requerimiento de software	ID – Función
[SW-ID-1]	handle_sensor_alert() on_button_click()
[SW-ID-2]	verify_PS() update_label()
[SW-ID-3]	verify_PS()
[SW-ID-4]	verify_PS()
[SW-ID-5]	_check_activated_sensors()
[SW-ID-6]	handle_sensor_alert() on_button_click()
[SW-ID-7]	handle_sensor_alert() on_button_click()
[SW-ID-8]	handle_sensor_alert() on_button_click()
[SW-ID-9]	on_button_click()
[SW-ID-10]	on_button_click()
[SW-ID-11]	verify_PS()
[SW-ID-12]	verify_PS()
[SW-ID-13]	Var Sensors_list
[SW-ID-14]	handle_sensor_alert()
[SW-ID-15]	save_sensors_list()
[SW-ID-16]	Var Sensors_list
[SW-ID-17]	admin_mode_sm()
[SW-ID-88]	actualizar_sensor()
[SW-ID-89]	read_Users_list() read_utils_list() read_sensors_list()
[SW-ID-90]	format_alert_message()
[SW-ID-91]	rest_system()
[SW-ID-92]	actualizar_sensor()
[SW-ID-93]	-

[SW-ID-94]	-
[SW-ID-95]	format_alert_message()
[SW-ID-18]	verify_PS()
[SW-ID-19]	verify_PS()
[SW-ID-20]	verify_PS()
[SW-ID-87]	class SimSensors
[SW-ID-21]	on_button_click() admin_mode_sm() class Modo1Monitor class Modo0Monitor
[SW-ID-22]	admin_mode_sm()
[SW-ID-23]	admin_mode_sm()
[SW-ID-24]	admin_mode_sm()
[SW-ID-25]	admin_mode_sm()
[SW-ID-26]	save_Codes_list() read_Codes_list() admin_mode_sm()
[SW-ID-27]	Var Sensors_list
[SW-ID-28]	admin_mode_sm()
[SW-ID-29]	save_sensors_list()
[SW-ID-30]	admin_mode_sm()
[SW-ID-31]	admin_mode_sm()
[SW-ID-32]	admin_mode_sm()
[SW-ID-33]	_check_activated_sensors()
[SW-ID-34]	handle_sensor_alert()
[SW-ID-35]	_check_activated_sensors()
[SW-ID-36]	_check_activated_sensors()
[SW-ID-37]	on_button_click()
[SW-ID-38]	on_button_click()
[SW-ID-39]	_evaluate_secondaries()
[SW-ID-40]	_get_active_main_sensors()
[SW-ID-41]	_deactivate_secondaries()
[SW-ID-42]	on_button_click()
[SW-ID-43]	on_button_click()
[SW-ID-44]	on_button_click()

[SW-ID-45]	on_button_click()
[SW-ID-46]	on_button_click()
[SW-ID-51]	admin_mode_sm()
[SW-ID-48]	admin_mode_sm()
[SW-ID-54]	admin_mode_sm()
[SW-ID-55]	on_button_click()
[SW-ID-56]	on_button_click()
[SW-ID-57]	update_label()
[SW-ID-58]	start_monitoring()
[SW-ID-59]	on_button_click()
[SW-ID-60]	on_button_click()
[SW-ID-61]	update_label()
[SW-ID-62]	_check_activated_sensors()
[SW-ID-63]	_check_activated_sensors()
[SW-ID-64]	on_button_click()
[SW-ID-65]	stop_monitoring()
[SW-ID-66]	update_label()
[SW-ID-67]	start_monitoring()
[SW-ID-68]	update_label()
[SW-ID-69]	_monitor_loop()
[SW-ID-70]	_check_activated_sensors()
[SW-ID-71]	format_alert_message()
[SW-ID-72]	handle_sensor_alert()
[SW-ID-73]	_monitor_loop()
[SW-ID-74]	handle_sensor_alert()
[SW-ID-75]	handle_sensor_alert()
[SW-ID-76]	_trigger_delayed_alert()
[SW-ID-79]	format_alert_message()
[SW-ID-80]	format_alert_message()
[SW-ID-77]	on_button_click()
[SW-ID-78]	on_button_click()
[SW-ID-81]	on_button_click()
[SW-ID-82]	on_button_click()
[SW-ID-83]	on_button_click()

