**Análisis de Gestión del Riesgo**

**Herramienta IoT Ingeniería de Software II - Basado en norma ISO 31000**

1. **Contexto**

**Contexto Externo e Interno de la solución a implementar**: Nuestro proyecto, implementa la metodología SCRUM, definiendo claramente las fechas de inicio, fin y los roles asignados. Además, identifica que para el proyecto se contemplan las normas ISO necesarias en cada sprint, lo que da un marco apropiado en cuanto a calidad y seguridad requerida para el desarrollo del proyecto.

**Objetivos del Proyecto**: Desarrollar y fabricar un dispositivo IoT con especificaciones claras y definidas en términos de funcionalidad y tecnología empleada (ESP8266, protoboard, cableado, sensor de proximidad HC-SR04) para recopilar la información que genera el mismo, trasmitirla y recibirla a través de AWS y mostrarla en un aplicativo (front) diseñado en Flutter.

**2. Identificación del Riesgo**

Dentro del análisis del montaje del dispositivo IoT y la integración de este con los servicios de AWS para la suscripción y publicación de los datos generados en el modelo de aplicación en Flutter, se contemplaron los posibles riesgos que se pueden generar, evidenciando la importancia de adherir la capacidad de riesgo en el desarrollo de cada sprint aplicando la norma ISO 31000 de gestión del riesgo. Es vital realizar una identificación exhaustiva de posibles riesgos que pueden afectar tanto el desarrollo como la implementación de nuestro proyecto, como lo son los riesgos técnicos, riesgos de seguridad o riesgos operacionales.

**3. Análisis del Riesgo**

**Evaluación de Impacto y Probabilidad**: Es necesario realizar un análisis de impacto y probabilidad de los riesgos potenciales que se vayan a definir. La norma ISO 31000 recomienda evaluar estos aspectos para priorizar los riesgos y asignar recursos adecuadamente.

**Métodos de Análisis**: Para nuestro proyecto, es necesario implementar una matriz de riesgos para el análisis de los escenarios propuestos y retroalimentar lo identificado para profundizar en el entendimiento de lo realizado a través de una medición de riesgos a través del tiempo.

**4. Evaluación del Riesgo**

**Priorización:** La evaluación de los riesgos en nuestro proyecto se enfoca a clasificar los riesgos según su criticidad y el estado actual de cada sprint del proyecto, para enfocarse en los riesgos más significativos mediante una clasificación y/o priorización de riesgos.

**5. Tratamiento del Riesgo**

**Planes de Acción**: Es necesario detallar planes específicos para tratar los riesgos que se identifiquen. Cada riesgo debe tener un plan de mitigación o contingencia, el cual debe estar alineado con la estrategia del proyecto.

**Asignación de Responsabilidades**: Dentro del proyecto, se tienen asignados roles y desglosadas las responsabilidades específicas y asi, realizar el análisis de riesgo por cada actor en cada etapa.

**6. Monitoreo y Revisión**

**Seguimiento Continuo**: La norma ISO 31000 enfatiza la necesidad de un monitoreo y revisión constante de los riesgos y los planes de tratamiento. Es necesario realizar este analisis en el documento.

**Revisiones Periódicas:** Se tienen establecido puntos de revisión al final de cada uno de los sprint definidos en el SCRUM, para evaluar la efectividad de las acciones de mitigación y actualizar la identificación de riesgos.

**7. Comunicación y Consulta**

**Transparencia y Comunicación:** La comunicación efectiva y la consulta continua entre los interesados no se encuentra detallada actualmente. Se han definido reuniones y ceremonias SCRUM, pero no se tiene el detalle del manejo de la comunicación específica sobre la gestión del riesgo.

**Documentación y Reportes**: Es necesario incluir una bitacora para documentar y reportar los riesgos inherentes al aplicativo y su tratamiento de forma continua.

**Tareas generales:**

* Realizar una Identificación de los riesgos y documentar todos los riesgos potenciales.
* Evaluar y clasificar estos riesgos a través de matrices de impacto y probabilidad para priorizar los riesgos.
* Desarrollar los planes de mitigación y contingencia asignando responsables.
* Implementar un seguimiento continuo del proceso de riesgos en las reuniones daily y revisiones de sprint para una gestión proactiva.
* Establecer canales claros para la comunicación de riesgos, dando accesibilidad a la información a los interesados en el proyecto.

**ANALISIS GENERAL DE LA INTEGRACIÓN DEL PROYECTO REALIZADO**

**RIESGOS TÉCNICOS (RT)**

**Fallos probables en la Configuración del Hardware**

Descripción: Funcionalidad del dispositivo IoT, posibles fallas al conectar y calibrar el sensor de ultrasonido HC-SR04 con el ESP8266.

* Impacto: Alto, ya que afectaría la capacidad del dispositivo IoT para recopilar y enviar datos.
* Probabilidad: Media, considerando la posible complejidad en la configuración.

