SISTEMA INTELIGENTE PARA MONITORIZAR PERSONAS MAYORES Y/O DEPENDIENTES

INTRODUCCIÓN

Objetivo del sistema

Proporcionar a las personas mayores y/o dependientes que viven solas, un sistema inteligente con carácter **no intrusivo** para que en caso de alguna urgencia que pueda afectar su bienestar:

- Alerte a sus cuidadores, responsables y/o tutores.
- Sea capaz de anticiparse a posibles situaciones de riesgo y actuar en consecuencia.

Requerimientos funcionales (I)

Cada persona mayor y/o dependiente llevaría consigo una **pulsera** para monitorizar algunas de sus funciones vitales así como su ubicación dentro y fuera de casa.

Un **botón de ayuda** que dependiendo del nivel de la alerta, se trasladaría la emergencia al móvil del personal especializado o bien a familiares y/o tutores.

Sensores de presión, con el objeto de poder determinar si se encuentra acostado en la cama o sentado en diferentes sillones.

Requerimientos funcionales (I)

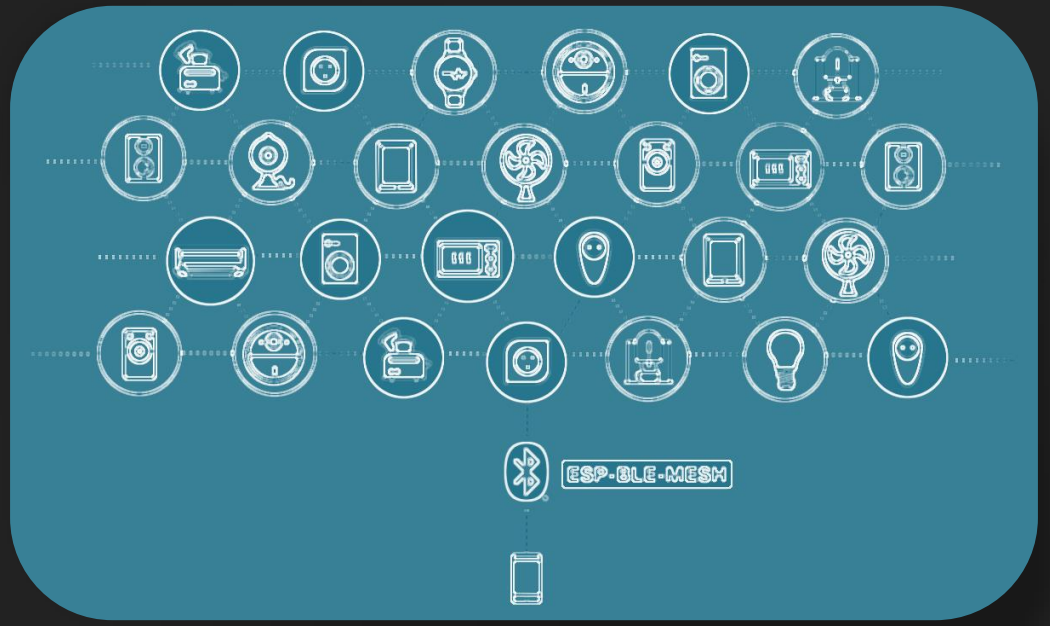
El sistema alertará cuando se detecte una **caída** u otras emergencias observadas por un comportamiento anormal derivado del aprendizaje con Inteligencia Artificial.

Requerimientos funcionales (II)

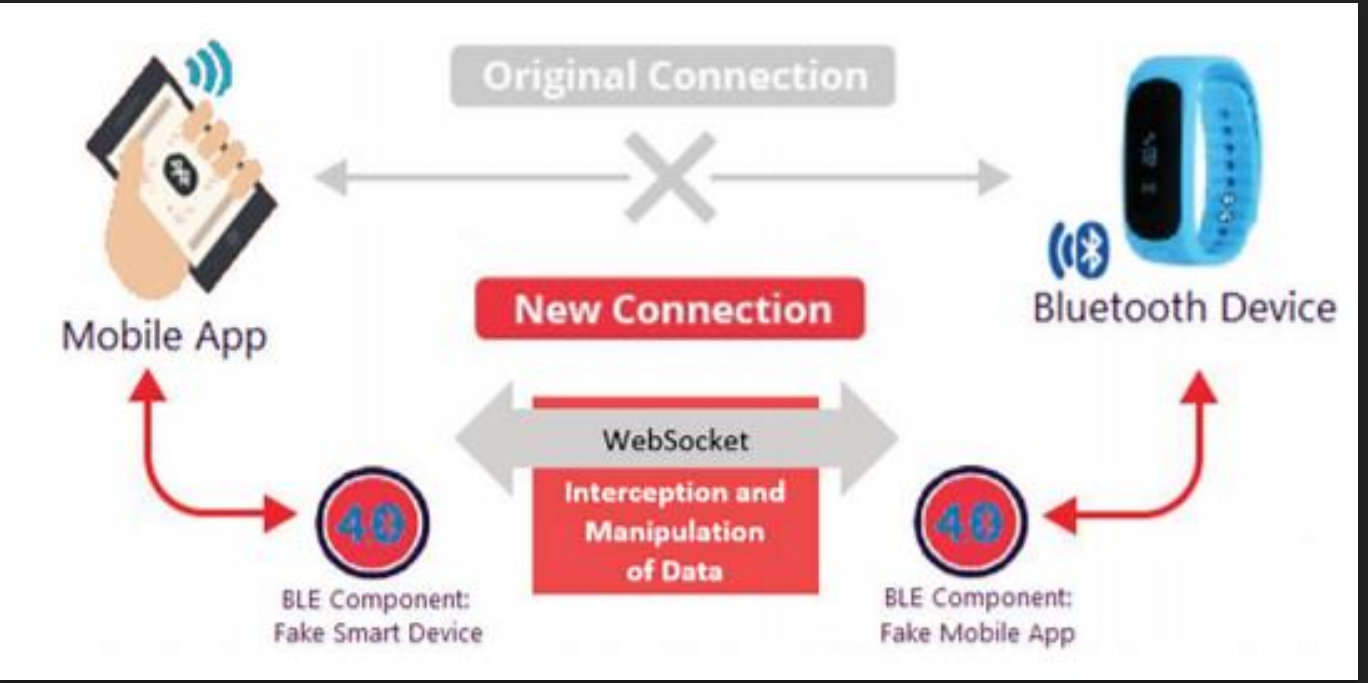
Para avisar ante una situación de emergencia, se incluirá un **altavoz inteligente** que permitirá a las personas mayores o dependientes interactuar con el dispositivo a través de la voz natural, consiguiendo de esta forma **solicitar que se realice una llamada** según la gravedad del momento o establecer **alarmas**.