[SW-ID-84]	on_button_click()
[SW-ID-85]	on_button_click()
[SW-ID-86]	on_button_click()
[SW-ID-49]	-
[SW-ID-52]	admin_mode_sm()

Apéndice 3. Matriz de Trazabilidad Requerimiento de Software – Casos de Prueba

ID - Requerimiento de software	ID – Caso de Prueba
[SW-ID-3]	TP-BAT-002 TP-BAT-004 TP-BAT-006 TP-BAT-008 TP-BAT-010 TP-BAT-012 TP-BAT-014 TP-BAT-016 TP-BAT-018 TP-BAT-020 TP-BAT-022 TP-BAT-024 TP-BAT-026 TP-BAT-028
[SW-ID-4]	TP-BAT-001 TP-BAT-003 TP-BAT-005 TP-BAT-007 TP-BAT-009 TP-BAT-011 TP-BAT-013 TP-BAT-015 TP-BAT-017

	TP-BAT-019 TP-BAT-021 TP-BAT-023 TP-BAT-025 TP-BAT-027
[SW-ID-11]	TP-BAT-002 TP-BAT-004 TP-BAT-006 TP-BAT-008 TP-BAT-010 TP-BAT-012 TP-BAT-014 TP-BAT-016 TP-BAT-018 TP-BAT-020 TP-BAT-022 TP-BAT-024 TP-BAT-026 TP-BAT-028
[SW-ID-12]	TP-BAT-002 TP-BAT-004 TP-BAT-006 TP-BAT-008 TP-BAT-010 TP-BAT-012 TP-BAT-014 TP-BAT-016 TP-BAT-018 TP-BAT-020 TP-BAT-022 TP-BAT-024 TP-BAT-026 TP-BAT-028
[SW-ID-19]	TP-BAT-001 TP-BAT-003

	TP-BAT-005 TP-BAT-007 TP-BAT-009 TP-BAT-011 TP-BAT-013 TP-BAT-015 TP-BAT-017 TP-BAT-019 TP-BAT-021 TP-BAT-023 TP-BAT-025 TP-BAT-027
[SW-ID-20]	TP-BAT-001 TP-BAT-003 TP-BAT-005 TP-BAT-007 TP-BAT-009 TP-BAT-011 TP-BAT-013 TP-BAT-015 TP-BAT-017 TP-BAT-019 TP-BAT-021 TP-BAT-023 TP-BAT-025 TP-BAT-027
[SW-ID-81]	TP-INC-PANIC-001 TP-INC-PANIC-002
[SW-ID-82]	TP-INC-PANIC-001 TP-INC-PANIC-003 TP-INC-PANIC-004 TP-INC-PANIC-005
[SW-ID-84]	TP-INC-PANIC-006 TP-INC-PANIC-007
[SW-ID-85]	TP-INC-PANIC-006

	TP-INC-PANIC-008 TP-INC-PANIC-009 TP-INC-PANIC-010
[SW-ID-71]	TP-MP0-000 TP-MP0-005 TP-MP0-006 TP-MP0-07
[SW-ID-33]	TP-MP0-001
[SW-ID-34]	TP-MP0-001 TP-MP0-002 TP-MP0-003 TP-MP0-004
[SW-ID-57]	TP-MP0-001
[SW-ID-58]	TP-MP0-002 TP-MP0-003 TP-MP0-004
[SW-ID-70]	TP-MP0-004
[SW-ID-37]	TP-DES-000 TP-DES-003
[SW-ID-65]	TP-DES-001
[SW-ID-66]	TP-DES-002 TP-DES-003