# **Gestión de Riesgos**

## **1. Introducción**

Este documento identifica y analiza los riesgos potenciales en el desarrollo e implementación del sistema automatizado para el cuidado de plantas basado en IoT.

## **2. Identificación de Riesgos**

### **2.1 Riesgos Tecnológicos**

* **Falla en los sensores**: Los sensores pueden dejar de funcionar debido a desgaste o errores en la comunicación.
* **Problemas de conectividad**: Pérdida de conexión entre el microcontrolador y el servidor.
* **Seguridad de datos**: Posibles ataques a la comunicación o acceso no autorizado a la base de datos.

### **2.2 Riesgos Operativos**

* **Fallas en la alimentación eléctrica**: Interrupción del sistema debido a cortes de energía.
* **Errores en la interpretación de datos**: Lecturas incorrectas pueden generar alertas erróneas.
* **Mantenimiento de hardware**: Sensores y microcontroladores pueden requerir reemplazo periódico.

### **2.3 Riesgos de Desarrollo**

* **Errores de software**: Bugs en la aplicación móvil o en el backend pueden afectar la funcionalidad.
* **Demoras en la implementación**: Problemas en el desarrollo pueden retrasar la entrega del proyecto.
* **Compatibilidad con dispositivos**: Posibles problemas de compatibilidad entre sensores y la plataforma IoT.

## **3. Estrategias de Mitigación**

### **3.1 Medidas Preventivas**

* Uso de sensores de alta calidad con pruebas de rendimiento.
* Implementación de redundancia en la comunicación de datos.
* Cifrado de datos y autenticación en la aplicación.

### **3.2 Plan de Contingencia**

* **Fallas de hardware**: Procedimientos para reemplazo rápido.
* **Pérdida de conexión**: Reconexión automática y almacenamiento temporal de datos.
* **Errores de software**: Pruebas continuas y despliegues iterativos con rollback.

## **4. Monitoreo y Revisión**

* Auditorías periódicas de seguridad.
* Revisión de logs y análisis de fallos.
* Encuestas a usuarios para identificar posibles mejoras en el sistema.