Gestión de Riesgo y Planes de Contingencia

Identificación de Riesgos

- **Técnicos:**
    - **Fallos en el servidor**: Pueden causar interrupciones en el servicio, pérdida de datos y afectar la experiencia del usuario.
    - **Problemas de compatibilidad**: Incompatibilidades entre diferentes navegadores, dispositivos o versiones de software pueden causar errores o mal funcionamiento.
    - **Errores de código**: Bugs y errores en el código pueden llevar a fallos en el sistema, pérdida de datos o vulnerabilidades de seguridad.
- **De Gestión:**
    - **Retrasos en el cronograma**: Pueden ser causados por subestimación del tiempo necesario, problemas imprevistos o falta de recursos.
    - **Falta de recursos**: Incluye insuficiencia de personal, herramientas o presupuesto.
    - **Problemas de comunicación**: Malentendidos o falta de comunicación clara pueden llevar a errores y retrasos.
- **Externos:**
    - **Cambios en las regulaciones**: Nuevas leyes o regulaciones pueden requerir cambios en el proyecto.
    - **Problemas con proveedores**: Retrasos o fallos en la entrega de servicios o productos necesarios para el proyecto.
    - **Desastres naturales**: Eventos como terremotos, inundaciones o incendios pueden interrumpir el progreso del proyecto.

Análisis de Riesgos

- **Probabilidad:**
    - **Alta**: Es muy probable que ocurra.
    - **Media**: Puede ocurrir, pero no es seguro.
    - **Baja**: Es poco probable que ocurra.
- **Impacto:**
    - **Alto**: Tendrá un efecto significativo en el proyecto.
    - **Medio**: Tendrá un efecto moderado en el proyecto.
    - **Bajo**: Tendrá un efecto menor en el proyecto.

- **Matriz de Riesgos:**
    - Clasificar los riesgos en una matriz de probabilidad e impacto para priorizarlos. Por ejemplo:
        - **Alta probabilidad y alto impacto**: Prioridad máxima, requiere atención inmediata.
        - **Baja probabilidad y bajo impacto**: Prioridad baja, puede ser monitoreado pero no requiere acción inmediata.

Planes de Contingencia

- **Riesgo: Fallo en el servidor:**
    - **Plan de Contingencia:**
        - **Implementar un sistema de respaldo y recuperación**: Realizar copias de seguridad regulares y tener un plan de recuperación ante desastres.
        - **Monitoreo continuo**: Utilizar herramientas de monitoreo para detectar y resolver problemas rápidamente.
        - **Redundancia**: Configurar servidores redundantes para asegurar la disponibilidad del servicio.
- **Riesgo: Retrasos en el cronograma:**
    - **Plan de Contingencia:**
        - **Ajustar el cronograma**: Revisar y actualizar el cronograma regularmente para reflejar el progreso real.
        - **Reasignar recursos**: Mover recursos de tareas menos críticas a tareas prioritarias.
        - **Comunicación clara**: Mantener una comunicación abierta y clara con el equipo y los stakeholders sobre los cambios en el cronograma.
- **Riesgo: Problemas de compatibilidad:**
    - **Plan de Contingencia:**
        - **Pruebas de compatibilidad tempranas y frecuentes**: Realizar pruebas en diferentes navegadores, dispositivos y versiones de software desde el inicio del proyecto.
        - **Documentación clara**: Mantener una documentación detallada de los requisitos de compatibilidad.

- **Actualizaciones regulares**: Mantener el software y las herramientas actualizadas para minimizar problemas de compatibilidad.