Requerimientos de seguridad (I)

Dentro de las medidas de seguridad más relevantes en este sistema, se haría énfasis en tener controladas ciertas amenazas en **dispositivos Bluetooth** al ser la parte fundamental de este diseño, además de parchear sistemas operativos, ordenadores, routers y aplicaciones en general.



Requerimientos de seguridad (II)



Requerimientos de seguridad (III)

A fin de mitigar posibles ataques y vulnerabilidades del sistema, se incluirán procedimientos para salvaguardar:

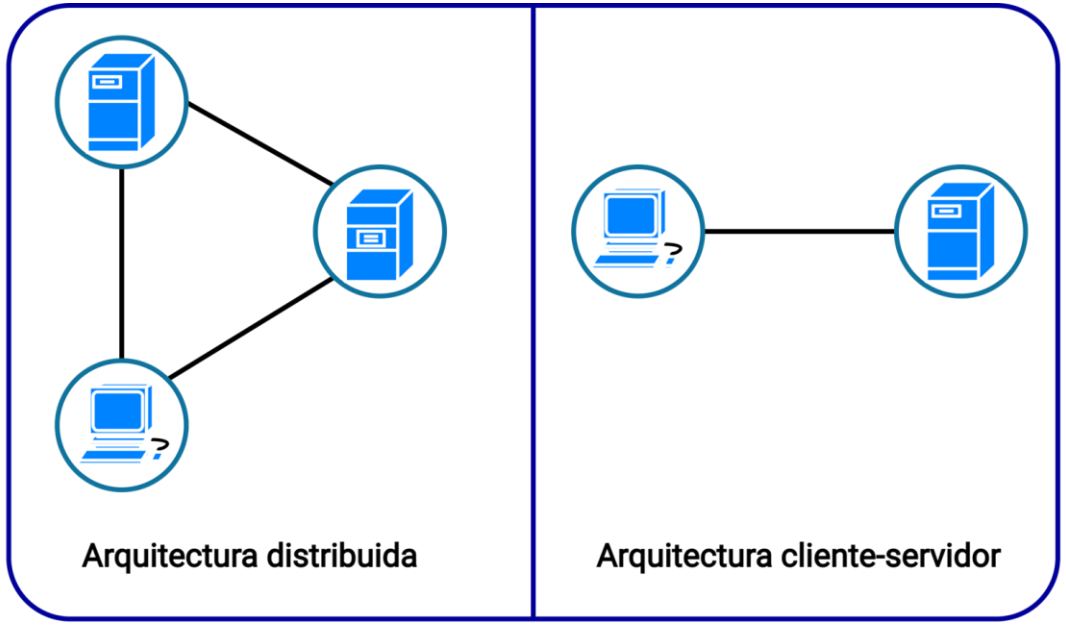
- Posibles **ataques de IoT**.
- Asegurar con proveedores las **aplicaciones en la nube**.
- Crear **procedimientos de cifrado** para garantizar la autenticidad de quien envía, el origen de la información y que esta no haya sufrido alteraciones durante la transmisión.

