**Análisis de Gestión del Riesgo**

**Dispositivo IoT - Basado en norma ISO 31000**

La fabricación física de nuestro dispositivo IoT utiliza componentes como son tarjeta de desarrollo ESP 8266 Wifi, Resistencias de 220 ohm, Leds de colores, Sensor Ultrasonido Ref. HC-SR04, Protoboard, Cable conector por USB y cables para conexión, los cuales al integrarse para conformar un dispositivo IoT , debe evaluarse y realizar una validación de riesgos específicos. Aplicando la norma ISO 31000, se identifican y gestionan los siguientes riesgos para asegurar la funcionalidad y fiabilidad del dispositivo.

A continuación, presentamos una matriz de riesgos enfocada en la fabricación física y la funcionalidad del dispositivo IoT.

**Matriz de Riesgos para la Fabricación Física y Funcionalidad del Dispositivo IoT**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Descripción del Riesgo** | **Impacto** | **Probabilidad** | **Nivel de Riesgo** | **Estrategia de Mitigación** |
| RF1 | Conexiones Inestables en la Protoboard | Alto | Alta | Alto | Asegurar que todas las conexiones estén adecuadas correctamente en la protoboard y revisarlas regularmente. |
| RF2 | Fallo de Componentes Electrónicos | Alto | Media | Alto | Realizar pruebas de funcionamiento antes de la integración completa. Tener componentes de repuesto disponibles. |
| RF3 | Cortocircuitos en la Protoboard | Alto | Media | Alto | Inspeccionar visualmente todas las conexiones antes de la conexión por cable al dispositivo de enlace. |
| RF4 | Sobrecarga de Corriente en LEDs y Resistencias | Medio | Media | Medio | Utilizar resistencias adecuadas y de ohmios necesarios para limitar la corriente. |
| RF5 | Interferencia Electromagnética | Medio | Media | Medio | Asegurar el correcto aislamiento y la separación de componentes sensibles. |
| RF6 | Fallo de la Fuente de Alimentación de corriente | Alto | Media | Alto | Utilizar fuentes de alimentación de calidad y probarlas bajo diferentes condiciones de carga. |
| RF7 | Sobrecalentamiento generado por los Componentes | Alto | Media | Alto | Implementar mecanismos de disipación de calor como disipadores o una ventilación adecuada. |
| RF8 | Problemas de Compatibilidad con Arduino | Alto | Media | Alto | Realizar pruebas exhaustivas de integración con el software Arduino y ajustar configuraciones según sea necesario. |
| RF9 | Desconexión Accidental de Componentes | Medio | Media | Medio | Fijar adecuadamente los componentes críticos a la protoboard para evitar desconexiones accidentales. |

**Descripción Detallada de Estrategias de Mitigación**

**RF1: Conexiones Inestables en la Protoboard**

**Estrategia para Mitigar:**

* Asegurar que todas las conexiones estén adecuadas correctamente en la protoboard y revisarlas regularmente.

**Acciones:**

* Inspeccionar visualmente las conexiones antes de cada prueba.
* Utilizar cables y conectores de buena calidad.

**RF2: Fallo de Componentes Electrónicos**

**Estrategia para Mitigar:**

* Realizar pruebas de funcionamiento de los componentes antes de la integración completa.
* Tener componentes de repuesto disponibles.

**Acciones:**

* Probar cada componente de manera individual.
* Mantener un stock de repuesto de los dispositivos a utilizar.

**RF3: Cortocircuitos en la Protoboard**

**Estrategia para Mitigar:**

* Inspeccionar visualmente todas las conexiones antes de la conexión por cable al dispositivo de enlace.
* Utilizar protectores contra cortocircuitos.

**Acciones:**

* Revisar visualmente las conexiones.
* Usar fusibles o en su defecto protectores de circuitos.

**RF4: Sobrecarga de Corriente en LEDs y Resistencias**

**Estrategia para Mitigar:**

* Utilizar resistencias adecuadas y de ohmios necesarios para limitar la corriente.

**Acciones:**

* Calcular el valor correcto de las resistencias refiriendonos al plano de construcción suministrado.
* Verificar el funcionamiento de los LEDs a utilizar por medio de un multímetro.

**RF5: Interferencia Electromagnética**

**Estrategia para Mitigar:**

* Asegurar el correcto aislamiento y la separación de componentes sensibles.

**Acciones:**

* Utilizar cables apantallados para conexiones críticas.
* Separar los componentes digitales de los analógicos para minimizar estas interferencias.

**RF6: Fallo de la Fuente de Alimentación de corriente**

**Estrategia para Mitigar:**

* Utilizar fuentes de alimentación de calidad y probarlas bajo diferentes condiciones de carga.

**Acciones:**

* Verificar que la fuente de alimentación es confiable y la tomacorriente sea certificada.
* Realizar pruebas de estrés a la fuente de alimentación.

**RF7: Sobrecalentamiento generado por los Componentes**

**Estrategia para Mitigar:**

* Implementar mecanismos de disipación de calor como disipadores o una ventilación adecuada.

**Acciones:**

* Adecuar disipadores de calor o ventilación natural a los componentes que generen mucho calor.
* Asegurar una ubicación adecuada del dispositivo en conjunto que no genere sobrecalentamiento.

**RF8: Problemas de Compatibilidad con Arduino**

**Estrategia para Mitigar:**

* Realizar pruebas exhaustivas de integración con el software Arduino en cuanto a versiones, compatibilidad y ajustar su configuración según sea necesario.

**Acciones:**

* Verificar la compatibilidad de los componentes en las bibliotecas de Arduino.
* Probar el software en entornos controlados para verificar su funcionalidad antes de su implementación en el dispositivo final.
* Consultar información tecnica del fabricante del software.

**RF9: Desconexión Accidental de Componentes**

**Estrategia para Mitigar:**

* Fijar adecuadamente los componentes críticos a la protoboard para evitar desconexiones accidentales.

**Acciones:**

* Utilizar herramientas manuales y/o soportes necesarios para asegurar los componentes a la protoboard.
* Revisar y ajustar de manera global las conexiones antes de utilizar el dispositivo.

Este levantamiento de información basado en la norma ISO 31000 inicia con la identificación y evaluación de los riesgos asociados en el primer sprint definido para nuestro proyecto. Los riesgos aquí mencionados pueden variar según la capacidad y tamaño del dispositivo IoT.