1. Identificación de Riesgos

Riesgos Técnicos

Desarrollo con retrasos

- Posibles demoras en la implementación de funcionalidades clave debido a problemas técnicos o falta de recursos.

Incompatibilidad con dispositivos móviles

- Que el sitio no funcione correctamente en algunos navegadores o dispositivos.

Fallas en la integración de sistemas

- Problemas al conectar el sistema de reservas con el de facturación o la base de datos.

Riesgos Legales y de Cumplimiento

Incumplimiento de normativas de protección de datos

- Sanciones por no cumplir con la Ley 1581 de 2012 (protección de datos personales).

Problemas con la facturación electrónica

- Errores en la emisión de facturas que generen inconvenientes con la DIAN.

Riesgos Operativos y de Recursos

Falta de disponibilidad del equipo

- Retrasos por ausencias imprevistas de miembros clave del equipo.

Problemas con proveedores externos

- Fallas en servicios de hosting, pasarelas de pago o APIs de terceros.

Riesgos de Seguridad

Ataques cibernéticos o fugas de datos

- Vulnerabilidades en el sistema que expongan información sensible de clientes.

Pérdida de datos por fallas en backups

- Corrupción de la base de datos o falta de copias de seguridad.

Riesgos de Comunicación y Gestión

Falta de alineación con el cliente

- Cambios de último momento en los requerimientos por falta de comunicación clara.

Sobrecarga de trabajo en etapas críticas

- Cuellos de botella en el desarrollo debido a una mala planificación.

2. Planes de Contingencia

Para Riesgos Técnicos

Retrasos en el desarrollo

- **Contingencia**: Implementar sprints más cortos con entregables parciales y priorizar funcionalidades críticas.
- **Acción**: Usar metodologías ágiles (Scrum/Kanban) para ajustar prioridades en tiempo real.

Incompatibilidad con dispositivos móviles

- **Contingencia**: Realizar pruebas tempranas en diferentes navegadores y dispositivos.

- **Acción**: Usar herramientas como BrowserStack y diseño responsive desde el inicio.

Fallas en integración de sistemas

- **Contingencia**: Desarrollar APIs robustas y documentadas, con pruebas de integración continuas.
- **Acción**: Usar entornos de staging para simular integraciones antes del lanzamiento.

Para Riesgos Legales y de Cumplimiento

Incumplimiento de normativas de protección de datos

- **Contingencia**: Asesorarnos con un abogado especializado en protección de datos desde la fase de diseño.
- **Acción**: Implementar encriptación de datos y políticas de privacidad claras.

Problemas con facturación electrónica

- **Contingencia**: Validar el módulo de facturación con un contador antes del lanzamiento.
- **Acción**: Usar soluciones previamente certificadas (ej: Facturador electrónico homologado).

Para Riesgos Operativos y de Recursos

Falta de disponibilidad del equipo

- **Contingencia**: Tener un plan de reemplazo temporal con otros miembros del equipo o freelancers.
- **Acción**: Documentar procesos clave para facilitar la transición.

Problemas con proveedores externos

- **Contingencia**: Contratar servicios alternativos (ej: tener un backup de hosting).
- **Acción**: Negociar SLAs (Acuerdos de Nivel de Servicio) con proveedores críticos.

Para Riesgos de Seguridad

Ataques cibernéticos o fugas de datos

- **Contingencia**: Implementar firewalls, autenticación de dos factores y auditorías de seguridad.
- **Acción**: Realizar pruebas de penetración (pentesting) antes del lanzamiento.

Pérdida de datos por fallas en backups

- **Contingencia**: Configurar backups automáticos en la nube y en servidores físicos.
- **Acción**: Hacer restauraciones de prueba periódicas para verificar integridad.

Para Riesgos de Comunicación y Gestión

Falta de alineación con el cliente

- **Contingencia**: Realizar reuniones semanales de seguimiento y prototipos interactivos.
- **Acción**: Usar herramientas como Figma o Miro para validar diseños antes de codificar.

Sobrecarga de trabajo en etapas críticas

- **Contingencia**: Distribuir tareas en subequipos y evitar dependencias críticas en una sola persona.
- **Acción**: Usar herramientas de gestión como Trello o Jira para monitorear el avance.

Conclusión

Hemos identificado los principales riesgos que podrían afectar el proyecto y definido planes de acción para minimizar su impacto. **Nuestra estrategia se basa en:**

✓ **Prevención** (pruebas tempranas, documentación, backups).
✓ **Mitigación** (soluciones alternativas, asesoría legal, comunicación constante).
✓ **Respuesta rápida** (protocolos claros para actuar ante imprevistos).

Si surge algún riesgo no previsto, el equipo está preparado para ajustar el plan y garantizar el éxito del proyecto.