DISEÑO DE LA ARQUITECTURA

Diseño de la arquitectura

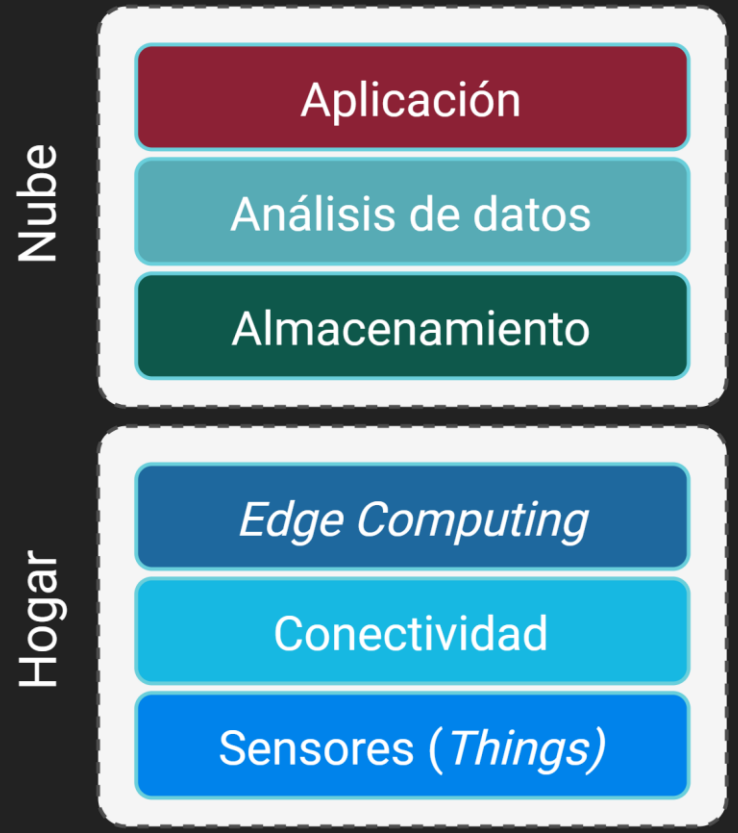
Patrones de arquitectura seguidos:

- Arquitectura **distribuida**
- Arquitectura **cliente/servidor**
- Arquitectura **IoT**
- Arquitectura en la **nube**
- Edge computing

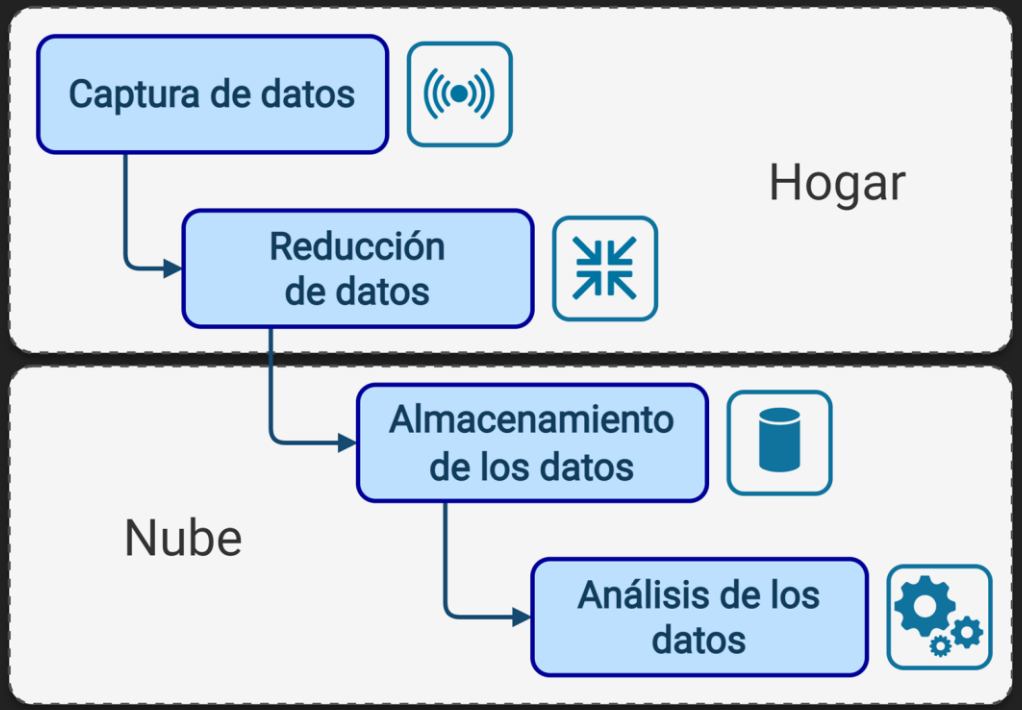


Diseño de la arquitectura

Capas Internet of Things (IoT)