**Problemas en el Uso del Software Arduino**

* Impacto: Alto, ya que afecta la lectura de datos y la funcionalidad del dispositivo iot
* Probabilidad: Media, teniendo en cuenta que, por calidad, debe utilizarse la versión más reciente del software

**Problemas en la Integración de Microservicios en AWS**

Descripción: Dificultades en la implementación y despliegue de microservicios para recibir y procesar datos.

* Impacto: Alto, puede impedir la correcta recepción y procesamiento de datos.
* Probabilidad: Media, debido a la posible complejidad y dependencias de servicios.

**Errores en el Desarrollo de la Aplicación Móvil en Flutter**

Descripción: Bugs o fallos en la lógica de la aplicación móvil para suscribirse a temas MQTT y manejar los datos.

* Impacto: Alto, ya que afectaría la usabilidad de la aplicación por parte del usuario final.
* Probabilidad: Media, basado en la complejidad del desarrollo de aplicaciones móviles.

**RIESGOS DE SEGURIDAD (RS)**

**Vulnerabilidad en la seguridad de la información**

Descripción: Protección adecuada de los datos transmitidos entre los dispositivos IoT, la nube y la aplicación móvil.

* Impacto: Bajo, poco riesgo de exposición de datos sensibles.
* Probabilidad: Baja, dependiendo de la implementación de medidas de seguridad.

**Acceso No Autorizado a Servicios AWS**

Descripción: Posibilidad que actores malintencionados accedan a servicios AWS debido a configuraciones incorrectas.

* Impacto: Alto, comprometer la integridad y disponibilidad de los datos.
* Probabilidad: Media, si no son configuradas las políticas de seguridad correctamente.

**RIESGOS OPERACIONALES (RO)**

**Falla en la conexión ante MQTT**

Descripción: Interrupciones en la conexión del cliente MQTT con el servidor, afectando la transmisión de datos.

* Impacto: Alto, ya que impediría la comunicación entre dispositivos y la aplicación.
* Probabilidad: Media, depende de la estabilidad de la red y la configuración.

**Problemas en el despliegue y mantenimiento de la infraestructura en AWS**

Descripción: Dificultades técnicas y errores en el despliegue de la infraestructura en AWS.

* Impacto: Alto, podría retrasar el proyecto y afectar su funcionalidad.
* Probabilidad: Alto, basado en la experiencia y habilidades del equipo en la gestión de AWS.

**RIESGOS OPERATIVOS (RM)**

**Planeación y comunicación**

Descripción: Retrasos en las tareas planificadas, afectando la entrega del proyecto.

* Impacto: Medio, puede llevar a sobrecostos y desconfianza por parte del cliente.
* Probabilidad: Alta, si no se gestiona adecuadamente el tiempo y los recursos.

**Falta de comunicación efectiva entre equipos**

Descripción: Problemas de comunicación entre los diferentes roles y equipos del proyecto.

* Impacto: Medio, puede llevar a malentendidos y errores en la implementación.
* Probabilidad: Media, basado en la estructura de comunicación definida.

**MATRIZ DE RIESGOS**

Esta matriz ha sido implementada con la información obtenida y analizada en nuestra primera sesión como equipo SCRUM donde se incluye la descripción, impacto, probabilidad, nivel de riesgo (teniendo en cuenta el impacto y la probabilidad del suceso) y las estrategias de mitigación mencionadas.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Descripción del Riesgo** | **Impacto** | **Probabilidad** | **Nivel de Riesgo** | **Estrategia de Mitigación** |
| RT1 | Fallo en la Configuración del Hardware | Alto | Media | Alto | Realizar pruebas exhaustivas del hardware antes del despliegue. Documentar y seguir guías de configuración precisas. |
| RT2 | Problemas en la Integración de Microservicios en AWS | Alto | Media | Alto | Implementar pruebas unitarias y de integración. Contar con un plan de rollback para el despliegue. |
| RT3 | Errores en el Desarrollo de la Aplicación Móvil en Flutter | Alto | Media | Alto | Realizar revisiones de código y pruebas de usuario. |
| RT4 | Problemas en el Uso del Software Arduino | Alto | Media | Alto | Capacitar al equipo en el uso del software Arduino. Documentar procedimientos y mantener ejemplos de código reutilizables. |
| RS1 | Vulnerabilidades en la Seguridad de la Información | Alto | Media | Alto | Implementar cifrado de datos en tránsito y en reposo. Realizar auditorías de seguridad periódicas. |
| RS2 | Acceso No Autorizado a Servicios AWS | Alto | Media | Alto | Configurar políticas de acceso mínimo necesario y utilizar autenticación multifactor (MFA). |
| RO1 | Fallo en la Conectividad MQTT | Alto | Media | Alto | Implementar mecanismos de reconexión automática. Realizar pruebas de carga para asegurar la estabilidad de la conexión. |
| RO2 | Problemas en el Despliegue y Mantenimiento de Infraestructura AWS | Alto | Media | Alto | Utilizar herramientas de infraestructura como código (IaC). Realizar despliegues en etapas controladas. |
| RM1 | Desviaciones en el Cronograma del Proyecto | Medio | Alta | Alto | Monitorear el progreso continuamente y ajustar las estimaciones de tiempo. Tener márgenes de tiempo para imprevistos. |
| RM2 | Falta de Comunicación Efectiva entre Equipos | Medio | Media | Medio | Establecer reuniones regulares y utilizar herramientas de colaboración efectivas (e.g., Slack, Jira). |

**Clasificación de Nivel de Riesgo**

* Alto: Riesgo crítico que requiere atención inmediata y detallar un plan de mitigación.
* Medio: Riesgo significativo que debe ser monitoreado y gestionado según el avance del proyecto.
* Bajo: Riesgo menor que puede manejarse con un seguimiento mínimo.

