# **PLAN DE GESTIÓN DE RIESGOS**

**Proyecto:** Sistema de Gestión de Rutas  
 **Versión:** 1.0  
 **Fecha:** 2 de abril de 2025  
 **Responsable:** Equipo de Desarrollo y Administración

## **1. INTRODUCCIÓN**

Este documento establece el Plan de Gestión de Riesgos del proyecto "Sistema de Gestión de Rutas", cuyo objetivo es identificar, evaluar, mitigar y controlar los riesgos que puedan afectar negativamente el desarrollo, la implementación y la operación del sistema. Este plan es un componente clave de la gestión del proyecto y servirá como guía para la toma de decisiones en situaciones de incertidumbre.

## **2. METODOLOGÍA**

### **Identificación de riesgos**

La identificación de riesgos se realiza mediante el análisis del alcance del proyecto, entrevistas con el equipo, revisión de documentación técnica y análisis de experiencias previas. Los riesgos se clasifican en categorías como técnicos, humanos, operativos, de seguridad o externos.

### **Evaluación de riesgos**

Cada riesgo identificado se evalúa de acuerdo con dos parámetros:

* **Probabilidad de ocurrencia**: Alta, Media o Baja.
* **Impacto en el proyecto**: Alto, Medio o Bajo.

Se priorizan aquellos con mayor probabilidad e impacto.

### **Estrategia de respuesta**

Para cada riesgo se define una estrategia:

* **Evitar**: Eliminar la causa del riesgo.
* **Mitigar**: Reducir la probabilidad o el impacto.
* **Aceptar**: Asumir el riesgo si su impacto es tolerable.
* **Transferir**: Delegar el riesgo a un tercero.

## **3. MATRIZ DE RIESGOS**

| **ID** | **Riesgo** | **Probabilidad** | **Impacto** | **Estrategia** | **Responsable** |
| --- | --- | --- | --- | --- | --- |
| R1 | Caída del servicio de Firebase | Media | Alta | Mitigar: Backups regulares y contingencia local | Dev Backend |
| R2 | Conductor no completa el registro inicial | Alta | Media | Mitigar: Envío automático de recordatorios por correo | Admin del sistema |
| R3 | Incompatibilidad de la app con dispositivos Android | Media | Alta | Mitigar: Pruebas en múltiples versiones y dispositivos | QA Tester |
| R4 | Error humano en la asignación de rutas | Baja | Alta | Mitigar: Validaciones automáticas y revisión por parte del administrador | Admin Web |
| R5 | Problemas de conectividad móvil | Alta | Media | Mitigar: Sincronización diferida y almacenamiento local temporal | Dev App |
| R6 | Configuración insegura de reglas en Firebase | Baja | Alta | Evitar: Auditoría periódica de reglas de seguridad y control de acceso | Dev Backend |
| R7 | Dificultades de uso por parte del conductor | Media | Media | Mitigar: Mejora continua de UX y pruebas de usabilidad | UX/UI Designer |
| R8 | Pérdida de acceso a cuentas por olvido de credenciales | Baja | Alta | Mitigar: Implementar recuperación de contraseña por correo electrónico | Dev Backend |

## **4. PLAN DE RESPUESTA**

### **Riesgo R1 – Caída del servicio de Firebase**

* Realizar respaldos automáticos semanales de la base de datos.
* Definir procedimiento de contingencia y restauración.
* Utilizar sistema de monitoreo de disponibilidad.

### **Riesgo R5 – Problemas de conectividad móvil**

* Implementar lógica de sincronización en segundo plano.
* Permitir carga y edición offline temporal.
* Mostrar mensajes de estado de conexión al usuario.

### **Riesgo R6 – Configuración insegura**

* Configurar reglas por rol en Firestore antes del despliegue.
* Habilitar registros de acceso.
* Realizar auditorías mensuales del sistema de seguridad.

## **5. MONITOREO Y CONTROL**

* **Frecuencia de revisión:** Semanal, durante reuniones de seguimiento de sprint.
* **Herramientas utilizadas:** Google Sheets para la matriz de riesgos, Notion para tareas y documentación.
* **Actualización del plan:** Se actualizará al final de cada sprint o ante la aparición de nuevos riesgos.
* **Responsables del monitoreo:** Líder de desarrollo y administrador del sistema.