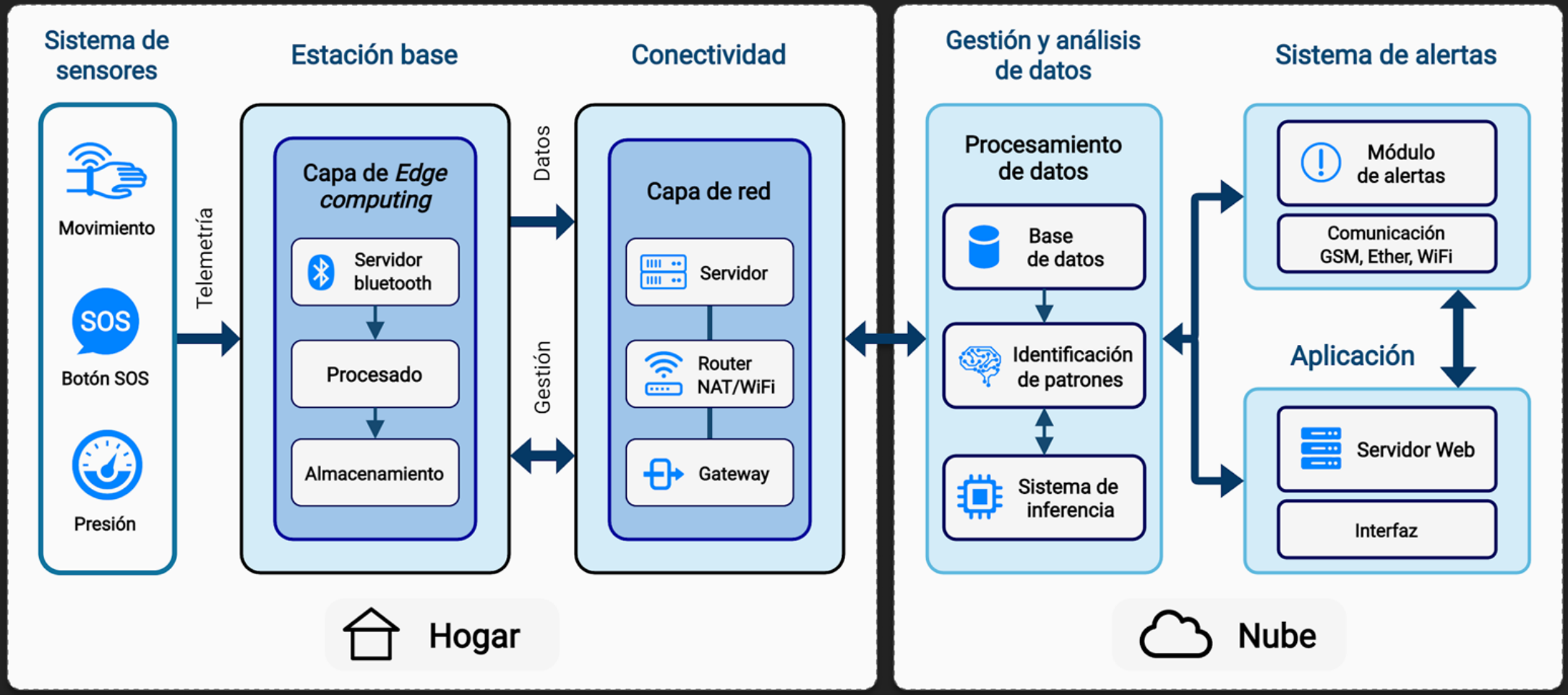


El procesamiento de datos



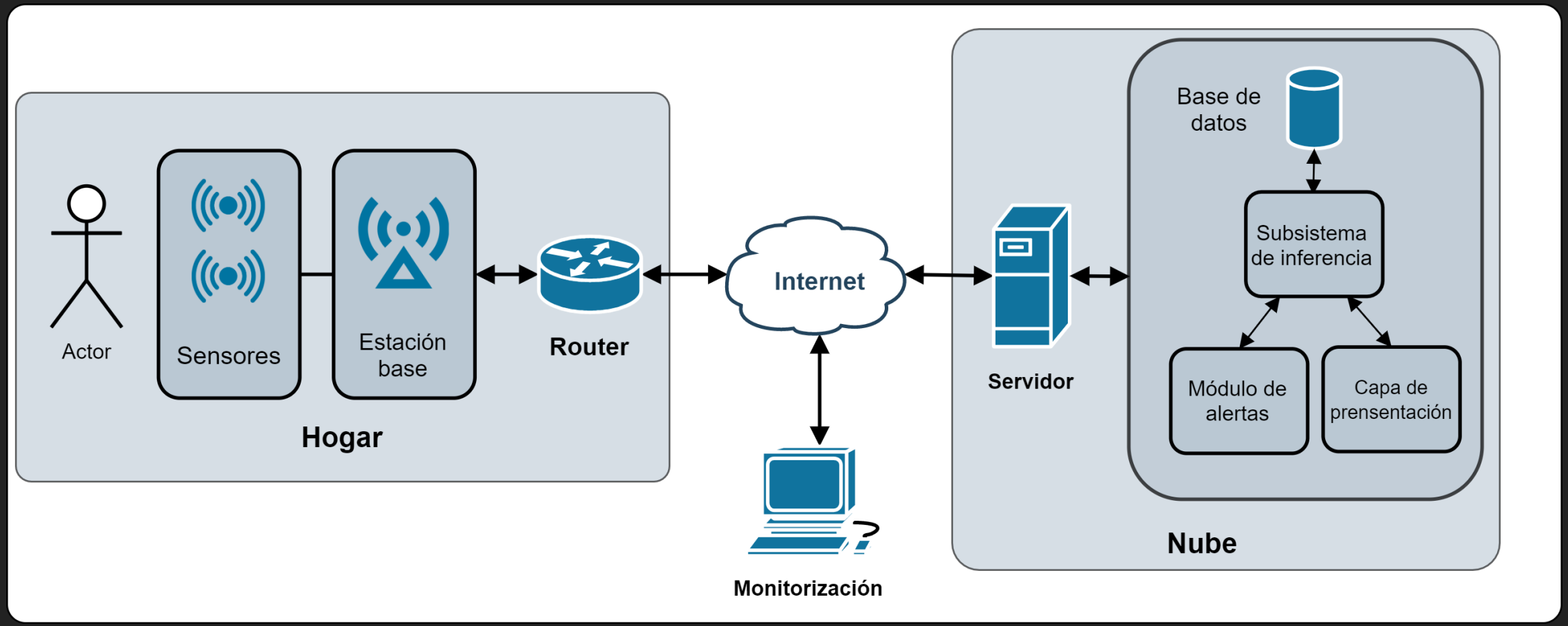
Diseño de la arquitectura

Arquitectura del sistema

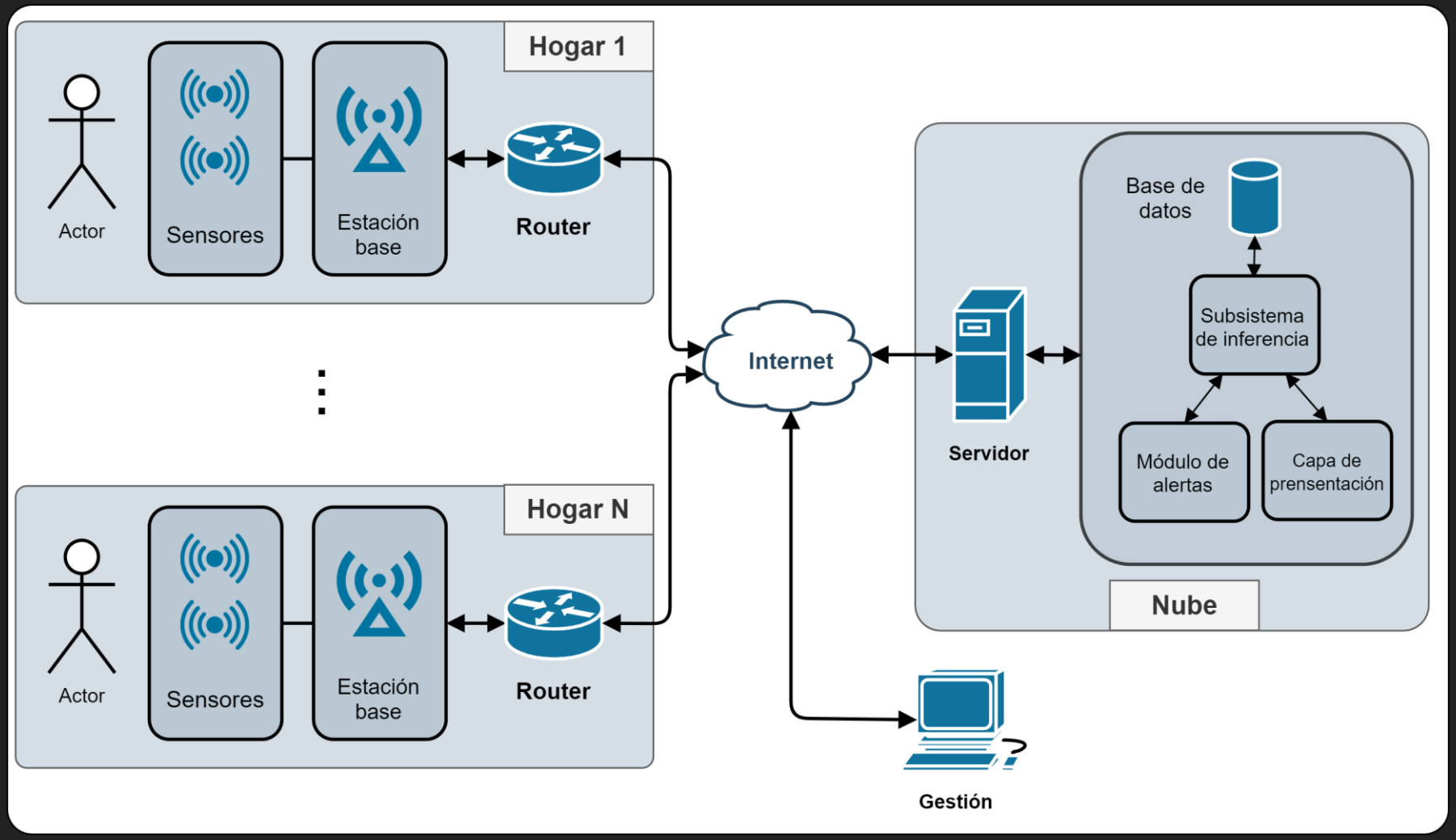


ESBOZO DEL DISEÑO DETALLADO

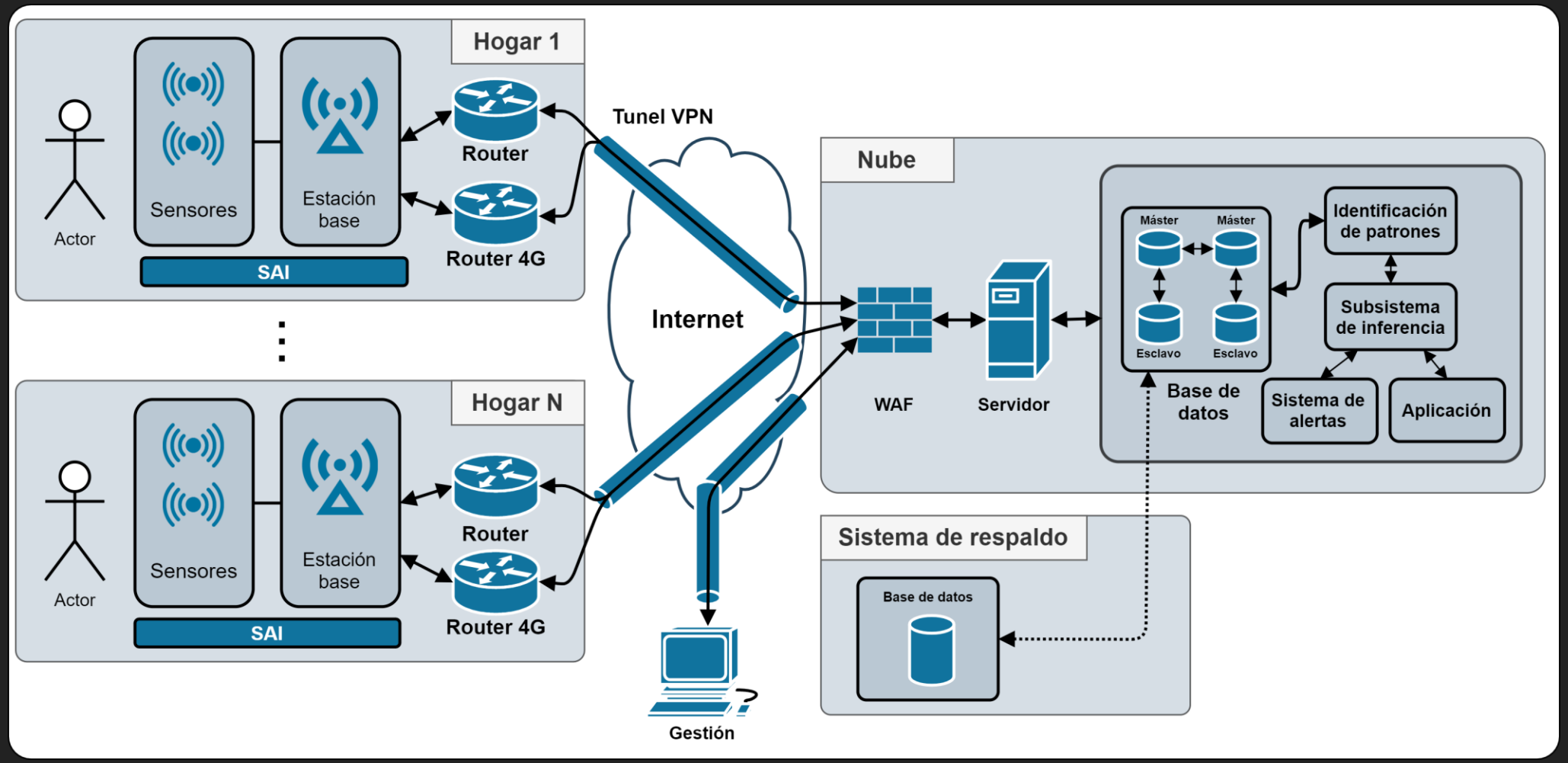
Esbozo del diseño detallado



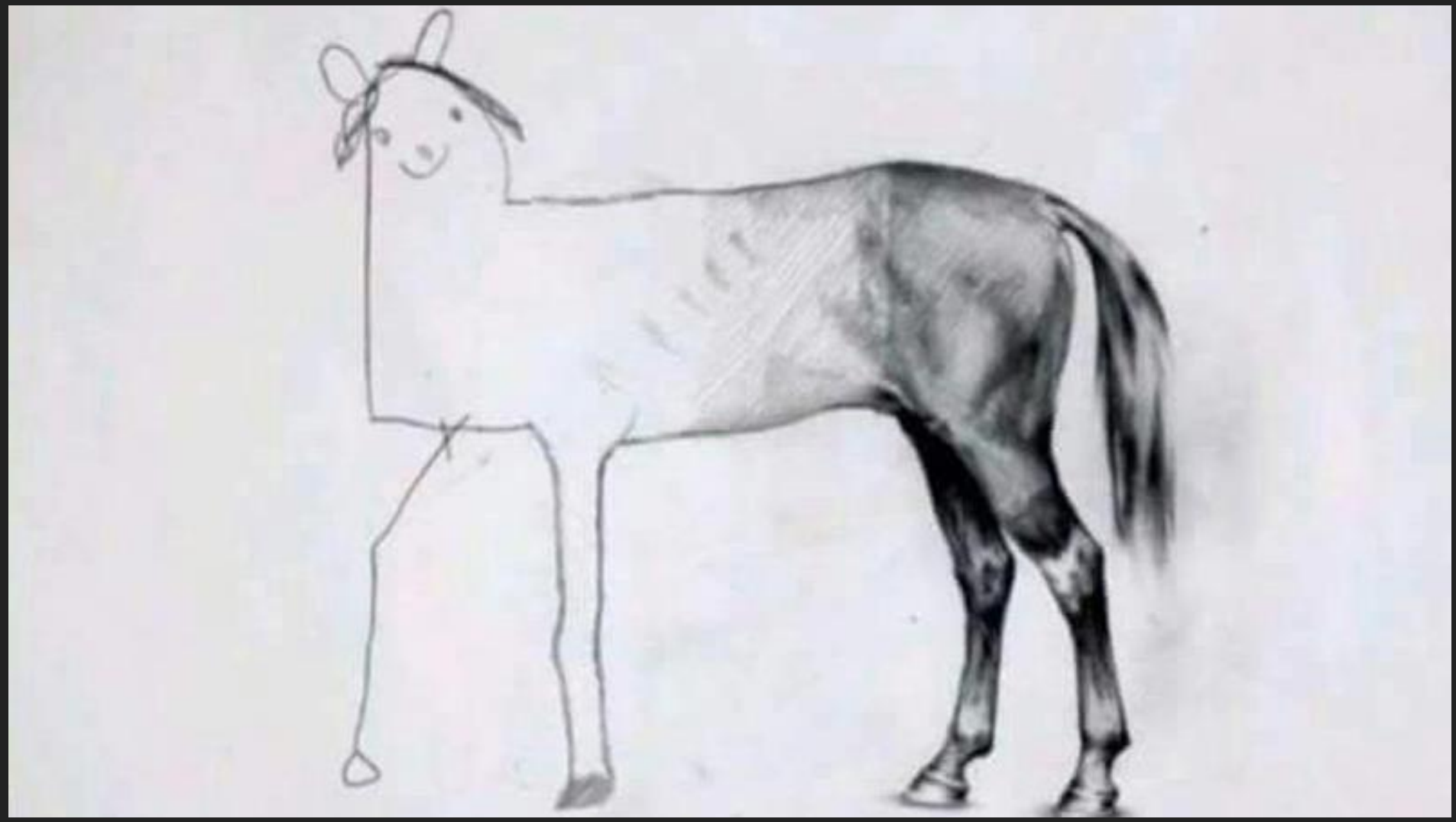
Esbozo del diseño detallado



Esbozo del diseño detallado



Esbozo del diseño detallado



Esbozo del diseño detallado

Hogares

- Sensores de movimiento y de presión.
- Pulsera IoT.
- Comunicación bluetooth con la estación base.
- Proceso de reducción y filtrado de datos en la estación base (Edge Computing).
- Almacenamiento temporal en la estación base.
- Segmentación de los datos de fuentes no confiables (posible suplantación de algún sensor).