**DETALLE DE LAS ESTRATEGIAS DE MITIGACIÓN**

**RIESGOS TÉCNICOS:**

**RT1: Fallo en la Configuración del Hardware**

**Estrategia de Mitigación:**

* Realizar pruebas exhaustivas del hardware antes del despliegue.
* Documentar y seguir guías de configuración precisas.

**Acciones:**

* Crear un checklist de configuración y pruebas.
* Asegurar que todos los componentes están correctamente conectados y calibrados.

**RT2: Problemas en la Integración de Microservicios en AWS**

**Estrategia de Mitigación:**

* Implementar pruebas unitarias y de integración.
* Contar con un plan de rollback para el despliegue.

**Acciones:**

* Desarrollar y ejecutar pruebas automatizadas.
* Planificar y documentar el proceso de rollback para despliegues fallidos.

**RT3: Errores en el Desarrollo de la Aplicación Móvil en Flutter**

**Estrategia de Mitigación:**

* Realizar revisiones de código y pruebas de usuario.

**Acciones:**

* Programar revisiones de código periódicas.
* Realizar pruebas de usabilidad con usuarios finales.

**RT4: Problemas en el Uso del Software Arduino**

**Estrategia de Mitigación:**

* Capacitar al equipo en el uso del software Arduino.
* Documentar procedimientos y mantener ejemplos de código reutilizables.

**Acciones:**

* Organizar sesiones de capacitación y talleres prácticos sobre el uso de Arduino.
* Crear y mantener una biblioteca de ejemplos de código y procedimientos de solución de problemas comunes.

**RIESGOS DE SEGURIDAD**

**RS1: Vulnerabilidades en la Seguridad de la Información (Especifico, no general)**

**Estrategia de Mitigación:**

* Definir la ruta de aplicación para transferencia de la información y los datos entre los integrantes del proyecto Realizar chequeos de seguridad periódicos en cada daily.

**Acciones:**

* Implementar FTP seguro, encriptación y llaves privadas.
* Planificar auditorías de seguridad en cada sesión con los integrantes del equipo.

**RS2: Acceso No Autorizado a Servicios AWS**

**Estrategia de Mitigación:**

* Configurar políticas de acceso mínimo necesario al cloud de AWS y utilizar autenticación multifactor (MFA).

**Acciones:**

* Revisar y actualizar las políticas de IAM en AWS.
* Implementar MFA para todos los usuarios con acceso a AWS.

**RIESGOS OPERACIONALES**

**RO1: Fallo en la Conectividad MQTT**

**Estrategia de Mitigación:**

* Implementar mecanismos de reconexión automática.
* Realizar pruebas de carga para asegurar la estabilidad de la conexión.

**Acciones:**

* Configurar el cliente MQTT para reconectarse automáticamente en caso de desconexión.
* Ejecutar pruebas de carga para evaluar la resiliencia de la conexión MQTT.

**RO2: Problemas en el Despliegue y Mantenimiento de Infraestructura AWS**

**Estrategia de Mitigación:**

* Utilizar herramientas de infraestructura como código (IaC).
* Realizar despliegues en etapas controladas.

**Acciones:**

* Implementar Terraform o CloudFormation para la gestión de infraestructura.
* Planificar despliegues en entornos de prueba antes de producción.

**RM1: Desviaciones en el Cronograma del Proyecto**

**Estrategia de Mitigación:**

* Monitorear el progreso continuamente y ajustar las estimaciones de tiempo.
* Tener márgenes de tiempo para imprevistos.

**Acciones:**

* Utilizar herramientas de gestión de proyectos para seguimiento del progreso.
* Revisar y ajustar estimaciones de tiempo periódicamente.

**RM2: Falta de Comunicación Efectiva entre Equipos**

**Estrategia de Mitigación:**

* Establecer reuniones regulares y utilizar herramientas de colaboración efectivas (por ejemplo, en Slack, o Jira).

**Acciones:**

* Programar reuniones diarias de seguimiento (dailies) y reuniones de revisión de sprint.
* Adoptar herramientas de colaboración y asegurar su uso consistente.

Este levantamiento de información basado en la norma ISO 31000 inicia con la identificación y evaluación de los riesgos asociados en los sprint definidos para nuestro proyecto. Los riesgos aquí mencionados pueden variar según la aplicación realizada de cada una de las tecnologías que hemos involucrado en el proyecto. Por lo anterior y según lo planteado en la norma ISO de riesgos, es necesario realizar una evaluación detallada de riesgos para cada tecnología aplicada.