- Identificación y autenticación de las estaciones base con la nube.

Esbozo del diseño detallado

Nube

- Conexión segura con los hogares a través de una VPN.
- Conexión segura con el personal de monitorización a través de una VPN.
- WAF y CDN para la aplicación web.
- API para la monitorización de alertas.
- Revisión y análisis de las librerías de terceros.
- Sistema de alertas con inteligencia artificial.
- Clúster de base de datos master-master para alta disponibilidad.
- Datos anonimizados.
- Copias de seguridad en una localización diferente.

IMPLEMENTACIÓN

Esbozo del diseño detallado (caso de uso)

El proceso de funcionamiento sería el siguiente:

1. La pulsera detecta una alarma por movimientos o parámetros de salud anormales.
   - Adicionalmente, una persona puede pulsar el botón que llevaría consigo, el cual va conectado por bluetooth a la pulsera, cuando detecta un cambio anómalo en su estado de salud.
2. Inmediatamente envía una señal desde la pulsera al punto de acceso (router) vía wifi o al móvil en caso de no estar en casa.
3. El sistema transmite una señal de alarma al centro de monitorización (CM).
4. Cuando el CM recibe el mensaje, trata de comunicar con la persona por medio del manos libres.
   - Éste cuenta con un altavoz y un poderoso micrófono a fin de poder comunicarse con la persona dependiente y tomar las correspondientes medidas.
5. En caso de no poder comunicar con la persona, se envía al equipo de emergencias al domicilio.

Implementación en el cliente

Dentro de la vivienda del cliente se instalará:

1. **Pulsera IoT**: Similar a Xiaomi Mi Band 5.
2. **Pulsador** que lleva encima la persona en todo momento.
3. **Sensores** IoT con el microprocesador NRF51822.

Importancia de la tecnología 5.0 respecto a 4.2.

Implementación en el cliente

El lado del servidor contará con las siguientes características:

1. Conexiones cifradas con SSL
2. APIS para comunicación entre aplicaciones en cloud.
3. Redundancia en las aplicaciones cloud.

Los servidores cloud representan el presente y el futuro.

- Se ha elegido Amazon Cloud Drive.

Todos los operarios tienen acceso a la nube y atienden las llamadas de auxilio.

Se debe contar con una buena respuesta ante incidentes ante posibles fallos en la nube

ESTRATEGIA DE ENTREGA Y SOPORTE

Estrategias de entrega y soporte

Cadena de suministro:

- Muestra de interacciones entre proveedores y clientes.
- Monitorización de la cadena de suministro.

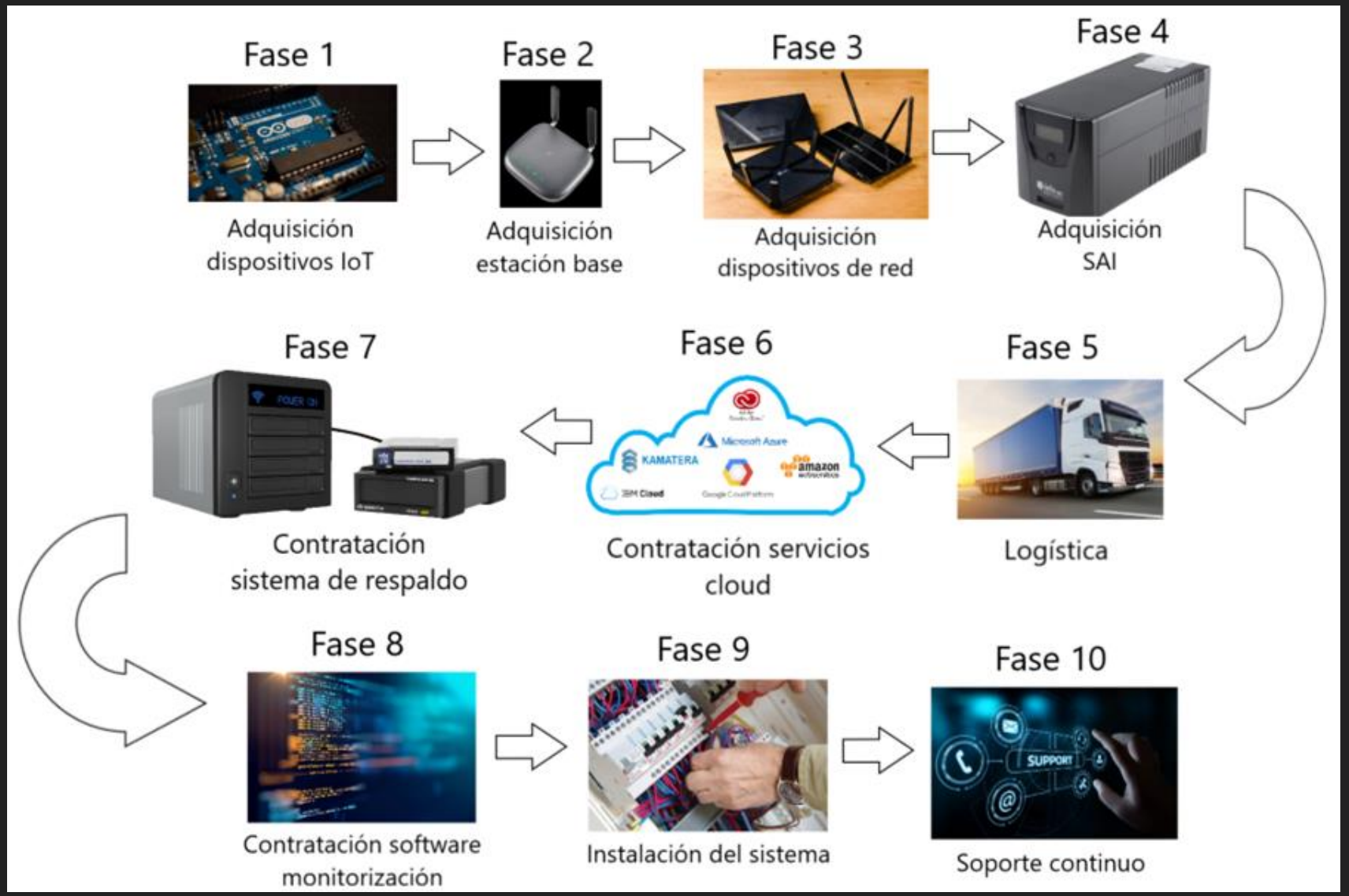
Formada por 10 fases principales:

- Desde adquisición de dispositivos IoT hasta el soporte continuo del sistema.

A tener en cuenta:

- El proveedor de dispositivos IoT compra su equipo a otro proveedor.

Cadena de suministro



MODELADO DE AMENAZAS Y SEGURIDAD

Modelado de amenazas y seguridad

Spoofing
Tampering
Repudiation
Information Disclosure
Denial of service
Elevation of privilege

- **Paso 1. Identificación de los objetivos de seguridad**
- **Paso 2. Descomposición del sistema e identificación de componentes clave**
- **Paso 3. Determinar las amenazas del sistema**

Modelo de clasificación **STRIDE**.

Identificación de los objetivos de seguridad

- Comunicación de los sensores inalámbricos.
- Utilización de la tecnología Bluetooth Low Energy (BLE).
- Objetivo final de velar por la seguridad de la persona dependiente.
- Mantener disponible el sistema en todo momento.

Identificación de componentes clave

- Sensores de presión.
- Pulsera de monitorización.
- Botón de ayuda con llamada a emergencias.
- Estación base (con manos libres para establecer la comunicación).

Amenazas del sistema y posibles contramedidas. Tecnología Bluetooth Low Energy (I)

- **Spoofing identity**: Falta de autenticación, atacante puede **suplantar a la persona dependiente**.
  - Implementar el “nivel 4” del modo de seguridad 1. Incluye autenticación y emparejamiento.
  - Configurar dispositivos en modo “no visible”.
- **Tampering with data**: Falta de autenticación o **errores de emparejamiento**. Atacante podría manipular datos de los sensores.
  - Implementar el “nivel 4” del modo de seguridad 1. Soluciona errores de emparejamiento y autenticación.
- **Repudiation**: **Ataques MIM**, permiten interceptar señales de los sensores. No se puede asegurar quién es el autor de los datos mandados a emergencias.
  - Algoritmo “**Numeric Comparison**” en la fase de autenticación. Requiere confirmación por parte del usuario legítimo.

Amenazas del sistema y posibles contramedidas. Tecnología Bluetooth Low Energy (II)

- **Information disclosure**: Confidencialidad puede verse afectada si se asocia la **dirección** "**BD_ADDR**" al usuario. Clave estática que desvela las conexiones.
  - Utilizar políticas de privacidad.
  - Algoritmo IRK que resuelve correctamente la dirección del dispositivo de confianza.
- **Denial of service**: Ataques "**signal jamming**" mediante inhibidores de frecuencias. Incluir sensores de potencia que alerten de altas potencias.
- **Elevation of privilege**: Los **dispositivos** utilizados **no requieren privilegios**.
  - Los usuarios que pueden acceder tienen los mismos privilegios.
  - No se puede tener una elevación de privilegios.

Amenazas del sistema y posibles contramedidas Vulnerabilidades routers internos

- **Debilidades**
  - Utilizar contraseñas por defecto en los routers.
  - Utilizar métodos de cifrado débiles.
    - **WEP**
    - **WPA**

- **Contramedidas**
  - Cambiar contraseñas por defecto.
  - Combinar mayúsculas, minúsculas, letras, números y caracteres especiales.
  - Utilización de **WPA2**.

GRACIAS

Sistema inteligente para monitorizar personas mayores y/o dependientes